

AC 23.1309-1-E PUBLIC COMMENTS FROM CESSNA, GARMIN, EMBRAER, AND CIRRUS

Originating Office: ACE-100	Document Description: SYSTEM SAFETY ANALYSIS AND ASSESSMENT FOR PART 23 AIRPLANE	Project Lead/Reviewer ERVIN DVORAK	Reviewing Office: ACE-111	Date of Review: 2-22-11
---------------------------------------	---	--	-------------------------------------	-----------------------------------

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	5a	This paragraph seems to conflict with the paragraph “a. System Safety Assessment Requirements” section (found in the preamble on page 41529) of the Certification of Turbojets NPRM published in the Federal Register. That paragraph implies that 23.1309 does not apply to conventional mechanical and electromechanical systems with well established design and certification processes. If the preamble in the FR carries the weight of the rule, and it conflicts with the AC, doesn't the preamble have greater precedence?			<p>Adopted.</p> <p>The first part of the preamble is not clear on the application of conventional mechanical systems, but it is clarified later in the preamble. Simple and conventional systems only required a design and installation appraisal not quantitative analysis.</p> <p>This was due to changes later in the process of the rulemaking. Later in the preamble it explained the intention of the simple and conventional systems for design and/or installation appraisal. There should not be any quantitative involved.</p> <p>The introductory text in the rule is reduced. New advance technology in mechanical systems such as complex</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
					<p>actuators may need a 23.1309 analysis.</p> <p>Section 23.1309 (b) (4), (b) (5), (c), (d), and (e) and Appendix K are deleted from the rule since they are represent Figure 2 and Figure 3 in the AC and is only an overview of the process.</p>
Cessna	6.a.(5)	This part seems to support what was posted in the Certification of Turbojets NPRM, but it conflicts with the paragraph 5.a.			<p>Adopted.</p> <p>This section is explaining the difference amendments of 23.1309. The preceding paragraph is for amendment 23-49 so the requirements are different. This section is revised.</p>
Cessna	6.a.(6)	The requirements in the new Appendix K to Part 23 are more stringent than part 25 in some cases. For example, a control and monitor situation on part 25 usually has one channel as level A (control) and the other channel as level C (the monitor). If the ACO agrees, this path is			<p>Adopted.</p> <p>For quantitative assessment please see note that states on the order.</p> <p>See Cessna 5a disposition for more information.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>supported by the process outlined in SAE ARP 4754 (which is referenced in this AC). Now, the AC table is part of the rule, and the table for a commuter aircraft has P=A, S=B. This would seem to indicate that the part 25 processes is not good enough, and the monitor for this part 23 program, now has to be level B. A solution would be to secure ACO acceptance of the hardware/software level for the secondary path if it is not level B. At the same time, placing the numerical requirements in the rule also raises the bar because for Hazardous and Catastrophic failure conditions, the note (note 1) that conveys the intent that "on the order of" analysis is gone. So a probability of 1.00000e-9 per flight hour no longer complies with the rule, because the rule in appendix K has a target of less than 1e-9. The same is true of hazardous classification. Cessna Engineering understands the</p>			<p>The S=B is for the secondary system, not for the monitor of the primary system. Simple and conventional systems only required a design and installation appraisal not quantitative analysis.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		desire to place a hard number in the rule, but there are many simple and conventional systems that don't meet the hard number if the analysis is done correctly, but they do meet the "on the order of" goal.			
Cessna	7	Cessna Engineering suggests an update of the Acronyms list and the note in Paragraph 4.c to reflect the use of EASA Certification Specifications in lieu of Joint Aviation Requirements.			Adopted. When this AC went out for comments, the existing ARP 4754 referred to JAR. With the revision of ARP 4754a after this AC was issued for comments, the JAR acronym can be deleted.
Cessna	8.h	Cessna Engineering has concerns regarding this definition. If a flight test is being done to show that the effects on the aircraft are crew are no worse than Major, and flight test uses "continued safe flight and landing" for pass/fail, all that has really been shown is that the effects are not catastrophic. They could be hazardous, or minor, but we haven't shown they are not major. Cessna Engineering suggests that			Not adopted. This phrase is used throughout the regulations and guidance in parts 23 and 25. It is the term used that is related to the definition of catastrophic failure conditions. Flight test, if necessary, should determine the appropriate failure conditions, not just pass fail criteria for continued safe flight

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		this definition be deleted from the Draft AC.			and landing.
Cessna	8.i	This seems to disagree with the Certification of Turbojets NPRM preamble that implies that if the system is simple and conventional, 23.1309 does not apply to that system. Cessna Engineering requests clarification of this potential opportunity for discrepancy.			<p>Adopted.</p> <p>The introductory text is reduced and only has this portion of the text only in the AC. New advance technology in mechanical systems such as complex actuators may need a 23.1309 analysis.</p> <p>Also, Appendix K and 23.1309 (b) (4), (b) (5), (c), (d), and (e) will be deleted and they will only appear in the text, Figure 2, and Figure 3 of the AC.</p> <p>See Cessna 5a disposition for more information.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	8.j	Cessna Engineering has reservations regarding this definition due to the fact that it supports the previous definition in 8.h by indicating that continued safe flight and landing is the pass/fail criteria.			<p>Not Adopted.</p> <p>This phrase is used throughout the regulations and guidance in parts 23 and 25. It is the term used that is related to the definition of catastrophic failure conditions.</p> <p>The term “critical function” is associated with a catastrophic failure condition. Newer documents may not refer specifically to the term “critical function.”</p>
Cessna	8.k	Cessna Engineering believes that this definition is applicable if the applicant chooses to follow the process in SAE ARP 4761 on their small part 23 airplane. The applicant will not do a design appraisal on the minor failure conditions because the major, hazardous and catastrophic failure conditions are passed to the PSSA.			<p>Not Adopted.</p> <p>ARP 4761 is just guidelines and this AC oversteps the ARP. This AC is guidance and it agrees with the rule and past and current parts 23 & 25 ACs including part 25 itself. ARP 4761 is not required for part 23 airplanes.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	8.m	Cessna Engineering recommends that 8.1 and 8.m are combined.			<p>Not Adopted.</p> <p>They are different terms, but are similar in the definition used in the RTCA documents.</p> <p>For this AC, DALs in figure 2 and throughout this AC are also intended to correlate to software levels in RTCA/DO-178B and complex hardware design assurance levels in RTCA/DO-254 for the system or item.</p>
Cessna	8.p	This class of failure conditions between major and hazardous is not defined in the proposed rule (appendix K) or in AC 23.1309-1C, -1D, -1E or in SAE ARP 4761. Cessna Engineering requests that the FAA clarify its position with respect to this failure condition.			<p>Not Adopted.</p> <p>“Essential” was and still used in older rules and other documents for safety assessments and the part 23 and 25 regulations use this term. So sometimes the requirements may have to be related to even in this AC.</p>
Cessna	8.r	If the power to the equipment is lost, would the hazard condition be hazardous or catastrophic? If this relates to the Part 91 requirements (TOMATO FLAMES) isn't the hazard			<p>Not Adopted.</p> <p>“Essential” was and still used in older rules and other documents for safety assessments and the part 23 and 25 regulations use</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		condition driven by the effect on the aircraft and crew? Cessna Engineering requests that the FAA clarify its position with respect to this failure condition.			this term. So sometimes the requirements may have to be related to even in this AC.
Cessna	8.v.(5)	Cessna Engineering recommends that Note 2 be deleted since the referenced AC is now over 10 years old, and it is cancelled.			Not Adopted. This term is still used in older rules and other documents for safety assessments. The regulations in Part 23 and 25 still use this term. So sometimes the requirements may have to be related to even in this AC.
