Certification Authorities for Large Transport Aircraft (CATA)

CATA Worklist Item TCCA-001 – HIRF Testing

Date Raised:	Sept. 28/2016	Updated: 24 October 2019	Status:	**Closed**
Subject:	**HIRF Testing**			
Related Issue(s): (Identify Discussion Paper number, if any)	GAMA17-03 Industry Recommendation – Report dated January 10, 2017			

Description of Issue(s):

(Give a brief background of issue(s)

Type validations of transport category airplanes have revealed inconsistencies in the application of the harmonized HIRF rule and associated advisory material. Similar findings are anticipated to persist unless remediated by amending the associated guidance.

Background:

State-of-the-art electrical and electronic systems installed in modern transport category airplanes may exhibit performance degradation when exposed to high intensity radiated fields (HIRF).

The HIRF rule was introduced to prescribe minimum immunity requirements for installed electrical and electronic systems when the airplane is exposed high levels of radiated energy. These minimum requirements are commensurate with a system's functional criticality - higher immunity requirements as the criticality increases. Hence, the HIRF rule prescribes distinct environments corresponding to each hazard classification (Catastrophic, Hazardous, and Major).

Particular to those electrical and electronic systems performing functions whose failure would prevent the continued safe flight and landing, referred to as critical airplane functions by advisory material, the HIRF rule prescribes two "HIRF certification environments" that must be complied with; namely when the airplane is exposed to HIRF Environment I and HIRF Environment II; noting that Environment I is more severe than Environment II.

More specifically, the HIRF Rule [condition 1] assures the availability of critical airplane functions during and after the airplane is exposed to HIRF Environment I; it however allows for some acceptable level of system performance degradation provided that the critical airplane functions are recoverable. The HIRF rule [condition 2] also assures that each electrical and electronic system demonstrates satisfactory performance of the critical airplane functions during and after the airplane is exposed to HIRF Environment II. Note that these statements are simplifications of the HIRF rule to illustrate the challenges facing applicants and certification authorities.

The subjectivity in the application of the HIRF rule resides primarily in the identification of those «critical airplane functions» and the «electrical and electronic systems» performing or contributing to those critical airplane functions for which compliance to conditions 1 and 2 is required. The applicant and certification authority must also reach agreement on the degree of performance degradation that is considered acceptable to meet the intent of the HIRF rule.

On a modern transport category airplane for example, a critical airplane function would normally be assured by an architecture that may comprise multiple redundant electrical and/or electronic systems, or paths. Per condition 1, at least one of the redundant path of the multi-system architecture must continue to perform that critical airplane function during and after the airplane is exposed to HIRF Environment I, the other paths however must recover normal performance of that critical airplane function after exposure. Per condition (2), all redundant paths of the multi-system architecture must demonstrate satisfactory performance of that critical airplane function during and after the airplane is exposed to HIRF Environment II. It is emphasized that both conditions must be met and that all redundant paths of the multi-system

architecture must be exposed to HIRF Environment I and II in order to reveal and remedy any adverse vulnerabilities. It is noted that condition 2 can be satisfied by demonstrating no adverse performance degradation in all redundant paths during and after the airplane is exposed to Environment I under condition 1. The above example reflects the approach applied by Transport Canada for certification of Canadian products.

Type validations conducted by Transport Canada have shown that applicants, in agreement with their certification authority, have only applied condition 1 to only one of the redundant paths of the multi-system architecture. Predictably, applicants are motivated by the considerable time and cost savings, and risk reduction realized by minimizing the number of airplane electrical and electronic systems subject to the HIRF rule.

There are two recent examples identified during independent validations where this interpretation was used:

1) The third set of instruments (referred to as standby) required by the type designs were not qualified to the same HIRF level A requirements as were the primary instruments even though all these instruments perform or contribute to the same critical aircraft level functions; and
2) The alternate electrical power source (provided by a ram air turbine or RAT) required by the type design was qualified to the HIRF Level A requirements whereas the normal electrical power sources (derived for the main engine generators) were qualified to HIRF Level B even though all three sources perform or contribute to the same critical aircraft level function.

