



U.S. Department  
of Transportation

**Federal Aviation  
Administration**

# Memorandum

Subject: INFORMATION: Identification of Flight Critical System  
Components

Date: DRAFT

From: Manager, Transport Airplane Directorate, Aircraft  
Certification Service, ANM-100

Reply to  
Attn. of: ANM-03-117-10

To: SEE DISTRIBUTION LIST

Regulatory § 25.1309, AC 25.1309-  
Reference: 1A

## Summary

As directed by the Safer Skies initiative, this memorandum sets forth the Federal Aviation Administration (FAA) Transport Airplane Directorate (TAD) policy on defining flight critical system components for use in existing design and certification guidance, and developing guidance for continuing airworthiness and maintenance processes.

The policy contained herein is limited only to establishing a set of criteria for standardizing the identification of system components that could cause an adverse effect on safety using the Aviation Rulemaking Advisory Committee (ARAC)- recommended FAA/JAA harmonized § 25.1309. At this time, this policy is to be applicable only to new designs (TC and STC). This policy memorandum is not intended to establish the criteria or processes for managing the safety risks that may be associated with the identified airplane components. Those risk management criteria and processes are expected to be defined by future implementation of other Safer Skies and Commercial Airplane Certification Process Study (CPS) findings, and they will be addressed in additional policy statements, advisory circulars, or rulemaking actions, as appropriate, at a later date.

## Current Regulatory and Advisory Material

1. Section 25.1309 of 14 Code of Federal Regulations (CFR) Part 25.
2. Advisory Circular (AC) 25.1309-1A
3. Society of Automobile Engineers (SAE) Aerospace Recommended Practice ARP4754, Certification Considerations for Highly-Integrated or Complex Aircraft System, issued 1996-11.
4. Society of Automotive Engineers Aerospace Recommended Practice APRP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, issued 1996-12.
5. Radio Technical Commission for Aeronautics (RTCA) DO-254, Design Assurance Guidance for Airborne Electronic Hardware, issued April 19, 2000.

6. Radio Technical Commission for Aeronautics DO-178B, Software Considerations in Airborne Systems and Equipment Certification, issued December 1, 1992.

## **Background and Scope**

Under the auspices of the Safer Skies and the CPS initiatives (particularly CPS Findings 2, 3, and 4), this memorandum puts into practice one of the Commercial Aviation Safety Team (CAST) safety enhancement recommendations titled “Approach and Landing Accident Reduction (ALAR) – Implementation Plan for Aircraft Design.” This memorandum addresses the specific recommendation that states “*Utilize the definition developed by the ARAC 25.1309 working group to identify flight critical system components as the basis for design guidance, continuing airworthiness, and maintenance.*” Although the ARAC recommendations do not explicitly contain a definition of “flight critical system component,” the information contained in the recommendations can readily be used to identify the said components.

The criteria for identifying flight critical system components, as contained in this memorandum, are applicable to *all* aircraft systems and associated non-structural components, including the interfaces with structural components, and items consumed by the systems, such as lubrication, fuel, and hydraulic fluid. While this memorandum is based on § 25.1309 principles, other regulations (such as §§ 25.671, 25.901, 25.933) may have specific (or more restrictive) procedures to identify flight critical system components. In those cases, those specific procedures will take precedence.

Although the ALAR recommendations apply to parts 23 and 25 aircraft, this memorandum addresses only the latter. Appendix 1 contains relevant excerpts from the ALAR recommendations. Appendix 2 provides a brief background of the Safer Skies, CPS, and the harmonized FAR/JAR 25.1309 rulemaking activities, as well as the rationale behind the policy below.

## **Definition of Terms**

For the purpose of this policy:

1. A “component” is any software or equipment that would normally be part-number-controlled at the aircraft level. These part numbers are typically shown on the system or airplane-level installation drawings. It should be noted that some equipment could have modification or revision levels that may not be tracked by operators in their maintenance activities. In this case, their failure effects, as shown in the policy below, will determine whether that equipment is critical, regardless of modification or revision levels.
2. A “failure” means failure to function as intended, i.e., a loss of function or a malfunction. Failures of sub-components, safety features, or consumable items associated with a part-number-controlled component are considered within the context of the higher-level component failure effect.

3. The failures to be considered are based on the most severe airplane-level effect that cannot be reasonably ruled out by knowledgeable persons.