Cessna	8.x	Cessna Engineering recommends the FAA to place a reference to SAE ARP 4761 here.			Not Adopted. ARP 4761 is just guidelines and this AC oversteps the ARP. This AC is guidance and it agrees with the rule and past and current part 23 & 25 ACs including part 25 itself. ARP 4761 is not required for part 23 airplanes.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	8.pp	Cessna Engineering recommends that this should be expanded to include the reduction in DAL for HW/SW and the guidance in SAE ARP 4754.			<p>Not Adopted.</p> <p>ARP 4761 is just guidelines and this AC oversteps the ARP. This AC is guidance and it is agrees with the rule and past and current part 23 & 25 ACs including part 25 itself. ARP 4761 is not required for part 23 airplanes.</p> <p>The ARP is still in the draft stage and has not been approved by the SAE and accepted by the FAA.</p>
Cessna	8.qq	The preamble in the Certification of Turbojets NPRM gives greater latitude than this definition. The wording in the NPRM allows for “close similarity” and does not require nearly identical (see pg 41532 of the NPRM Federal Register notice).			<p>Adopted.</p> <p>Minor changes were made to the definition.</p>
Cessna	8.ss	Why not just reword this to say that no catastrophic failure condition can result from a single failure using the process described in SAE ARP 4761?			<p>Not Adopted.</p> <p>ARP 4761 is just guidelines and this AC oversteps the ARP. This AC is guidance and it is agrees</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
					with the rule and past and current part 23 & 25 ACs including part 25 itself. ARP 4761 is not required for part 23 airplanes.
Cessna	10.b(1)	The Certification of Turbojets NRPM seems to imply that a conventional mechanical and electromechanical system with well established design and certification processes do not have to comply with 23.1309. Cessna Engineering thinks the first step in this process would be to determine if 23.1309 applies to the system if it is a conventional mechanical system without SW or HW DAL.			Not Adopted. These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before the regulations required a safety assessment. Adopted. See Cessna 5a disposition for more information.
Cessna	Figure 1	It seems here that “essential to operation” means the failure condition is catastrophic. Cessna Engineering suggests that the FAA set up the flow chart to say that.			Not Adopted. These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before the regulations required a safety assessment. Figure 1 does not apply to safety assessment and the related

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
					ARPs.
Cessna	10.b(3)(a)	This is covered by the Particular Risks Analysis in SAE ARP 4761. In this case, does hazard include minor failure conditions, major failure condition, hazardous and catastrophic?			<p>Not Adopted.</p> <p>These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before the regulations required a safety assessment. Figure 1 does not apply to safety assessment and the related ARPs</p> <p>As noted in the AC.</p> <p>There is a difference between “hazardous” as used in general policy or regulations and “hazardous failure condition” as used in an FHA. When the term "hazard" or "hazardous" is used in general policy or regulations, it is generally used as shown in this definition. A hazard could be a failure condition that</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
					relates to major, hazardous, or catastrophic.
Cessna	10.b(3)(b)	Cessna Engineering requests clarification on the use of “similarity” in this passage. Is this usage of “similarity” tantamount to the “nearly identical” definition above, or does it follow the interpretation in the Certification of Turbojets NPRM?			Adopted. The word “similarity” in the AC or in the preamble is not intended to be different. Minor changes were made to the definition in the AC.
Cessna	10b(3)(c)	This passage seems to indicate that even if the hazard can be caused by 10 independent probable things, it is not acceptable on a multiple engine aircraft. If each of the things have a probability of 1e-3, and each of the 10 are truly independent, then the probability is 1e-30. This far exceeds the requirement of 1e-9 for a catastrophic, yet the paragraph seems to indicate that a redesign may be required. Is this correct understanding?			Not Adopted. These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before we required a safety assessment. Figure 1 does not apply to safety assessment and the related ARPs. See definition of probable in the AC.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	11.a	Cessna Engineering requests that the standards staff at SAD take the opportunity to address the difference between “prevent hazards” and “safeguard against hazards”. Cessna Engineering’s interpretation of “prevent” can’t happen, and “safeguard” means can happen, but there still is some protection. In addition, it is not clear if “hazards” in this paragraph line up with failure conditions that are minor, major, hazardous.			<p>Adopted.</p> <p>The AC was revised for clarification.</p> <p>These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before the regulations required a safety assessment. Figure 1 does not apply to safety assessment and the related ARPs</p>
Cessna	11.b	In this section, the difference between safeguard and prevent still seems unclear (reference the comment for 11.a).			<p>Adopted.</p> <p>The AC was revised for clarification.</p> <p>Not Adopted.</p> <p>These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before the regulations required a safety assessment.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	12.e	This paragraph seems to contradict the words in the Certification of Turbojets NPRM that say 23.1309 has been applied in situations where it wasn't intended.			<p>Adopted.</p> <p>The AC was revised for clarification.</p> <p>These paragraphs do not apply to the safety assessments process. They were a requirement for 23.1309 before we required a safety assessment.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	13.a	<p>This seems very vague and therefore open to inconsistent application: Cessna Engineering would propose that the Preliminary System Safety Assessment as done per SAE ARP 4761 would meet this requirement and should be listed as an acceptable means. Additionally, the probability requirements as applied in 23.1309 are based on random distribution across a fleet of aircraft, i.e. a 10E-5 event can happen the first hour (then not for another 100,000 hours) and be fully compliant with the requirements. They simply cannot be applied to the typical flight test or F&R environment because the sample is too small to determine if the probability has really been met. Cessna Engineering would propose that the FAA consider language to reflect what is current practice in some areas of aircraft development and certification-- that is to require root cause</p>			<p>Partial Adopted.</p> <p>The rule and this paragraph are revised and the guidance is in the preamble of the rule and the AC to explain the intent.</p> <p>It was not intended that the probability requirements as applied in 23.1309 that are based on random distribution across a fleet of aircraft can be applied on the first hour and be fully compliant with the requirements.</p> <p>They simply cannot be applied to the typical certification flight test or F&R environment because the sample is too small to determine if the probability has really been met. The current practice in some areas of aircraft development and certification; that is to require root cause analysis and corrective action (including traceability to production incorporation of the change) for any and all failures</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>analysis and corrective action (including traceability to production incorporation of the change) for any and all failures encountered during the identified phase of flight test, F&R, qualification or bench testing with more robust corrections and substantiation of the correction required for higher criticality parts</p>			<p>encountered during the identified phase of flight test, F&R, qualification or bench testing with more robust corrections and substantiation of the correction required for higher criticality parts.</p> <p>Some system can be approved and still have known defects (e.g., software open problem reports) in required functions as long as the defects do not rise to the level that they are deemed not certifiable. However, functional defects that are deemed not certifiable would have to be corrected prior to obtaining approval.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	13 a	<p>23.1309(a)(3): Revised 10-12-10 Change due to cost analysis.</p> <p>From: George Thurston/AWA/FAA, APO-300, Regulatory Analysis,</p> <p>09/21/2010 09:17 AM 23.1309(a)(3) This change has the potential to add significant cost to a project depending on how much documentation is required to satisfy the FAA that the requirement has been met. As written the ACO's would have significant latitude in what they feel is adequate documentation to show that something meets the requirements. Also, it could require the applicant to write new specifications that would have been more simply addressed by review of the suppliers documents in the past.</p> <p>23.1309(a)(4) This proposed change has the potential to add a large cost to all certification projects. For a lot of minor failure conditions the current practice is to identify the problem and make the type design change and there would be little formal documentation in the records of every one of those changes. This proposed change will require formal documentation of the root cause and corrective action. As an example, one recent program had approximately 200 minor failure conditions. If it is assumed that it takes 4 hours to write the root cause and corrective action documentation (and this might be on the low side) and at a rate of \$150/hour this would amount to a cost impact just for the minor conditions of approximately \$120,000. It is questionable whether this amount of effort is justifiable for the minor items.</p>			