Transport Canada has brought these findings to the attention of the certification authority using the «concern paper» process. In response to these concern papers, the certification authority supported Transport Canada's interpretation and proceeded with awareness campaigns aimed at certification specialists and design organizations accordingly.

Transport Canada further notes that guidance is currently found in FAA (AC 20-158A) and EASA (Int/Pol/25/2, AC/AMJ20.1317) published material as well as SAE (ARP 5583A) published practices. The industry as a whole would greatly benefit from consolidated, harmonized and updated HIRF guidance material that reflects the current experience acquired over the years and acceptable practices.

Proposed Prioritization:

(Per CATA Technical Issues List Prioritization schema, SME proposes along with authority CATA members)

Question	Answer
1. Is there an active working group related to this issue?	Yes, SAE WG AE-4
2. In which documents are there deviations amongst the authorities?	Deviations are in interpretations of the guidance documents.
3. Was this issue raised by or at the CMT?	No.
4. What is the level of impact on projects in the future (i.e. minor, major, critical)?	Major; historical issues with HIRF validations have taken up significant time and effort.
5. How many authorities does the issue impact?	Issue impacts all 4 authorities
6. What is the approximate technical complexity of the issue (i.e. low, medium, high)?	Medium complexity.

Recommendation:

(SME proposes expected resolution of the issue)

A working group made up of cognisant certification specialists from each CMT Member State and Agency be convened to discuss their respective experience in applying the HIRF rule, reaffirm the intent and interpretation of the HIRF rule, review existing guidance (FAA AC 20-158A, EASA AMC 20-158, and SAE ARP-5583A) and formulate a strategy for its revision and/or consolidation, and make recommendations to the CMT.

Certification Authorities for Large Transport Aircraft (CATA)

CATA Worklist Item TCCA-001 – HIRF Testing

CATA Decision:
(Using CATA criteria for determination of technical issues)

CATA decision to action this issue. Authorities' SMEs consensus that topic deserved CATA attention.

Final CATA Position:
(Explain agreement, dissent or conclusion on this IP)

CATA accept the SME team recommended guidance provided in sections 6 ("Findings") and 7 ("Application of Findings") of the final report developed by the SME working group.
These sections are appended directly to this CWI form. The CWI form, including the appended guidance, document a CMT member authority agreement that member authorities may reference when they are acting as the certificating authority (CA). Following CA endorsement for a particular project, the other CMT member authorities, when acting as validating authority, will accept the approach. This CWI is closed.

The complete report, and the recommended revisions to AC-20-158A, will be retained by the CATA for internal authority reference and future consideration outside of the CATA charter-mandated transport airplane scope.

Release of CWI:

CATA Representative	Name	Signature	Date
ANAC	Marcelo Leite	/s/	04.11.2019
	Daniel Pessoa	/s/	01.11.2019
EASA	Colin Hancock	/s/	30.10.2019
	Mathilde Labatut	/s/	30.10.2019
FAA	Tom Groves	/s/	24.10.2019
TCCA	Canh Nham	/s/	25.10.2019

1. Findings

The task group clarified the following key terms in the regulations.

a. Failure: Failure includes damage, malfunction, and misleading information. When addressing compliance with § 25.1317(a), the applicant must address systems that perform functions whose failure would prevent continued safe flight and landing. Section 25.1317(a) does not specifically address combination of unrelated failures. Therefore, the applicant is not required to assume a combination of failures when performing the HIRF safety assessment. Section 25.1317(a) refers to failures and does not refer to failures specifically attributed to HIRF. Failures due to HIRF observed in service and during HIRF tests show that it is unlikely that the applicant can predict the type of failure caused by HIRF exposure.

b. Normal Operation: When addressing compliance with § 25.1317(a)(2), the level A function should be in the same undisturbed state that is was before exposure to the HIRF Threat.