## **Policy**

A component is critical when it has one or more of the following attributes:

1. Its single failure results in a hazardous or catastrophic failure condition. (See Appendix 2 for a list of harmonized § 25.1309 hazard categories. The “hazardous” classification has been added and will be used throughout this document. The term “severe major” has often been used to connote the same classification.) Although the design and certification processes normally strive to eliminate single failures that could result in catastrophic events, this policy is intended to also cover the continued airworthiness process where *potentially* catastrophic single failures may be discovered. Common cause or cascading failures are considered single failures. When specific regulations allow exceptions for potentially catastrophic single failures, such as uncontained engine failures and flight control jams, those regulations shall take precedence over this memorandum.
2. When a combination of 2 failures results in a hazardous failure condition, or a combination of 3 failures results in a catastrophic failure condition, every component in the combination is a flight critical system component regardless of their individual hazard classification. There may be cases where a combination of 4 (or more) failures warrants additional review and validation. See discussion in Appendix 2.
3. All components contributing to a significant latent failure condition are considered flight critical system components.

## **Applications to Current Safety Assessment and Continued Operations Safety Processes**

The primary purpose of this memorandum is to provide criteria for determining flight critical system components for new designs (TC and STC). As indicated earlier, upcoming implementation of other Safer Skies and CPS findings (see discussions in the appendices) may result in new policies and guidance for design, certification, continued airworthiness, maintenance, and training activities. Until then, the applicants, the cognizant Aviation Safety Engineer (ASE), and Aviation Safety Inspector (ASI) should use the above policy statements to:

1. Compile a list of flight critical system components for each airplane model in the existing fleet as well as for new designs. Once a flight critical system component is identified, its design, and/or maintenance procedures may need to be reviewed to ensure the level of safety required by the regulations. The list should be modified as needed for STC and derivative changes.

System safety assessment data plays a central role in compiling this list. While newer products are expected to have these data, the TAD recognizes that these data may not be available on some older products. In the interests of continued operational safety, these data should be generated, as practicable, at the time changes are made to the products. See also

item 4 below.

2. Ensure that the safety assessment assumptions associated with the flight critical system components are validated with respect to environmental conditions, operational conditions, modification, repair, and maintenance activities. For example, if a Certification Maintenance Requirement is proposed to detect a significant latent failure, then it should be verified that the maintenance procedure contains specific tests that indeed detect and resolve the latent failure in question within the assumed exposure time. Other examples may be found in the CPS report, in the Finding 2 discussion.

Where it is not possible to fully justify the safety assessment assumptions, and where data or assumptions are critical to the acceptability of the failure conditions associated with the flight critical system components, or when a safety assessment result is sensitive to the assumptions, extra conservatism should be built into either the analyses or the design of the components. A high severity event should not be dismissed solely on the basis of low probability. Independence and other assumptions used in the safety and risk assessments should be scrutinized.

Single failures resulting in only Major, or less severe, effects are not included in the above policy statements. However, such failures and their underlying assumptions should be validated to confirm they are indeed no worse than Major. Testing (flight, ground, laboratory, or simulator) at critical points, and under flight-realistic conditions should be included in the validation process.

3. Flight testing per AC 25-7A normally applies to Major or less severe failure conditions, hence the policy herein does not affect the AC (hazardous failure conditions are normally extrapolated from less severe test conditions.) As discussed in Appendix 1, CAST has recommended that AC 25-7A be reviewed and, if necessary, it may be revised. For hazardous failure conditions, laboratory testing (including computer modeling and simulation) may be necessary to validate airplane, system, crew response, and environmental assumptions used in the safety assessment. Catastrophic failure conditions need not be tested.
4. When assessing continued operational safety, the ASE's are encouraged to review safety analyses (fault trees or other failure analyses) to identify the flight critical system components and then analyze fleet performance (trend analysis) of those components for factual evidence of potential unsafe conditions, and determine any necessary corrective actions. This should be done in conjunction with any continued airworthiness programs established between the Aircraft Certification Offices (ACO's) and the manufacturers. Reportable events may be defined using the identified flight critical system components.

The TAD recognizes that the current processes for data collection and trend analysis need to be improved. A joint FAA and Industry effort, known as CPS Change Area 1.B "COS Information," has been organized to study improvements in the data collection, management, and trend analysis process.