Cessna	13 a	<p>23.1309(a)(3): Revised 10-12-10 Change due to cost analysis.</p> <p>9-23-10: Pat, For the final rule, I do not have a problem in deleting 23.1309 (a)(4) since Parts 25,27, and 29 do not have such a requirements and do not have any problems. It was added by recommendations due to Eclipse program. We should also be able to delete 23.1309 (a)(3), since the Part 25 NPRM does not have this requirements. If we delete both 23.1301(d) and 23.1309(a)(3), part 23, the human factors may not be to happy. Regardless what is deleted or change the preamble of the rule needs to be revised.</p> <p>9-28-10: Pat, I reviewed and I concur. However, due to the cost analysis, we may have to change sections 23.1309 (3) and (4). I am now working with George Thurston and the applicants that perform the costs analysis.</p> <p>9-29-10: Pat, I also called Cessna to request what they meant by root cause analysis in their comment. In my conversation with them, it appear to me that Cessna provided George the cost analysis on 23.1309 (a) (3) and (a) (4). I am planning to telework 3 hours this morning to work a change to the Certification of Part 23 Turbofan- or Turbojet Powered Airplanes and Miscellaneous Amendment final rule.</p> <p>9-29-10: Pat and George. George I called you yesterday and left a message on your answer machine. I also called Cessna to request what they meant by root cause analysis in their comment. In my conversation with them, it appear to me that Cessna provided George the cost analysis on 23.1309 (a) (3) and (a) (4) as shown on your email below.</p> <p>I have decided to deleted 23.1309(a)(3) that was not in the NPRM and make a slight revision to 23.1309 (a)(3) that was in the NPRM and</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>changed to 23.1309(a)(4) due to 23.1309(a) (3) was added in the final rule, but now deleted. I also made minor changes to the preamble. The final rule with the changes is attached.</p> <p>The changes to the preamble are minor since originally the intend in the NPRM of 23.1309 (a)(2) was included in the new 23.1309(a)(3) that is now deleted. Section 23.1309(a)(3) was added in the final rule for the human factors comments if they did not understand 23.1309(a)(2). I will have more guidance in AC 23.1309-1E for them.</p> <p>The change to 23.1309(a)(3) that was 23.1309(a)(4) will reduce the cost since a root cause analysis will only be required for the final phase of certification that is TIA for FAA flight test. This phase of flight test was the main concern during the Eclipse program. This change will reduce the number of minor changes so the cost will be much lower. This was the original intent of 23.1309(a)(3) in the NPRM. The preamble in the NPRM stated it was applicable fro all functional reliability, flight testing, or flight evaluations. This change makes it more specific that is for only during TIA for FAA flight test.</p> <p>In my conversation with Cessna they do the root cause analysis, but they did not want that the root cause analysis to require FAA approval since it takes too long. I will have this in the guidance of AC 23.1309-1E, but not in the preamble. George accepted the changes.</p>			
Cessna	14.a	<p>Cessna Engineering believes that this conflicts with the statement on page 41529 of the Certification of Turbojets NPRM. SAE ARP 4761 has a great chart on page 23 that has been used on previous certification programs.</p>			<p>Partially Adopted.</p> <p>See Cessna 5a disposition for more information.</p>
Cessna	Figure 2	<p>Cessna Engineering suggests that Note 1 be removed unless the table is also in Part 23. Cessna Engineering recommends that the table be removed from Part 23 and that the applicant should propose an agreeable plan for showing compliance to 23.1309. The same comment would be applied for hazardous and catastrophic cases in each of the</p>			<p>Adopted.</p> <p>For quantitative assessment please see note that states “on the order”.</p> <p>Also, The proposed Appendix K and 23.1309 (b) (4), (b) (5), (c), (d), and (e) are deleted and they will only appear in the text, Figure 2, and Figure 3 of the AC.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>four classes of aircraft. Cessna Engineering suggests only noting it in one place. Because of the issue with the difference between control and monitor, and the fact that this table cannot capture the detail in SAE ARP 4754 and DO-254, Cessna Engineering recommends not placing the table in Part 23, leaving it here, and for the Class IV catastrophic case, open the door for the applicant to propose a monitor (secondary) path using the SAE ARP 4754 or DO-254 process.</p>			
Cessna	16.a	<p>Cessna Engineering recommends the placement of a reference to Figure 4 in SAE ARP 4761. Cessna Engineering suggests that the input to the table is to first identify if 23.1309 applies to the system being considered?</p>			<p>Not Adopted.</p> <p>ARP 4761 is just guidelines and this AC oversteps the ARP. This AC is guidance and it is agrees with the rule and past and current part 23 & 25 ACs including part 25 itself. ARP 4761 is not required for part 23 airplanes.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	Figure 3	In Part 25, Minor Failure Conditions are placed in the FHA summary table and not carried to the PSSA. The design and installation appraisal for Minors is not described in 4761			Not Adopted. ARP 4761 is just guidelines and this AC oversteps the ARP. This AC is guidance and it is agrees with the rule and past and current part 23 & 25 ACs including part 25 itself. ARP 4761 is not required for part 23 airplanes.
Cessna	16.b(4)	At what point does the applicant propose that 23.1309 does not apply because the system is conventional mechanical?			Adopted. See Cessna 5a disposition for more information.
Cessna	17.a & 17.b	If the applicant is following a top down approach, then starting with the top loss of function, all the things that contribute to it will be picked up, and they will be covered. Is the intent to address the design appraisal by the ZSA (as described in SAE ARP 4761?) Cessna Engineering does not believe an applicant can adequately determine safety effects without an FHA.			Adopted. A revision was made. Agree an FHA is always required, but it may not require much detail for no safety effects and minor failure conditions.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	17.c(1)	The Certification of Turbojets proposed rule as published in the Federal Register seems to allow more latitude in similarity determinations, Cessna Engineering believes that the wording here should be adjusted to agree with the preamble of the proposed rule.			Adopted. A minor change was made to the definition.
Cessna	17.c(2)	How are conventional mechanical systems or electromechanical systems with well established design and certification processes handled? The Certification of Turbojets proposed rule infers that they are exempt from the requirements of 23.1309.			Adopted. See Cessna 5a disposition for more information.
Cessna	17.c(3)	Cessna Engineering's opinion is that an FMEA really is not designed to handle high complexity systems. Practical experience has demonstrated that a Fault Tree Analysis (FTA) can really find that single point processor that does both control and monitor (which we agree is a bad thing) where an FMEA would not. Cessna Engineering			Adopted. The current text in this paragraph is very similar to the part 25 AC; however, a minor change was made.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		suggests that the AC recommend the use of an FTA for these situations.			
Cessna	17.c(4)	Cessna Engineering suggests deletion of references to an FMEA in this paragraph using the same rationale as given in response to 17.c(3).			<p>Adopted.</p> <p>The current text in this paragraph is very similar to the part 25 AC; however, a minor change was made.</p>
Cessna	17.d	How does this section relate to conventional mechanical and electromechanical systems that have had 23.1309 applied to them when it was never intended that 23.1309 should apply to them?			<p>Adopted.</p> <p>See Cessna 5a disposition for more information.</p>
Cessna	18.a(5)(a)	Is a zonal safety analysis what the FAA means by a “design or installation appraisal”?			<p>Not adopted.</p> <p>The word “standard” is used not “appraisal”. These terms are also used in the part 25 AC and defined in this AC.</p> <p>This AC is not depended on the ARPs and the ARPs are not required for compliance to</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
					23.1309.