As part of the discussions related to the §25.1317(a)(2) and definition of "Normal Operation", the Task Group reviewed the applicable parts of the §25.1317 Preamble, concluding that the presented Task Group Finding and proposed revision of AC 20-158 definition for "Normal Operation" are consistent with the rule, including its Preamble.

c. Electrical or Electronic System: When addressing § 25.1317, an electrical or electronic system includes all electrical and electronic equipment, components and electrical interconnections that are required to perform a particular function. When showing compliance with § 25.1317(a), the electrical and electronic system is that required to perform the function whose failure would prevent continued safe flight and landing. This electrical and electronic system must also automatically recover normal operation in a timely manner to comply with § 25.1317(a)(2). As noted above, the electrical and electronic system includes, as a minimum, all equipment, components and electrical interconnections required for normal operation. The system defined for § 25.1317(a) is not required to include equipment, components and electrical interconnections required only for non-normal situations, provided all equipment, components and electrical interconnections required for normal operation are not susceptible when it complies with paragraph (a), or equipment required only when operating as defined by minimum equipment lists and time-limited dispatch operations. In this case, the elements or channels of the system which were not included under the scope of 25.1317(a), must comply with 25.1317(b), since failures on these elements or channels should be considered to "significantly reduce the capability of the airplane or the ability of the flight crew to respond to an adverse operating condition."

Note: Non-normal situation is any event, condition, or situation that requires non-normal, abnormal, emergency, unusual procedures or configurations for operating an aircraft.

d. Adverse Effect: A response of a system that results in an unexpected and unacceptable operation of an aircraft system, or unexpected and unacceptable operation of the function performed by the system.

This finding is applicable to adverse effect of the function, mentioned in §25.1317(a)(1), and to adverse effect of the system, mentioned in §25.1317(a)(3), (b) and (c).

When showing compliance with §25.1317(a), both aspects of adverse effect – related to the function and the system, should be evaluated. The §25.1317(a)(1), which is related to adverse effect of the function, requires an aircraft level evaluation of the function. Compliance with §25.1317(a)(1) may allow a momentary upset of a certain system performing the function, provided the function is properly maintained by other systems and the affected system recovers normal operation, in compliance with 25.1317(a)(2).

The concept of adverse effect of the system for compliance with 25.1317(a)(3) is restricted to the system under consideration, that shouldn't be affected. Therefore, the pass/fail criteria are normally more stringent, since no credit from other systems performing the function is allowed. This is consistent with the rule, that requires a more severe HIRF environment for §25.1317(a)(1) and (a)(2) – HIRF Environment I - than what is required for §25.1317(a)(3) – HIRF Environment II.

e. "Unless its recovery conflicts with other operational or functional requirements of the system": This exception for recovery must be based on aircraft operational or functional requirements. Aircraft operational or functional requirements used for this exception are independent of HIRF exposure. That is, aircraft operational or functional requirements should not be based on mitigating adverse effects observed during or after HIRF exposure. This exception is rarely applicable. The electrical and electronic system lightning protection regulations in §§ 25.1316 and 29.1316 do not include this exception. The NPRM for these regulations comments that FAA was "… unable to identify a situation where such an exception would be appropriate, nor could we justify the need for such an exception and propose requirements that could ensure an equivalent level of safety." The CATA HIRF team was also unable to identify a situation where such an exception would be appropriate.

f. Required HIRF Certification Level for Protection Systems: The HIRF Safety Assessment for Protection Systems (e.g. cargo fire protection system, engine fire protection system) must consider the combination of the associated event with the HIRF environment, since these systems must be protected against HIRF to ensure availability and proper operation when required for protection.

If the probability of occurrence of the event is remote or lower, the required HIRF Certification Level of the Protection System can be one level below the criticality of the resulting combination. For example, a non-annunciated failure of the cargo fire protection system in combination of cargo fire is classified as Catastrophic in the System Safety Assessment. If the probability of cargo fire is remote or lower, considering this specific failure condition, it is acceptable to define a HIRF Certification Level B to the fire protection system. If the probability of fire is higher than remote, a HIRF Certification Level A would be required.