5. Some safety features that are not part-number-controlled at the aircraft level (such as bonding and grounding, wire separation requirement, consumables such as lubrication, etc.) may have significant impacts in determining if a component is critical when installed. These features should also be identified and communicated to the cognizant ASI's. The goal is to include any information that would assist Aircraft Evaluation Group (AEG) in ensuring that maintenance, alterations, modifications, or repairs do not violate the integrity of the type design approval. (Reference CPS Finding 4.)
6. Maintenance activities, alterations, modifications, and repairs should be reviewed with an explicit purpose of identifying any negative safety impact to flight critical system components. How to identify the flight critical system components to all maintenance, modification, repair personnel and communicate the safety assessment assumptions to them is a process that still needs to be developed in most instances. It is expected that implementation of the initiatives mentioned earlier will provide further facilitation and standardized guidance in this area. (Reference CPS Finding 4.)

### **Effect of Policy**

The general policy stated in this document does not constitute a new regulation or create what the courts refer to as a "binding norm." The office that implements policy should follow this policy when applicable to the specified project. Whenever an applicant's proposed method of compliance is outside this established policy, it must be coordinated with the policy issuing office, e.g., through the issue paper process or equivalent.

Applicants should expect that the certificating officials will consider this information when making findings of compliance relevant to new certificate actions, [or actions relating to maintenance, alterations, and repairs](#). Also, as with all advisory material, this policy statement identifies one means, but not the only means, of compliance.

Questions and comments regarding this policy should be directed to the Transport Standards Staff, Safety Management Branch, ANM-117, c/o Mr. Linh Le, email [linh.le@faa.gov](mailto:linh.le@faa.gov), phone 425-227-1105, fax 425-227-1100.

# APPENDIX 1

The information below is copied verbatim from the Safer Skies records. This information is only intended to provide the reader a general understanding of what will come later, following the application of this Policy Memorandum, as the Safer Skies and CPS initiatives are implemented.

## Excerpts from Safer Skies ALAR “Aircraft Design” Safety Enhancements

### Approach and Landing Accident Reduction Joint Safety Implementation Team

#### Implementation Plan For Aircraft Design

**Output 1:** *[Editor: Only this Output is addressed in this policy memorandum]*

- Utilize the definition developed by ARAC 25.1309 working group to identify flight critical system components as the basis for design guidance, continuing airworthiness, and maintenance.

**Output 2:**

- Issue design guidance to ensure flight critical system components are fault tolerant and are subjected to critical-point, flight-realistic-condition, certification testing/analysis.

**Actions:** Review AC’s 23.1309-1B (Equipment, Systems, and Installations in Part 23 Aircraft), 25.1309-1A (System Design and Analysis) and 25-7 (Flight Test Guide for Certification of Transport Category Airplanes) to insure these AC’s adequately address flight critical component fault tolerance, error tolerance, unintended functions, and hazard assessment to include critical point flight envelope testing (including computer modeling and simulation) and reliability requirements. Issue new guidance on the control of design changes to flight critical components (including STC/PMA).

**Output 3:**

- Issue guidance to 1) ensure continuing airworthiness processes adequately analyze fleet performance to verify that the original design level of safety remains unchanged and 2) ensure that safety risk management processes are applied to identify and prioritize safety critical threats/trends and mitigating corrective action.

**Actions:** Regulators will develop guidance on acceptable procedures to ensure that there is timely closure of all safety related reported events. Manufacturers will develop a process that ensures original reliability design assumptions are valid and a new safety issue has not occurred. The operators will

develop a process within their approved continuing airworthiness program that includes a method for reporting of all safety related events.

**Output 4:**

- Issue guidance on acceptable procedures to ensure maintenance activity involving flight critical system components does not reduce or compromise the designed level of safety and is in accordance with FAA approved data.

**Actions:** The FAA will 1) that maintenance activity involving flight critical system components does not reduce or compromise the designed level of safety, and 2) that maintenance activity is in accordance with FAA approved data. The bulletin will further provide that significant discrepancies noted during maintenance are reported in a timely manner.