Cessna	19.d	Cessna Engineering understands the concern about probability values; however, Cessna Engineering suggests that the AC also reference the use of an FTA analysis as a way of showing compliance to 23.1309.			<p>Adopted.</p> <p>Paragraph 19b states that “A probability analysis may be either an FMEA or an FTA, which also includes numerical probability information.”</p> <p>Even when using a tool or cut-sets, the basis data should come from proven data or operational experience and tests.</p>
Cessna	19.e	Cessna Engineering believes that this paragraph does not apply if the probability numbers are listed in the rule. If the probability requirement is in the rule, the applicant will need to explain why a conventional mechanical system that has been in place for 20 years now no longer complies with the hard requirement published in the rule. The two			<p>Adopted.</p> <p>Also, in the proposed rule, Appendix K and 23.1309 (b) (4), (b) (5), (c), (d), and (e) are deleted or the final rule. They will only appear in the text, Figure 2, and Figure 3 of the AC.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		paths will be to redesign the system or work the issue with an ELOS.			
Cessna	21.a	As Cessna Engineering understands it, the FAA now requires all "airborne electronic hardware" including "simple" devices that can be tested to use DO-254 to some extent (via FAA order 8110.105 which apparently supersedes AC20-152); therefore this guidance is outdated and should be updated to include a reference to the order and a note that it supersedes the AC. Discussion of the formal activities now required for "simple" devices should be considered for addition here			Adopted. Order 8110.105 was added. AC 20-152 explains to applicants that if they follow RTCA/DO-254, they'll demonstrate compliance to regulations and gain FAA approval for complex custom micro-coded components of airborne systems and equipment. The AC also recognizes RTCA/DO-254 as a way to demonstrate compliance to regulations for simple custom micro-coded components except for the levels.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Cessna	21.e	If there may be significant difference in the guidance provided, then why publish the requirement in the rule? That forces the applicant to follow the ELOS path for a system that may have been certified under 23.1309 adm. 41 using AC 23.1309-1C, which would not comply with the new 14CFR Appendix K.			Adopted. In the proposed rule o Appendix K and 23.1309 (b) (4), (b) (5), (c), (d), and (e) are deleted or the final rule. They will only appear in the text, Figure 2, and Figure 3 of the AC.
Cessna	24	The additional appendices to this Draft AC are missing. Cessna Engineering believes these are needed so the review can be complete.			Sorry, there was a mix up when the AC was sent out for comments. It should have included the Appendices. However, the appendices in AC 23.1309-1D are very similar. The only changes were only reference data such as pages, AC 23.1309-1E instead of AC 23.1309-1D.
Garmin	4.b	States in part: AC 21-16 RTCA, Inc. Document RTCA/DO-160F, Environmental Conditions and Test Procedures for	Suggest referencing “DO-160X” or “DO-160[]”.		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p style="text-align: right;">Airborne</p> <p>Equipment</p> <p>Since the RTCA/DO-160 version changes so often, it would be better to keep the references generic or not reference a specific revision.</p>			
Garmin	4.b	<p>Should add a reference to:</p> <p style="text-align: center;">AC 20-155 SAE Documents to Support Aircraft Lightning Protection Certification</p>	Add reference.		<p>Not Adopted.</p> <p>It was not intended to provide all the documents for lightning. AC 20-136 and AC 23-17 are the main documents for protection of EMI for electronic displays and they reference the other appropriate documents.</p>
Garmin	4.c(2)	<p>Should add references to:</p> <p style="text-align: center;">ARP 5412A Aircraft Lightning Environment and and Related Test Waveforms</p> <p style="text-align: center;">ARP 5414A Aircraft Lightning Zoning</p>	Add references.		<p>Not Adopted.</p> <p>It was not intended to provide all the documents for lightning. AC 20-136 and AC 23-17 are the main documents for protection of EMI for electronic displays and they reference the other appropriate documents.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	5.c	<p>States in part:</p> <p>c. ... This section should be used to determine software and hardware development assurance levels. ...</p> <p>It is unclear whether the term “hardware” is referring to all hardware, complex electronic hardware, custom micro coded devices, etc.</p>	Clarify the use of the term “hardware” to be consistent with AC 20-152.		Adopted.
Garmin	6.a(6)	<p>States in part:</p> <p>(6) ... This means of compliance identifies four classes of airplanes and applies appropriate probability values and development assurance levels for each class shown in Appendix K. ...</p> <p>Garmin strongly disagrees with codifying the means of compliance in § 23 Appendix K.</p>	The § 23 Appendix K guidance should remain in AC 23.1309, but be removed from proposed Part 23.1309.		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>NPRM § 23.1309 and Appendix K proposes to codify of the long established means of compliance used for § 23.1309. As submitted with the § 23 NPRM, Garmin is strongly opposed to codifying the means of compliance as development assurance is one means but not the only means of compliance for software and complex hardware to meet the rule. Furthermore, codifying the means of compliance significantly detracts from the ease of change allowed by leaving the means of compliance in AC 23.1309.</p>			
Garmin	6.b.(1)(b)	<p>States in part:</p> <p>(b) ... without the establishment of the four-tier certification classes of airplanes as shown in paragraph 15. ...</p> <p>Uses the term “paragraph” but the</p>	The AC should be consistent throughout in its internal references to paragraphs/sections.		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		Table of Contents uses the term “Section”.			
Garmin	7.	<p>Includes the acronym:</p> <p style="text-align: center;">DAL Development Assurance Level</p> <p>This definition of DAL is inconsistent with the AC 23.1309-1E 8.1 definition of “Design assurance level”.</p> <p>Additionally, DO-178B, which is referenced many times within this AC, uses the term “Software Level” but does not include the term “Development Assurance Level”. DO-254, which is referenced many times within this AC, uses the term “Design Assurance Level” instead of the term “Development Assurance Level”. At this point in time, there is not universal agreement on the use of the term</p>	At the very least, revise the AC 23.1309-1E 8.1 definition to be “Development Assurance Level” to be consistent.		<p>Not Adopted.</p> <p>Paragraph 7 is for acronyms, not a definition.</p> <p>Additional resolution will be in Garmin comment 8.1.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>“Development Assurance Level”.</p> <p>See also comments on 8.l and 8.m.</p>			
Garmin	8.g	<p>States in part:</p> <p>g. Complex. A system is “complex” when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured assessment methods. ...</p> <p>The word “complex” is defined in terms of a “complex system”. But there are multiple phrases throughout the document that use the word “complex” including “complex design”, “complex airplane”, “complex hardware”, etc.</p>	<p>The definition should be changed to “Complex System” to make it clear that it is only referring to the word “complex” in terms of a “complex system”. This is particularly important as there are instances where the word “complex” is used in the same paragraph as a reference to RTCA/DO-254, which has a much different definition of “complex”.</p> <p>Each use of the word “complex” should be examined in the rest of the document to</p>		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<p>determine whether additional definitions are warranted or adjustments should be made to the sentence structure to make it clear when the “Complex System” definition should be applied versus another definition.</p>		
Garmin	8.i	<p>States in part:</p> <p>i. Conventional. A system is considered “conventional” if its function, the technological means to implement its function, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly used. ...</p> <p>The word “conventional” is defined in terms of a “conventional system”. But there</p>	<p>The definition should be changed to “Conventional System” to make it clear that it is only referring to the word “conventional” in terms of a “conventional system”.</p> <p>Each use of the word “conventional” should be examined in the rest of the document to determine whether additional definitions</p>		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>are multiple phrases throughout the document that use the word “conventional” including “conventional technology”, “conventional installation”, etc.</p>	<p>are warranted or adjustments should be made to the sentence structure to make it clear when the “Conventional System” definition should be applied versus another definition.</p>		