The other failure conditions of the system, not combined with occurrence of the event (e.g. false detection), must also be considered in the HIRF Safety Assessment, according to the respective associated criticality.

g. Integrated System Tests for Level A Systems: The requirements in § 25.1317(a) address adverse effects to the airplane function and the system performing the function. The guidance in AC 20-158A describes integrated system tests as an acceptable means of demonstrating no adverse effects to the system and function. If the Level A System consists of multiple similar channels, the integrated system test can use one or more channels in the laboratory test setup for the integrated system, instead of all channels. This integrated system laboratory test setup must adequately perform the functions to demonstrate compliance with § 25.1317(a). The laboratory test setup should represent and monitor any cross-channel interactions, such as cross-channel data links, redundancy management, and system health monitoring. Note that similar channels are composed of equipment having the same hardware but not necessarily the same part numbers. If pin programming and/or software are used to identify or configure equipment of similar channels, the differences between channels and the impact on the functions performed should be assessed.

2. Application of Findings

The task group members agreed that establishing appropriate pass-fail criteria for complying with § 25.1316(a) and .1317(a) could only be achieved through a comprehensive review of the system design using an acceptable HIRF and Lightning functional hazard assessment process. The task group explored approaches whereby pass-fail criteria for compliance with § 25.1316(a) and .1317(a) could be specified on the merit of specific system architecture attributes. The following paragraphs summarize those discussions.

For discussion and evaluation purposes, the task group made certain assumptions and developed generic attributes for architectural strategies that implement functions whose failure may contribute or cause a condition which would prevent continued safe flight and landing. Systems are typically categorized with the following architectures:

(1) Similar Redundant Channels:

The multiple channels consist of equipment, components, electrical interconnections and configurations that are similar, typically with equipment that have identical part numbers. The channels should be independent. They may be configured in an active, active-backup and passive-backup modes.

(2) Dissimilar Redundant Channels:

Each channel is unique and independent of the others. They may be configured in an active, active-backup and passive-backup modes.

(3) Combination of Similar and Dissimilar Redundant Channels:

The combination of similar and dissimilar channels as defined above with independence between channels. They may be configured in active, active-backup and passive-backup modes.

Notes:

1) Active mode means the channel is performing the aircraft function.

2) Active-backup mode means the channel is operational but not used to perform the aircraft function until switched to active mode either automatically or by pilot action.

3) Passive-backup mode means the channel is not operational; switching to active mode is either automatic or by pilot action upon failure recognition.

(4) Combination of Electrical/Electronic and Mechanical, Hydraulic and/or Pneumatic Channels:

Certain architectures combine electrical and electronic channels with mechanical, hydraulic and/or pneumatic channels. These combinations of electrical/electronic and mechanical, hydraulic or pneumatic channels may be configured in active, active-backup and passive-backup modes.

Note that these examples are theoretical and intended to facilitate the discussion from which universal guidelines may be derived to help develop useful guidance material. It is not the intention to account for all possible configurations but only represent the most common system architectures or those that present unique challenges.

From these attributes and preceding discussions, the task group derived the following universal guidelines for establishing the appropriate pass-fail criteria for complying with § 25.1317(a) relative to the system architectural strategy proposed by an applicant.
Assumptions:

- The applicant performs a comprehensive and iterative HIRF safety assessment process involving Systems and the HIRF subject matter experts. The HIRF safety assessment must have input and be coordinated with safety specialists, system specialists, and HIRF specialists. This process may vary from applicant to applicant.

- The HIRF safety assessment must include all electrical and electronic equipment and components, assuming that they are potentially affected by HIRF. It is not appropriate to use the HIRF immunity data for electrical and electronic equipment or components as an input information on the HIRF Safety Assessment. This information should be used only in the next phase, to show compliance with the applicable §25.1317 sub-part, after the required HIRF Certification Level for the system is defined by the HIRF Safety Assessment.

- The applicant identifies the redundant channels (similar, dissimilar, active or passive) implemented in their system design using the above definitions.

- Compliance with § 25.1317 does not consider or assume pre-existing failure conditions.

