

2003 FAA National Software Conference

Overview of SAE ARP 4761

FAA AIRCRAFT CERTIFICATION
SERVICE NATIONAL SOFTWARE
CONFERENCE
Reno, Nevada
September 16 - 19, 2003

OVERVIEW OF SAE ARP 4761
GUIDELINES AND METHODS FOR
CONDUCTING THE SAFETY
ASSESSMENT PROCESS ON CIVIL
AIRBORNE SYSTEMS AND EQUIPMENT

JIM TREACY
FAA CHIEF SCIENTIST - AVIONICS

Safety Analyses

History of Aircraft Systems Reveals Many
Disasters

– Many of those disasters came about through
losses or violations of what was thought to be
sufficient redundancy

One purpose of a safety analysis is to
identify for removal all potential
redundancy violators

2003 FAA National Software Conference

Overview of SAE ARP 4761

System Safety Analyses

Redundancy Violators:

- Single Point Failures
- Latent Failures
- Combinations of Failures With Excessively High Probability
- Installation Problems
- Design Errors

So we need an approach that addresses these types of failures

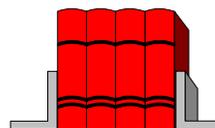
Safety Assessment Guidance

SAE ARP 926A (1979)

- Piece-Part Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis

SAE ARP 1834 (1986)

- Fault and Failure Analysis for Digital Systems



2003 FAA National Software Conference

Overview of SAE ARP 4761

Safety Assessment Guidance

Problems with ARP 926A and ARP 1834

- Guidance not complete for Safety purposes
- Addressed reliability/maintainability
- Outdated
 - Did not fit with DO-178B
 - Did not address Aircraft Level Analysis
 - Did not adequately cover Common Mode Analysis
 - No Preliminary System Safety Assessment (PSSA)

ARP 926A and ARP 1834 have been revised by SAE Sub-Committee S-18 to include a note that indicates for aerospace applications these Aerospace Recommended Practices are obsolete and have been superceded by ARP 4761.

HOWEVER, AC 23.1309-1C ALLOWS THEIR CONTINUED USE FOR SYSTEM SAFETY ASSESSMENT OF SMALL AIRPLANES UNDER SOME CIRCUMSTANCES.

2003 FAA National Software Conference

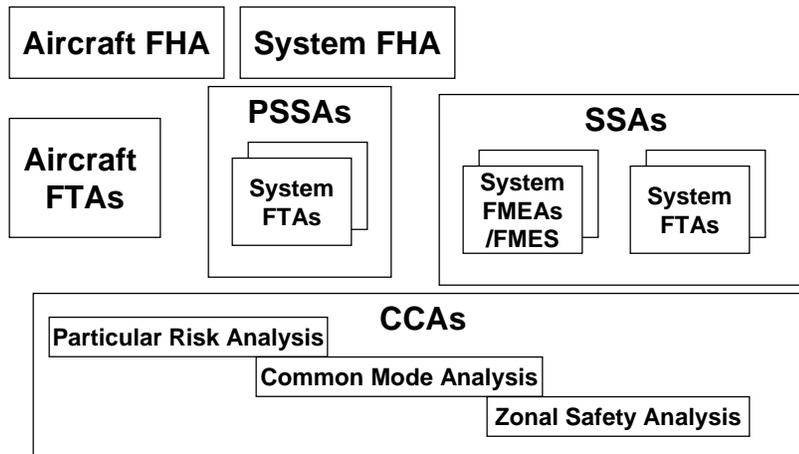
Overview of SAE ARP 4761

ARP 4761

Guidelines and Methods of Performing the Safety Assessment Process on Civil Airborne Systems and Equipment

- Describes in Detail the Process
 - Functional Hazard Assessment (FHA)
 - Preliminary System Safety Assessment (PSSA)
 - System Safety Assessment (SSA)
- Replaces ARP 926A and ARP 1834 for most aerospace applications.