Garmin	8.i	<p>States in part:</p> <p style="padding-left: 40px;">i. ... Normally conventional and simple systems may be analyzed by qualitative assessments and usually do not contain software or complex hardware that require compliance by detailed processes. ...</p> <p>Garmin disagrees that a simple and conventional system cannot have software or complex hardware. The implication of making this statement is that essentially all avionics assessed</p>	<p>Remove the phrase “and usually do not contain software or complex hardware that require compliance by detailed processes.”</p>		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>as having a Major failure classification will require quantitative analysis for § 23.1309 compliance even if the non-SW/CEH aspects of the system are simple and possibly even redundant. The SW and CEH aspects are covered by the development assurance requirements of DO-178B and DO-254, respectively. There is no reason to require quantitative analysis of an otherwise simple and possibly redundant system just because it has SW/CEH when the SW/CEH aspects aren't considered in the quantitative analysis anyway. If the system is non-traditional or complex in itself then quantitative analysis should be required but the inclusion of SW or a CEH device shouldn't be the limiting factor.</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	8.1	<p>States:</p> <p>1. Design assurance level. All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the items (hardware, software) satisfy the applicable certification basis. This term may be used in some SAE and RTCA documents, but in this AC it is intended that design assurance levels will correlate to the same levels as the DALs for the safety assessment process. See section 21 for more information. Design assurance level.</p> <p>DO-178B, which is referenced many times within this AC, uses</p>	<p>Revise the AC 23.1309-1E 8.1 definition to be “Development Assurance Level” to be consistent with the section 7 definition of “DAL” and Figure 2 and revise the use of “design” to “development” as appropriate within the definition.</p> <p>Additionally, acknowledge the “Software Level” and “Design Assurance Level” terms used in the DO-178B and DO-254 guidance as being “equivalent” to the intent of this definition.</p> <p>Finally, make the definition consistent with the NPRM</p>		<p>Partially Adopted.</p> <p>No changed required since the AC has adequate clarification. Appendix K is removed from the rule.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>the term “Software Level” but does not include the term “Development Assurance Level”. DO-254, which is referenced many times within this AC, uses the term “Design Assurance Level” instead of the term “Development Assurance Level”. At this point in time, there is not universal agreement on the use of the term “Development Assurance Level”. Currently, draft SAE ARP 4754A intends to use the term “item Development Assurance Level” or (iDAL).</p> <p>This inconsistency is an excellent reason not to codify AC 23.1309-1E Figure 2 as NPRM 23 Appendix K as in the future it will be much easier to modify the AC when there is a universally agreed definition.</p>	<p>preamble b.vii text (changes from preamble are <i>emphasized</i>):</p> <p>1. Development assurance level. All planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.</p> <p><i>Note: For this AC, development assurance levels in Figure 2 and throughout this AC are intended to correlate to software levels in</i></p>		

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
			RTCA/DO-178B and complex hardware design assurance levels in RTCA/DO-254 for the system or item. <i>See section 21 for more information.</i>		
Garmin	8.m	<p>States in part:</p> <p>m. DAL. All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.</p> <p>What benefit is provided by this definition being separate from the section 8.1 definition?</p>	Suggest removing the 8.m definition in favor of the suggested 8.1 definition in the preceding comment and allowing the section 7 “DAL” acronym definition to be the bridge between these terms.		<p>Not adopted.</p> <p>The definition of design assurance level and development assurance levels are similar, but not exactly the same. The AC provides adequate clarification.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	8.ii	<p>States in part:</p> <p>ii. ... An example for brake control system, the electronic brake system is normally used most of the time because of its better performance, but it does not comply with the all the requirements. In this case, the mechanical brakes are used as the backup systems; yet, it is consider the primary with regard to meeting the requirements and the electronic brake system is the secondary.</p> <p>These sentences are poorly worded.</p>	<p>Clarify the example sentences.</p> <p>Delete the word “the” from the phrase “with the all”.</p>		Adopted.
Garmin	8.rr	<p>States:</p> <p>rr. Simple. Usually a conventional system that can be evaluated by only qualitative analysis and it</p>	<p>The definition should be changed to “Simple System” to make it clear that it is only referring to the word “simple” in terms of a</p>		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>is not complex. Functional performance is determined by combination of tests and analyses. See the definitions for “conventional” and “complex” for more information.</p> <p>The word “simple” is defined in terms of a “conventional system”. But there are multiple phrases throughout the document that use the word “simple” including “simple qualitative installation evaluation”.</p>	<p>“simple system”. This is particularly important as there are instances where the word “simple” is used in the same paragraph as a reference to RTCA/DO-254, which has a much different definition of “simple”.</p> <p>Each use of the word “simple” should be examined in the rest of the document to determine whether additional definitions are warranted or adjustments should be made to the sentence structure to make it clear when the “Simple System” definition should be applied versus another definition.</p>		

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	9.	<p>States in part:</p> <p>... (See Note below) ...</p> <p>Is this referring to the Note that is now at the beginning of paragraph 10? If so, then there should be a better reference than “below” used to make the connection since the expectation is that the “Note below” is included in paragraph 9.</p>	<p>Improve reference to Note.</p>		<p>Adopted.</p>
Garmin	9.	<p>States in part:</p> <p>... With the certification basis at Amendment 23-14, systems that meet the single-fault concept should comply with the requirements of § 23.1309(a) if the guidance in the next section of this AC is used.</p> <p>...</p> <p>Is the term “single-fault concept” common knowledge? Should</p>	<p>Clarify the term “single-fault concept”.</p> <p>Additionally, replace the phrase “next section of this AC” with the specific section reference within AC 23.1309-1E.</p> <p>Clarify what other guidance should be used if the applicant chooses not to use “the</p>		<p>Partially Adopted.</p> <p>Single failure concept is defined. Change the word “fault” to “failure.”</p> <p>Regarding environmental conditions, the guidance you requested is in section 12.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>there be an expansion of the concept to clarify the intent of this guidance?</p> <p>To what section is the phrase “guidance in the next section of this AC” referring? Section 10? If so, Section 10 did not exist in AC 23.1309-1D, so should it be section 11? It would be better to have a specific section reference.</p> <p>Additionally, why is the word “if” used in the phrase “if the guidance in the next section”? What other guidance should be used if the applicant chooses <u>not</u> to use “the guidance in the next section of this AC”?</p> <p>Additionally, this section implies that the no single fault concept must be in combination with environmental conditions. Garmin does not believe this is warranted.</p>	<p>guidance in the next section of this AC”.</p> <p>If the single fault concept is tied to 23.1309(a) then it should be clearly stated that it is not intended to imply that a single fault criteria applies to systems under environmental conditions.</p>		

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	9.	States in part: ... In accordance with AC 21.101.1, ...	Change “21.101.1” to “21.101-1”.		Adopted.
Garmin	10.	States in part: ... All references to regulatory sections in this AC refer to § 23.1309, as amended by Amendment 23-49. ... The phrase that all references “in this AC refer to ... Amendment 23-49” since the NPRM proposes a new amendment and draft AC 23.1309-1E section 12 references “Amendment 23-XX” and this note also references “Amendment 23-XX”.	Correct the statement.		Partially Adopted. Clarification was made.
Garmin	10	Figure 1 contains 2 decisions in the flowchart that use the phrase “Adverse Effect”. AC23.1309-1E paragraph 8.a defines Adverse Effect as: “A response of a system that results in an	Clarify the definition of Adverse Effect.		Not Adopted. No additional clarification is needed. We had no other request in the past years for additional clarification.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		undesirable operation of an airplane system, or subsystem”; however, this definition is vague and may not be applied consistently. For example, is an Adverse Effect something that leads to a Catastrophic, Hazardous, or Major failure condition by itself? Or in combination with other probable failures?			