## APPENDIX 2

### DISCUSSION & TUTORIAL

#### BRIEF DESCRIPTION OF RELEVANT SAFETY INITIATIVES

1. Safer Skies Initiative: The FAA implemented the Safer Skies initiative in 1998. This initiative seeks to understand the root causes of aviation accidents and incidents and to identify and apply intervention strategies. The ALAR Implementation Plan referred to in this memorandum is one of many intervention strategies developed by the initiative. In June 2002, the Commercial Aviation Safety Team (CAST) selected the FAA's Aircraft Certification Service as the lead organization to oversee and implement the ALAR Implementation Plan shown in Appendix 1. Only "output 1" of the ALAR Implementation Plan is addressed in this memorandum. Other outputs will be addressed in additional policy statements, advisory circulars, and rulemaking actions.
2. Commercial Airplane Certification Process Study: As a complement to the Safer Skies initiative and to address the role that processes have in accident prevention, the FAA chartered the Commercial Airplane Certification Process Study (CPS) team in January 2001. The team conducted a year-long comprehensive review of the processes and procedures associated with aircraft certification, operations, and maintenance, starting with the original type certification activities and extending through the continued operational safety and airworthiness processes intended to maintain the safety of the US commercial airplane fleet in service. The complete CPS report can be found at <http://www.aia-aerospace.org/issues/subject/subject.cfm>. Of the 15 Findings and 2 Observations, Finding 2, 3, and 4 are particularly pertinent in the development of this memorandum. Specifically, these Findings state:

*Finding 2: There is no reliable process to ensure that assumptions made in the safety assessments are valid with respect to operations and maintenance activities, and that operators are aware of these assumptions when developing their operations and maintenance procedures. In addition, certification standards may not reflect the actual operating environment.*

*Finding 3: A more robust approach to design and a process that challenges the assumptions made in the safety analysis of flight critical functions is necessary in situations where a few failures (2 or 3) could result in a catastrophic event.*

*Finding 4: Processes for identification of safety critical features of the airplane do not ensure that future alterations, maintenance, repairs, or changes to operational procedures can be made with cognizance of those safety features.*

3. Section 25.1309 Rulemaking Activities: After a multi-year review of the current rule and AC 25.1309-1A, in August 2002 the Aviation Rulemaking Advisory Committee (ARAC) submitted to the FAA their recommendations for an amended rule and revised advisory materials. One of the most significant rule change recommendations is to bring the "no catastrophic single failure" policy (currently in AC 25.1309-1A) into the rule language itself. With respect to the AC material, the

“Hazardous” classification has been added, and an improved safety analysis methodology is recommended that included guidance on justifications of assumptions, data sources and analytical techniques.

The following are relevant excerpts from the ARAC recommended AC/AMJ 25.1309:

Hazard categories:

1. No Safety Effect: Failure conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the airplane or increase crew workload.
2. Minor: Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
3. Major: Failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flightcrew, or physical distress to passengers or cabin crew, possibly including injuries.
4. Hazardous: Failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be:
  - a. A large reduction in safety margins or functional capabilities;
  - b. Physical distress or excessive workload such that the flightcrew cannot be relied upon to perform their tasks accurately or completely; or
  - c. Serious or fatal injury to a relatively small number of the occupants other than the flightcrew.
5. Catastrophic: Failure conditions which would result in multiple fatalities, usually with the loss of the airplane. (Note: A “Catastrophic” Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.)

**POLICY DERIVATION:**

According to the ALAR Implementation Plan shown in Appendix 1, Output 1 is the basis for accomplishing the intent of Output 2 (design guidance), Output 3 (continued airworthiness guidance) and Output 4 (maintenance guidance). It is necessary that the definition for “flight critical system component” be at a high enough level to serve the purposes of the latter three Outputs. Therefore, “components” are identified at the aircraft level where part-number control is required. Non-part-

number-controlled hardware and software that are contained in the higher-level equipment need not be considered for the purpose of Output 1. This delineation is consistent with the guidance of SAE ARP4754 “Certification Considerations for Highly-Integrated or Complex Aircraft Systems” which is referenced in the ARAC recommended AC/AMJ 25.1309.

Policy statements are based on § 25.1309 and its advisory materials. The safety assessment guidance contained in the existing AC 25.1309-1A and the ARAC proposed AC 25.1309-1B (not yet available for public comments as of this writing) are deemed sufficient to identify the flight critical system components in the design phase as well as in the continued airworthiness programs. Although AC 25.1309 does not explicitly include a definition for “flight critical system component,” in light of their process, intent, and purpose, the information contained in the AC readily supports the ALAR Outputs.

Policy 1 covers single failures that could result in catastrophic events although these failures are normally eliminated (or their risks minimized to an accepted level) in the design and certification process. This is because common software and hardware components, such as the core elements of an operating system, potentially have common mode design errors that could be catastrophic; therefore they must be considered “critical.” Another reason to include catastrophic single failure conditions in policy 1 is because continued airworthiness programs may discover single failures that could have catastrophic effects if corrective actions are not taken.

The policy intentionally leaves out the Major failure classification, although it is a level of safety specifically regulated by § 25.1309 that should not be reduced or compromised by the maintenance process. This is done to avoid superfluous designations of flight critical system component. Additionally, CPS Finding 1 discusses incidents/accidents involving failures that are only classified as Major or Minor. However, human errors are cited as the prevalent contributors in these cases. Human errors mitigation is a complex topic that is beyond the scope of this memorandum.