Minimum conditions for complying with § 25.1317; Annex 1 uses examples to illustrate the concept:

I. All electrical and electronic system channels that perform functions whose failure would prevent continued safe flight and landing, and can operate in “Active” mode during normal operation, should fully comply with § 25.1317(a),

II. Channels that operate only in non-normal situations and are dissimilar should comply with § 25.1317(b) and

III. Aircraft functions performed by independent mechanical, hydraulic and/or pneumatic channel(s) are not subject to §25.1317. The HIRF aircraft safety assessment should consider electrical or electronic failures that would adversely affect the function of the mechanical, hydraulic and/or pneumatic channel(s). If electrical or electronic equipment, components and electrical connections are used to assist, augment, or monitor the mechanical, hydraulic and/or pneumatic channel(s) to perform functions with failures that would prevent continued safe flight and landing during normal operation, then the electrical and electronic channel(s) must comply with §25.1317(a). The HIRF aircraft safety assessment should also verify the assumptions for mechanical, hydraulic and/or pneumatic channel(s) reliability and availability, if these assumptions would affect whether the electrical/electronic or mechanical channel is the active channel during

normal operation. For example, if a mechanical channel has foreseeable latent failures, then the electrical/electronic channel would be the active channel during normal operations.

Annex 1: llustrates examples of aircraft systems with multiple independent and redundant channels performing a function whose failure would prevent continued safe flight and landing.

Annex 1
Examples of HIRF Safety Assessment considerations - Level A Systems

Example 1			
Function	**System**		**System**
	Channel	**Channel**	**Channel**
Display of Attitude, Altitude, and Airspeed Information to the Pilots During IFR Operations (e.g. Primary Display System and Associated Sensors, with Dissimilar Standby Display System and Sensors)	Active (Pilot Displays and Associated Sensors)	Active (Co-pilot Displays and Associated Sensors)	Active-Backup (Dissimilar Standby Display and Associated Sensors)
Applicable Parts of § 25.1317	(a)(1), (2), (3)	(a)(1), (2), (3)	(b)

Discussion:

This example depicts the requirement of § 25.1333 for independent displays of information essential to the safety of flight at each pilot station. The standby display is required in order to achieve the safety objectives of § 25.1309. Either the pilot or co-pilot can be the pilot flying or pilot monitoring during normal operations, so both the pilot or co-pilot display system should be considered the active system.

Compliance with § 25.1317(a)(1), (a)(2), and (a)(3) should demonstrate that each pilot display of aircraft attitude, altitude, and airspeed is not adversely affected and recovers normal operation when the aircraft is exposed to HIRF environments I and II. The dissimilar standby display should comply with § 25.1317(b). Adverse effects must include both loss of, and hazardous misleading, attitude, altitude, and airspeed information.

Example 2			
Function	**System**		
	Channel	**Channel**	**Channel**
Full Authority Control of Pitch, Yaw, and Roll Using Electrical and Electronic Flight Control Systems	Active or Active-Backup (Flight Control System #1)	Active or Active-Backup (Flight Control System #2)	Active or Active-Backup (Flight Control System #3)
Applicable Parts of § 25.1317	(a)(1), (2), (3)	(a)(1), (2), (3)	(a)(1), (2), (3)
Discussion: This example depicts an electronic flight control system comprising three independent channels to meet the safety objectives of § 25.1309. At any time, any one of the three channels can operate as the active channel. Only one channel operates in an active mode while others are in active-backup mode. Any channel can perform the control function at any one time, therefore all channels must comply § 25.1317(a)(1), (a)(2), and (a)(3).			

Example 3			
Function	**System**		
	Channel	**Channel**	**Channel**
Provide Engine Over-Speed Protection	Active (Electronic Engine Control System) (Normal Speed Control)	Active or Active-Backup (Electronic Engine Control System) (Over-speed Protection)	Active (Independent Mechanical Over-Speed Protection)
Applicable Parts of § 25.1317	(b)	(b)	Not subject to § 25.1317

Discussion:

This example depicts the function of engine over-speed protection performed by a combination of active electrical and electronic control and mechanical system control. The mechanical channel must provide over-speed protection during normal operations, and be independent of the active electronic control channels. The mechanical channel must not rely on electrical or electronic components to assist, augment, or monitor the over-speed protection. If the mechanical channel is independent of the electronic engine control speed control and over-speed protection, and has no electrical or electronic components, then the engine over-speed protection function is not adversely affected when the aircraft is exposed to HIRF environments I and II. The system therefore is not subject to 25.1317(a). The electronic engine control channels should comply with § 25.1317(b).