Garmin	10	Figure 1 contains a decision in the flowchart labeled “Will Any Probable Failure or Malfunction Result in a Hazard?” A Minor hazard could result in a Yes answer to the decision but a Minor hazard can be acceptable for multi-engine aircraft. For multi-engine aircraft, the question should be “Will Any Probable Failure or Malfunction Result in a Major or Higher Hazard?”	Adjust the flowchart to account for the Minor hazards being acceptable for multi-engine aircraft.		Not Adopted. Please see the definition of “hazard.” Figure 1 is not applicable for the safety assessment process for failure conditions.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	12.a	<p>States in part:</p> <p>(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the airplane operating and environmental conditions, including radio frequency energy and the effects (both direct and indirect) of lightning strikes.</p> <p>Garmin has also commented on the NPRM § 23.1309 change.</p> <p>Garmin agrees with the intent of the change as described in the preamble of the NPRM. However, the proposed wording is problematic. NPRM § 23.1309 (a)(1) and draft AC 23.1309-1E 12.a “(1)” requires that those systems and equipment “required for type certification or by operating rules” must “perform as</p>	<p>Delete the phrase “or whose improper functioning would reduce safety,” as § 23.1309 (b) deals with how to handle the effects of malfunctions.</p> <p>Delete the phrase “including radio frequency energy” (since this is addressed via Special Conditions and § 23.1308) and replace “the effects (both direct and indirect) of lightning strikes” with “the effects (both direct and indirect) of lightning strikes for systems with major, hazardous or catastrophic failure condition(s).”</p>		<p>Adopted.</p> <p>The paragraphs were changed to relate to the changes made to the rule.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>intended ..." Garmin agrees with this requirement. However, the inclusion of the phrase "or systems whose improper function could reduce safety" will be challenging to comply with under some circumstances.</p> <p>Garmin believes the intent is that if the airplane requires systems and equipment functionality to be safe, then it must function as intended. However, consider a non-essential system whose functionality is not required to safely operate the airplane, e.g. a coffee maker. If the coffee maker is not functioning and there is no coffee, there really is no issue. However, since the coffee maker may be designed with high watt heaters, it is conceivable that there may be failure conditions related to the coffee maker overheating that could reduce the safety of the airplane. The wording of NPRM § 23.1309 (a)(1) and draft AC 23.1309-1E</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>12.a “(1)” could be interpreted to mean that the coffee maker must function as intended (i.e. make coffee) throughout the entire “airplane operating and environmental conditions ...”, which is obviously not required.</p> <p>The normal operation of non-required systems should not interfere with the proper operation of any required, essential or critical systems or present a hazard in itself. Non-required systems are not required to perform their intended function throughout the aircraft operating and environmental conditions but in situations where the non-required system is not functional due to exposure to a particular operating or environmental condition, there can be no safety effect to the aircraft or its occupants or any adverse effect on required, essential or critical equipment and systems.</p> <p>Malfunctioning and erroneous</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>behavior of all systems including non-required should be addressed under § 23.1309 (b). Garmin would have no problem complying with this.</p> <p>Additionally, the phrase “including radio frequency energy and the effects (both direct and indirect) of lightning strikes” is problematic because there is no requirement to test functions with a minor failure condition under HIRF (§ 23.1308 & AC 20-158) and Indirect Effects of lightning (AC 20-136A). The phrase “including radio frequency energy and the effects (both direct and indirect) of lightning strikes” suggests otherwise.</p>			
Garmin	12.a	<p>States in part:</p> <p>(2) Those required for type certification or by operating rules and other equipment and systems do not adversely affect the</p>	<p>Evaluate § 23.1309 (a)(2) and AC 23.1309-1E 12.a “(2)” and adjust as necessary.</p>		<p>Adopted.</p> <p>The paragraphs were changed to relate to the changes made to the rule.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>safety of the airplane or its occupants, or the proper functioning of those covered by paragraph (a)(1) of this section.</p> <p>Garmin has also commented on the NPRM § 23.1309 change.</p> <p>It appears that there is a missing word in the phrase “Those required for type certification ...” Should the phrase be “Those <u>not</u> required for type certification ...”?</p>			
Garmin	12.a	<p>States in part:</p> <p>(2) Those required for type certification or by operating rules and other equipment and systems do not adversely affect the safety of the airplane or its occupants, or the proper functioning of those covered by paragraph (a)(1) of this section.</p>	<p>Evaluate § 23.1309 (a)(2) and AC 23.1309-1E 12.a “(2)” and adjust as necessary.</p>		<p>Adopted.</p> <p>The paragraphs were changed to relate to the changes made to the rule.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>Garmin has also commented on the NPRM § 23.1309 change.</p> <p>It appears that there is a missing word in the phrase “Those required for type certification ...” Should the phrase be “Those <u>not</u> required for type certification ...”?</p>			
Garmin	12.b	<p>States in part:</p> <p>Section 23.1309(a)(2) requires the applicant to show that all non required equipment and systems (including approved “amenities,” such as a coffee pot and entertainment systems) have no safety effect on the operation of the airplane.</p> <p>Garmin assumes that this guidance refers to the loss of function of a non-required</p>	Clarify the AC 23.1309-1E 12.b guidance.		

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>system. NPRM § 23.1309 (b) will address all failure conditions including loss of function and malfunction. However, the coffee pot used in this example could conceivably have a high watt heater with an unprotected overheat failure that could be more severe than no safety effect. The guidance as written could imply that these systems either:</p> <p>(a) don't have failure conditions associated with them that are more severe than NSE (although in reality, depending on the design, the failure conditions could be more severe than NSE) or</p> <p>(b) that non-required systems that have malfunction cases that are more severe than NSE cannot be compliant with NPRM § 23.1309 (a)(2) even if the failure condition meets the acceptable probability requirements for NPRM § 23.1309 (b).</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>What should matter under NPRM § 23.1309 (a) is that those equipment and systems required by rule or that are essential or critical to the airplane safe operation must operate under all of the airplanes operating and environmental conditions. And the expected operation of non-required equipment and systems throughout the aircraft operating and environmental conditions is that they can not introduce an unsafe condition by themselves or adversely affect the proper operation of any required, essential or critical equipment or systems.</p>			
Garmin	12.b	<p>States in part:</p> <p>b. ... to show that all non required equipment ...</p>	Change “non required” to “non-required”.		Not Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	12.c	<p>States in part:</p> <p>c. ... This section is for the applicant to take two actions. ...</p>	Suggest changing this to “This section describes two actions for the applicant.”		Adopted.
Garmin	12.c	<p>States in part:</p> <p>c. ... This section is for the applicant to take two actions. ...</p> <p>Is it correct to assume that the two actions are NPRM § 23.1309 (a)(1) and (a)(2). If the two actions are the “First ...” and “Second ...” described within 12.c, then this should be rephrased as the reader could make the same assumption, because, after all, this is in a section that is discussing NPRM § 23.1309 (a)(1) and (a)(2).</p>	Clarify the intent of the phrase “two actions”		<p>Not Adopted.</p> <p>There is adequate clarification for the two actions.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	12.c	<p>States in part:</p> <p>c. ... Second, the applicant must consider the anticipated external and internal airplane environmental conditions, as well as any additional conditions where equipment and systems are assumed to “perform as intended.” ...</p> <p>Regarding the phrase “as well as any additional conditions”: additional to what? The proposed regulation says nothing about <u>anticipated</u> external and internal airplane environmental conditions. The intent of NPRM § 23.1309 (a)(2) appears to be to insure that the equipment and systems are designed and installed such that they do not adversely affect the safety of the airplane or its occupants under airplane operating and environmental conditions. As</p>	Clarify the intent of AC 23.1309-1E 12.c ensuring consistency with the intent of NPRM § 23.1309 (a)(2)		<p>Not Adopted.</p> <p>The heading sentence states section § 23.1309 (a) not § 23.1309 (a)(2).</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>presently written, the quoted text from draft AC 23.1309-1E 12.c seems to imply the intent of NPRM § 23.1309 (a)(2) was to “stress test” the equipment with respect to operating and environment, which is not consistent.</p>			
Garmin	12.c	<p>States in part:</p> <p>c. ... In response to the observation that although certain operating conditions are foreseeable, achieving normal performance when they exist is not always possible (e.g., you may foresee ash clouds from volcanic eruptions, but airplanes with current technology cannot safely fly in such clouds).</p> <p>Why does this sentence include the phrase “In response to the observation that although certain</p>	Clarify the intent of AC 23.1309-1E 12.c ensuring consistency with the intent of NPRM § 23.1309 (a)		<p>Adopted.</p> <p>Clarification was made.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		operating conditions are foreseeable”? How does this sentence relate to the other guidance in this paragraph?			