Commercial Airplane Certification Process Study Finding 3 provides another criterion for defining flight critical system components. The CPS report states: *“Finding 3 suggests that the failure analysis should be examined in much more depth when the consequences of a failure or combination of one, two, or three failures may be an immediate or unavoidable loss of the airplane. The underlying assumptions of the analysis must be examined to determine if the effect of an incorrect assumption is loss of the airplane. ...Every assumption should be examined to understand the sensitivity of the assumption on the result. Where such sensitivity does exist, then the design should be changed to reduce the sensitivity.”* It should be noted that this finding covers single failures as well as combinations, because in the course of examination of the failure combinations, the effects of single failures are inevitably evaluated in depth, and policy 1 may appear redundant. However, it is crucial to highlight the need to evaluate the risks of single failures.

Conversely, as a matter of policy, it is not always practical or necessary to identify as critical all failure combinations that have 4 or more failed components, although there may be cases where these combinations deserve increased scrutiny. Situations with more than three active independent failures are not likely to degrade safety significantly without also becoming a recognized dispatch or economic problem, and hence they inherently get the needed mitigating attention. However, in cases such as the ability to establish and maintain the necessary failure isolation is uncertain (for example the independence

is provided through complex or potentially error prone means) the associated components are candidates for “critical” designation.

Although the safety analysis performed as part of the design, certification, or continued airworthiness activities may identify a component as critical, that component may not be explicitly identified to maintenance, repair, alteration personnel due to lack of requirements, or lack of specific instructions or other visible means such as placards. It is recognized that a process to communicate these types of instructions to the line personnel are needed to address ALAR Output 4 and CPS Finding 4. Such process will come into focus as the CPS and Safer Skies implementation progresses.

## **APPLICATION EXAMPLES**

### **Example 1: A Mechanical System**

*This example illustrates the fact that complicated analyses are not always needed to identify flight critical system components.*

A leading edge slat drive system consists of a single-load-path torque tube and a monitor to detect torque tube disconnection, and to shut down the power drive unit in order to prevent catastrophic asymmetric lift. The system employs multiple no-back devices to prevent the slats movement following a torque tube disconnect. Suppose the safety analysis determines that:

- a torque tube disconnect alone is a Major failure condition,
- loss of monitor function alone is latent and has a Minor effect,
- loss of no-back function (due to common mode failure) alone is Major,
- with the no-backs working, a torque tube disconnect in combination with loss of the monitor function is Hazardous,
- loss of no-back function in combination with torque tube disconnect is Catastrophic.

Per the policy, the torque tubes, the no-backs, and the monitor are flight critical equipment, even though their individual effects are less than hazardous. The underlying assumptions in the safety assessment associated with component integrity evaluation, anticipated risk due to duration of exposure, maintenance practices, etc., should be scrupulously reviewed and validated; the safety analysis may need to be revised if the safety outcome is found to be overly sensitive to these assumptions.