This example only considers the over-speed protection feature implemented by the system. Other functions whose failure may be classified as catastrophic, like the loss of thrust control where the function may be implemented by electronic control channels, should comply with § 25.1317(a).

*Note: This example assumes that the mechanical overspeed protection system has adequate reliability, integrity, and availability. If the mechanical system has failures that are not detected before the next normal flight, the active electronic engine control system may need to be classified with a higher criticality.

Example 4			
Function	**System**		**System**
	Channel	**Channel**	**Channel**
Provide Electrical Power for Electrical and Electronic Systems Including Those with Catastrophic Failure Conditions	Active (Left Engine Generator System)	Active (Right Engine Generator System)	Passive-Backup (Emergency Power Supply System driven by Ram Air Turbine)
Applicable Parts of § 25.1317	(a)(1), (2), (3)	(a)(1), (2), (3)	(b)

Discussion:

This example depicts a typical transport category aircraft electrical system on a two-engine aircraft where two or more independent sources of electrical power are required by § 25.1307(b) and a ram air turbine is necessary to meet the safety objectives requirements of § 25.1309 and § 25.1351(d).

For this example, the electrical system consists of two active channels provided by a single main engine driven generator on each engine with the associated distribution and controls, and a third passive-backup channel provided by a ram air turbine electrical power system. The ram air turbine electrical power system is stowed during normal operation and deployed either automatically and/or manually when power from the two main engine driven generators is lost.

The active engine generator system channels must not be adversely affected when the aircraft is exposed to HIRF environments I and II, and comply with § 25.1317(a)(1), (2), and (3). The passive-backup ram air turbine electrical power system does not mitigate adverse effects for compliance with § 25.1317(a). The ram air turbine electrical power system must comply with § 25.1317(b).

Example 5				
Function	**System**			**System**
	Channel	**Channel**	**Channel**	**Channel**
Provide Electrical Power for Electrical and Electronic Systems Including Those with Catastrophic Failure Conditions	Active (Left Engine Generator System)	Active (Right Engine Generator System)	Active (APU Driven Generator System required for ETOPS flight beyond 180')	Passive-Backup (Emergency Power Supply Driven by Ram Air Turbine)
Applicable Parts of § 25.1317	(a)(1), (2), (3)	(a)(1), (2), (3)	(a)(1), (2), (3)	(b)

Discussion:

This example depicts a two-engine transport category airplane electrical system where two or more independent sources of electrical power are required by § 25.1307(b) and an alternate source (driven by ram air turbine) is necessary to meet the safety objectives of § 25.1309 and § 25.1351(d). This configuration includes a third electrical power source driven by an auxiliary power unit (APU). This third source is required (Active channel) for ETOPS beyond 180 minutes. As in example 4, the emergency power source is a passive-backup channel provided by a ram air turbine that remains stowed during normal flight and deployed either automatically and/or manually when power from all other channels is lost.

All active electrical power generation channels should comply with § 25.1317(a)(1), (a)(2), and (a)(3). The passive-backup electrical power generation channel does not mitigate adverse effects due to HIRF exposure to meet the intent of the HIRF rule. The passive backup channel must be evaluated to the pass/fail criteria of 25.1317(b).

Note: For non-ETOPS or ETOPS until 180 minutes aircraft, the APU HIRF Certification Level should be defined based on specific aircraft safety assessment.

Example 6				
Function	**System**	**System**	**System**	**System**
	Channel	**Channel**	**Channel**	**Channel**

Example 6				
Function	**System**	**System**	**System**	**System**
	Channel	**Channel**	**Channel**	**Channel**
Reduce Aircraft Speed on Ground in a Controlled Manner Using Thrust Reverser Control System, Spoiler Deployment System, Wheel Braking System	Active Main Brake System (Electro-Mechanical)	Active (Electronic Engine Thrust Reverse Control with associated sensors)	Active (Electronic Spoiler Deployment Control with associated sensors)	Active (Independent Mechanical Wheel Braking)
Applicable Parts of § 25.1317	25.1317(a)(1)(2)(3)	Based on specific aircraft safety assessment	Based on specific aircraft safety assessment	Not subject to § 25.1317

Discussion:

This example depicts an aircraft level function that is performed by a combination of independent systems each contributing to the function in part during a specific phase of flight. In this case, each system implements a very distinct aircraft level function that serve in a complementary manner to decelerate the aircraft during the landing roll. The mechanical wheel braking system is assumed to be independent of the other channels, with no associated electrical or electronic equipment to assist, augment, or monitor the mechanical wheel braking system.