Garmin	12.d	<p>States:</p> <p>d. We accept equipment that is susceptible to failures if these failures do not contribute significantly to the existing risks (e.g., some degradation in functionality and capability is routinely allowed during some environmental qualifications, such as HIRF and lightning testing). System lightning protection specifically allows the functionality and capabilities of some electrical/electronic systems to be lost when the airplane is exposed to lightning, provided that</p>	<p>Delete the NPRM § 23.1309 (a)(1) phrase “including radio frequency energy” (since this is addressed via Special Conditions and § 23.1308) and replace the NPRM § 23.1309 (a)(1) phrase “the effects (both direct and indirect) of lightning strikes” with “the effects (both direct and indirect) of lightning strikes for systems with major, hazardous or catastrophic failure condition(s).”</p> <p>See also following comment suggesting revisions to 12.d.</p>		<p>Adopted.</p> <p>The AC and rule were revised.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>“these functions can be recovered in a timely manner.”</p> <p>Garmin concurs with the intent of AC 23.1309-1E 12.d but reiterates its concern that its guidance alleviates the NPRM § 23.1309 (a)(1) rule. In past experience, alleviation of a rule by an AC can be problematic as the rule is what must be met. The NPRM § 23.1309 (a)(1) rule implies that all systems and equipment must operate under HIRF and Lightning conditions. Draft AC 23.1309-1E 12.d says it may be ok to have degraded systems as long as the function remains, etc. It is not clear how it is possible to follow the draft AC guidance and still meet the NPRM § 23.1309 (a)(1) rule.</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	12.d	<p>States in part:</p> <p>d. ... System lightning protection specifically allows the functionality and capabilities of some electrical/electronic systems to be lost when the airplane is exposed to lightning, provided that “these functions can be recovered in a timely manner.”</p> <p>Garmin suggests the following clarifying text in lieu of the quoted draft 12.d text:</p> <p>d. ... System cable bundle lightning testing, designed to evaluate functional upset during a lightning strike, specifically allows the functionality and capabilities of some electrical/electronic systems to be lost when</p>	Revise the paragraph as suggested.		<p>Partially Adopted.</p> <p>Reference was made to “See AC 20-158 and AC 20-136 for more guidance.”</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>the airplane is exposed to lightning, provided that “these functions can be recovered in a timely manner.” Given the short duration of the lightning strike, momentary upsets may be tolerated if the automatic recovery time is of a duration that does not lead to an adverse effect for systems with major, hazardous or catastrophic failure condition(s). It also allows permanent loss of functions at higher test levels associated with higher certification levels (as defined by AC 20-158 and AC 20-136A) than what is required. As an example, a system may have certain functions classified as having major failure conditions (AC 20-158 and AC 20-136A Certification Level C) while other functions are</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>classified as having catastrophic failure conditions (AC 20-158 and AC 20-136A Certification Level A). In this case, when the system is tested to test levels associated with catastrophic failure conditions it is acceptable to for the test to result in a permanent loss of a function that has a major failure condition but it is not acceptable for the test to result in a catastrophic failure condition. However, no major or catastrophic failure conditions are acceptable when the system is tested to test levels associated with major failure conditions.</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	12.e	<p>States in part:</p> <p>e. ... these types of non required equipment ...</p>	Change “non required” to “non-required”.		Not Adopted.
Garmin	13.b	<p>States in part:</p> <p>b. The FAA will typically conduct some level of function and reliability testing during certification to ensure required functions demonstrate an acceptable level of reliability. ...</p> <p>This sentence uses the term “reliability” twice but it is not clear how reliability is measured. As defined in SAE ARP4754, reliability is a probability but it is not possible to actually test for reliability.</p>	Replace “reliability” with another term that is consistent with the intent of the paragraph or define how “reliability” will be measured.		<p>Adopted.</p> <p>A revision was made to the AC and rule.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	13.b	<p>States in part:</p> <p>The FAA expects the applicant to show that the system does not exhibit unintended or undesirable functionality for required flight critical functions that have failure conditions that are major, hazardous, or catastrophic.</p> <p>The use of the term “flight critical functions” is inconsistent with major and hazardous failure conditions.</p>	Change “flight critical functions” to “flight functions”.		<p>Partially Adopted.</p> <p>This paragraph was revised.</p>
Garmin	Figure 2	<p>Includes multiple instances of the term:</p> <p>Development Assurance Levels</p>	Ensure the term “Development Assurance Levels” is consistent with whatever modifications are made to the AC 23.1309-1E 7 definition of “DAL”, and the 8.1 and 8.m definitions of “Design		<p>Adopted.</p> <p>Only a minor change was made.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
			assurance level” and “DAL”, respectively.		
Garmin	Figure 2	<p>“←Hazardous→” column includes multiple instances of the phrase:</p> <p>Notes 4</p>	Change “Notes” to “Note” in each of these instances.		Adopted.
Garmin	Figure 2	<p>Note 4 states:</p> <p>Note 4. Secondary System (S) may not be required to meet probability goals. If installed, S must meet stated criteria.</p> <p>The first and second sentences of Note 4 are contradictory. The first sentence uses the verb “may not be” while the second sentence uses the verb “must”. Previously, the second sentence used the verb “should”.</p>	Restore the second sentence to the previous text by using the verb “should”.		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	17.	States: 1. Failure conditions.	Insert blank line before this text to be consistent with the formatting in the rest of the AC.		Not Adopted. The FAA did not see a need for correction.
Garmin	18.a(5)(b)	States in part: (b) Particular risk analysis. ...	Insert blank line before this text to be consistent with the formatting in the rest of the AC.		Not Adopted. The FAA did not see a need for correction.
Garmin	21.e	States in part: e. Where apparent differences exist between these two documents on this subject, ... It is not clear which “two documents” are being referred to in this context.	Revise the phrase “these two documents” to specify the two documents.		Adopted.
Garmin	22.a	States in part: a. ... The committee is planning new concepts for (DAL)and Design Assurance Levels. ...	Ensure the term “Design Assurance Levels” is consistent with whatever modifications are made to the AC		Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<p>23.1309-1E 7 definition of “DAL”, and the 8.1 and 8.m definitions of “Design assurance level” and “DAL”, respectively.</p> <p>Also, insert a space between “(DAL)” and “and”.</p>		
Garmin	23.b	<p>States in part:</p> <p>b. Section § 23.1309(f) specifics ...</p>	<p>Remove “§” symbol to be consistent with other references in the rest of the AC.</p> <p>Change “specifics” to “specifies”.</p>		Adopted.