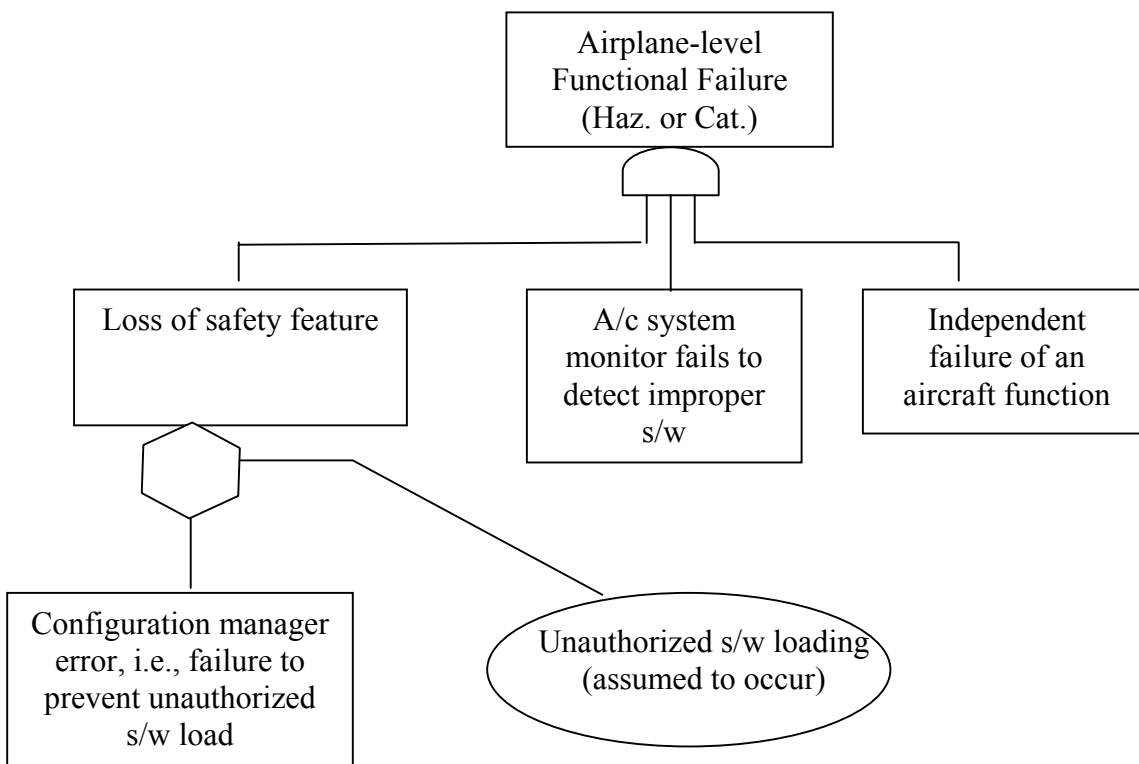
*Identifying flight critical system components in critical systems, such as flight controls in Example 1, is fairly obvious. The following scenarios illustrate more subtle applications of the policy.*

### **Example 2: A Critical Component May Be One That Is Not Active During Flight**

An integrated modular avionics (IMA) system supports multiple aircraft-level functions by allowing flexibility in configuring an aircraft. Configuration flexibility is possible through the use of field-loadable software. Suppose an IMA system has the following characteristics:

- A safety feature such as a safety monitor or a back up function is implemented in field-loadable software (i.e., the software can be loaded without removing equipment from the aircraft.)

- The IMA system has a “configuration manager” that prevents unapproved software from being field-loaded into the IMA system. The configuration manager itself is not modifiable by maintenance personnel.
- To provide redundant protection against unauthorized software configurations, an independent monitor is implemented in the receiving system to detect and annunciate improper functional software load to the flightcrew prior to flight. Suppose the safety analysis identifies the following scenario:



Because the configuration manager malfunction directly causes the loss of a safety feature, the configuration manager is a flight critical system component although its safety effect is not immediate. This example illustrates the definitions of “flight critical system component” are not limited only to components that are active in flight, and they are applicable to any installed components that can adversely affect the safety of flight or occupants. By recognizing the impact of the configuration manager on safety of flight, decisions such as assigning design assurance levels commensurate to the top-level hazards can be justified.

### Example 3: Common cause failures

Consider a dual-channel Communication system and a dual-channel Navigation system.

Suppose the safety assessment concludes that:

- loss of Navigation plus loss of Communication is Catastrophic

- loss of Navigation alone is Major
- loss of Communication alone is Major

Scenario 3.1: Both systems are designed with simple electronic technology. No software or “complex” electronic hardware as defined in RTCA DO-254, “Design Assurance Guidance for Airborne Electronic Hardware” are used. Suppose further that the safety analysis verifies that there are no common mode or cascading failures. Since system redundancy is adequate and because 4 independent failures would have to occur, in-service experience sufficiently validates the assumption that loss of all Communication and all Navigation due to random hardware failures is extremely improbable. Therefore, these components are not considered critical and they need no further scrutiny.

Scenario 3.2: Both channels of the communication system are driven by common software. Similarly, common software drives both channels of the Navigation system. A single common software error (or common hardware design error) in each system could cause the loss of that system. In this case, both components are considered critical.

#### **Example 4: Pay Attention To “Safety Features”**

Suppose the safety analysis of a powerplant installation identifies a condition where a wiring failure could cause an extreme overcurrent condition in a fuel shutoff valve solenoid. If the solenoid cracks, it could cause a fuel leak, ignition source, and damage to the firewall. This could result in a hazardous or catastrophic uncontained engine fire. Hence the safety feature that isolates and protects the wire from shorting (leading to the over current condition) is a flight critical system component.

Distribution:

All ACO Managers

All AFS Managers

All Transport Standards Staff Managers

Manager, Aircraft Engineering Division, AIR-100

Doug Anderson, ANM-7