In this example, it is assumed that the main brake system includes failures conditions that are catastrophic. For the electronic engine thrust reverser control and the electronic spoiler control systems, the applicable parts of § 25.1317 would depend on the specific failure conditions. The effectiveness, authority, and malfunctions associated with each system should be considered. Additionally, the interaction between the systems has also to be considered. Issues such as unsymmetrical thrust reverser activation or spoiler deployment could adversely affect the main brake and mechanical wheel braking functions, and could affect the safety classification for the thrust reverser and spoiler controls.

An aircraft safety assessment must be carried out for each of these systems performing a specific aircraft level function to identify and classify their failure conditions. The failure hazard classifications and the decomposition of each system into the constituent channels would then dictate which paragraphs of § 25.1317 are needed.

Example 7			
Function	**System**		**System**
	Channel	**Channel**	**Channel**

Example 7			
Function	**System**		**System**
	Channel	**Channel**	**Channel**
Provide Altitude Information to Display in IFR Using Air Data Computer Connected to PFD, and Pneumatic Standby Instrument with Alternate Static Port	Active (Air Data Computer 1 with Static Port)	Active (Air Data Computer 2 with Static Port)	Active-Backup (Pneumatic Standby Altimeter with Alternate Static Port)
Applicable Parts of § 25.1317	(a)(1), (2), (3)	(a)(1), (2), (3)	Not subject to § 25.1317

Discussion:

This example depicts the function to provide altitude information. The main sources are obtained from two ADCs coupled to static ports and a backup source from a standby pneumatic altimeter coupled to an alternate static port independent from the main static ports.

In such a case, the standby altimeter does not mitigate compliance with § 25.1317(a) for the active air data computer channels. The standby altimeter does not mitigate the common hazardously misleading altitude information from the active air data computer channels for compliance with § 25.1317(a).

Example 8			
Function	**System**		
	Channel	**Channel**	**Channel**
Control and protection of the aircraft Pneumatic (Bleed) System (Top-level failure condition classification: Catastrophic)	Active (Pneumatic System Controller #1) FDAL B	Active (Pneumatic System Controller #2) FDAL B	Passive Back-up (High Pressure switch + Valve) FDAL C
Applicable Parts of § 25.1317	(a)(1), (2), (3)	(a)(1), (2), (3)	(b)

Discussion:

This is a generic example with the objective to show that not rarely the HIRF Certification Level (HCL) of a given system will be different from the Functional Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL), defined according to SAE ARP4754A "Guidelines for Development of Civil Aircraft and Systems".

Therefore, it is important to use the proper nomenclature and avoid ARP 4754A "DAL" or similar terms when referring to the HIRF Certification Level (HCL).

In this example, the Pneumatic Control System is composed by two main Active controllers and a simpler Passive Back-up channel that can perform the function, preventing the catastrophic event in case of the failure of both controllers.

The FDAL for each Channel or Member (ARP4754A nomenclature) was defined for a Catastrophic top-level failure condition based on the "Option 2" column of the Table 3 "DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT TO MEMBERS OF A FUNCTIONAL FAILURE SET" of ARP4754A, which allows the combination of FDAL B+B+C for independent channels. In contrast, the respective HIRF Cert. Levels would be A+A+B.

Considering that HIRF can simultaneously affect all channels, the considerations used for FDAL assignment cannot be used and compliance with §25.1317(a) is required for both Active channels performing a function with the catastrophic top-level failure condition.

The FDAL for the passive back-up channel may be C, in this example. However, for HIRF, the applicable part of §25.1317 is (b), similarly to Example 5.