Garmin	23.b	<p>States in part:</p> <p>b. ... Unless they are accepted as part of normal aviation abilities, ...</p> <p>The phrase “normal aviation abilities” does not seem to convey the intent of this sentence.</p>	<p>Suggest changing the phrase “normal aviation abilities” to “normal aviation operational conventions” or “conventional aviation procedures”.</p>		<p>Not Adopted.</p> <p>This term has been used without any problems.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Garmin	24	<p>The title of this section is:</p> <p style="text-align: center;">24. Electromagnetic protection for electrical/electronic systems.</p> <p>However, this section only deals with external electromagnetic environment and not the internal electromagnetic environment as required by § 23.1431(b).</p>	<p>Change the section title to:</p> <p>24. Certification and protection of electrical/electronic systems from external electromagnetic environment.</p>		<p>Not Adopted.</p> <p>We added AC 21-16 for internal electromagnetic environment.</p>
Garmin	Appendix 1	<p>Table contains the Aircraft Function:</p> <p style="text-align: center;">Weather displays for situation awareness</p> <p>The FAA and SAD, in particular, have been vocal in recent years about “situation awareness” not being an intended function. Consequently, it is ironic to see the use of that term within this AC when describing an “Aircraft Function”. One could choose different words such as “Weather</p>	<p>Since FAA and SAD find the term “situation awareness” useful, it would be good of them to acknowledge its usefulness and allow industry to use it as well.</p> <p>Otherwise, the “Weather displays for situation awareness” Aircraft Function should be revised to</p>		<p>Not Adopted.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		displays for portraying weather information in relation to the aircraft position for the purpose of the pilot making advanced decisions about weather avoidance”, but “situation awareness” is a much more concise term which is understood in this context.	describe the intended function without using the term “situation awareness”.		
Embraer	Paragraphs l and m, Pages 9 and 10	There is a definition of Design Assurance Level and one for DAL. Do you intend to have both?			Not Adopted. Yes, we need both definitions. No change necessary.
Embraer	Paragraph q, Page 10	Some of the listed events are not independent of the airplane. We suggest that you remove fire, leaking fluids, tire burst, uncontained failure of high energy rotating machine from the definition.			Not Adopted. Not intended to be independent.
Embraer	Paragraph 8ii, Page 13	The definition of “primary” is unclear in the use of the word “requirements” in the sentence about the PFD, because in a typical installation, a single	As a suggested alternative, the PFD example would be more easily understood if the		Adopted. Clarification was made.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>electronic PFD cannot meet all the design requirements (specifically availability and malfunction (misleading indication)) without some form of standby indications.</p> <p>Concerning the brake example, we do not understand the separate mechanical and electronic systems nor which requirements are applicable to which of the different systems.</p> <p>In summary, we think the existing definition is sufficient to help the reader understand how to apply Figure 2.</p>	<p>following was added either to definition of “primary” or that of “secondary:”</p> <p>A standby PFD that is intended to be used in the event of failure of the PFD is an example of a secondary system.</p> <p>A reference to Figure 2 and Paragraph 21.e would aid the reader to understand the significance of the definitions of primary and secondary.</p>		
Embraer	Paragraph 13, page 19	<p>In our comments to the NPRM for Amendment 23-XX, we stated that we do not believe that § 23.1309(a)(3) was necessary and that it may have some unintended effects. That comment notwithstanding, the guidance provided in the draft AC is generally good.</p> <p>Similar to our NPRM comment, we do object to the fourth sentence of subparagraph (b)</p>			<p>Adopted.</p> <p>Clarification was made to the AC and rule.</p>

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>(“The FAA expects that the applicant show . . .”) because it would require all design errors be removed from the applicable systems even though many design errors have no safety effect, or the effect can be easily and safely mitigated through operational or maintenance procedures. This is unnecessarily restrictive and this sentence appears to conflict with the fifth sentence of the paragraph where design errors, for example, are acceptable if their occurrence rate is compatible with their safety effect. We suggest removing the fourth sentence.</p>			
Embraer	Paragraph 21 (e), page 34	<p>The draft AC changes the second sentence of this paragraph to say "The FAA recognizes that consideration of system architecture for this purpose is appropriate in some cases." System architecture is always relevant to the design of a software or complex hardware item with regard to a particular failure condition. Evaluation of</p>			Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>the architecture may or may not indicate that the appropriate levels for a particular item are lower than the level associated to the failure condition hazard class. We think the intent would be better stated as "The FAA recognizes that consideration of system architecture for the purpose of determining DALs is appropriate and may lead to lower levels in some cases".</p>			
Embraer	Paragraph 21 (e), page 34	<p>This section should use different terms to distinguish between lowered required levels, such as those allowed for class I, II and III airplanes, and those situations where analysis indicates that a particular item does not need to meet the DAL associated to the top level failure condition due to architectural considerations. In the first case there is effectively a reduced DAL, where in the second case the DAL for the top level failure condition is actually met. Even though a</p>			Not Adopted.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>particular item within the system has a lower DAL, the architecture is such that the system as a whole meets the top level DAL.</p> <p>Proposed language: refer to modified DAL requirements of Class I, II and III aircraft as "reduced DALs". Refer to DAL assignments to specific items as "item DALs" - which may or may not differ from the top level failure condition DAL depending on system architecture.</p>			
Embraer	Paragraph 13a, Page 19	<p>It is not necessary to conduct tests for validation in all cases. This would be more clearly conveyed if the second sentence was written as "The applicant should conduct bench, ground and/or flight testing when necessary to validate hazard classifications, acceptability of crew procedures, human factors, and other assumptions made during the safety analysis processes."</p>			Adopted the minor changes.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
Embraer	Paragraph 15, Page 24	Subparagraph "15.i" should be "15.h"			Adopted.
Embraer	Paragraph 8, Page 13	To maintain the alphabetical order, the definitions of Probable and Probable Failure Conditions should go behind the definition of Primary System.			Adopted.
Cirrus	Figure 2	Software Level An allowable reduction in software level for Class I and Class II aircraft for COM/NAV/surveillance systems was removed from Figure 2 in Draft AC 23.1309-1E. This removal is not addressed in the change documentation. Cirrus recommends that this reduction remain as it appeared in AC 23.1309-1D for Class I and Class II aircraft. The reduction in software level has allowed for simplified and reduced certification effort while retaining a suitable level of safety for these			Not Adopted. Note 5 states: "A reduction of DALs applies only for navigation, communication, and surveillance systems if an altitude encoding altimeter transponder is installed and it provides the appropriate mitigations." During the safety assessment process, if the transponder provides the appropriate mitigation to reduce the level, then it is appropriate to reduce the level (e.g., Level C to Level D) even without the note. The problem was some applicants

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		products.			were using the note when there was no mitigation.
Cirrus	15 and Figure 2	Airplane Certification Class Section 15 and Figure 2 provide a breakdown for classes of airplane that defines Class II as "...under 6000#". This is inconsistent with the remainder of Part 23, which delineates as "6000 lb or less" and "greater than 6000 lb." It is recommended that Section 15 and Figure 2 be adjusted to be consistent with other Part 23 weight delineations.			Adopted.
Michael E. Bailey		This AC is great news for all part 23 Manufacturers and operators. It is critical to safety the FHA safety process, and safety testing and probability for the four classes of Part 23 aircraft. It also provides a high degree of flexibility in how each class of aircraft in the Part 23 group can be fitted out with the safety equipment appropriate and			Thank You.

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		<p>needed by each class. That makes all aircraft in the Part 23 group allot safer and also controls the cost of equipment needed. So a GA pilot with a small single engine plane can afford to buy it with automated safety features installed appropriate to that type of plane whereas a multiple turbo engine commuter plane would need a lot more and more advanced safety equipment. In this way pilots are able to buy planes with the automated safety cockpit equipment they need to safely operate the plane instead of having a one size fits all approach that could result in only partial installation of important equipment or not installing it because of cost. This flexibility has resulted in Part 23 group plane accidents being cut significantly; and this maybe one of the most important things recognized by this AC. I do need to fly from time to time and safety is a very important</p>			

Commenter	Page & Paragraph	Comment	Reason for Comment	Suggested Change	Comment Resolution
		concern. This AC helps a lot. It should be implemented. Thank you,			