Safety Assessment Process Overview



2003 FAA National Software Conference

Overview of SAE ARP 4761

ARP 4761

- NEW CONCEPTS
 - More Formal Description of Common Cause Analysis
 - Zonal Safety Analysis
 - Particular Risks Analysis
 - Common Mode Analysis

ARP 4761

- NEW CONCEPTS
 - Aircraft Level Functional Hazard Assessment
 - Preliminary System Safety Assessment

Provides a more systematic means of evaluating safety early in the design process and to reduce surprises at the end of the development program.

2003 FAA National Software Conference

Overview of SAE ARP 4761

ARP 4761

- NEW CONCEPTS
 - Fault Tree Analyses
 - Probability calculations of the failure condition based on a per flight basis
 - Probability per flight hour determined by dividing result by average flight time for the particular model aircraft
 - Exposure time for latent failures is resolved and other cases of monitored failures with imperfect monitors are explained

ARP 4761 CAUTION

- ARP 4761 Represents a Consensus
- Techniques have not been used in their entirety by any one manufacturer
- Gradual Implementation Over Time
- Existing Methods Acceptable If:
 - Intent of the Safety Analysis is Met
 - May Need Additional Analysis Where Needed

2003 FAA National Software Conference

Overview of SAE ARP 4761

The graphic features the text 'SAFETY ASSESSMENT TOOLS' in a serif font. The word 'SAFETY' is partially obscured by a hammer icon, 'ASSESSMENT' is partially obscured by a wrench icon, and 'TOOLS' is partially obscured by a screwdriver icon.

SAFETY ASSESSMENT TOOLS

- Functional Hazard Assessment
- Fault Tree Analysis
(Dependence Diagram/Markov Analysis)
- Failure Modes and Effects Analysis
- Common Cause Analysis

FHA PROCESS

- Start With List of System/Aircraft Functions
- Postulate Hazards Based on the Failures in These Functions
- Derive Overall Effect of Hazard on System/Aircraft and People - Failure Condition
- Assess Severity of Failure Condition - Assign Classification

2003 FAA National Software Conference

Overview of SAE ARP 4761

FHA

Relationships

- Independent of Hardware
- Provides criteria against which the other analyses will be assessed.
- Provides the FTA Top Events in the Form of Events of Concern (Failure Conditions)

FHA

When To Do Or Revise It

- Early in the design process
- Revise when functions are added, deleted, altered, or used in different applications
- As a final check, it is prudent to review the FHA again at the end of the program.
- A Functional Hazard Assessment should be conducted for all type certification projects.

2003 FAA National Software Conference

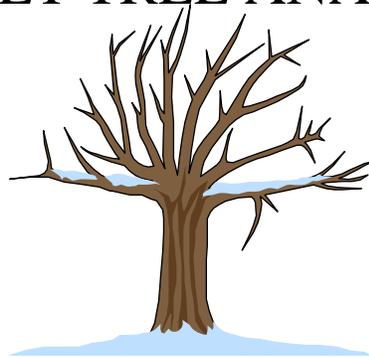
Overview of SAE ARP 4761

FHA

SUMMARY:

- Provides the Top Level Design Criteria
- Determines the Depth of Further Analyses
- Allows for Derivation of the System Architecture
- Independent of Hardware and Software

FAULT TREE ANALYSIS



2003 FAA National Software Conference

Overview of SAE ARP 4761

FAULT TREE ANALYSIS

- Top Down Deductive Analysis
- Focuses on One Undesired Event
- Provides Method for Determining Causes
- Hierarchical Graphical Format
- Ensures That Design Safety Aspects are Identified and Controlled

FAULT TREE ANALYSIS

Attributes:

- Facilitates Technical/Regulatory Reviews
- Assesses Design Modification
- Quantifies Top Event Probabilities
- Allocates Budgets to Lower Level Events
- Assesses Single and Multiple Faults
- Identifies Common Cause Boundaries
- Assesses Contribution of Design Errors
- Assesses Exposure and Latency Intervals

2003 FAA National Software Conference

Overview of SAE ARP 4761

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

FMEA

- Bottom up Inductive Analysis
- Identifies the failure modes of a system, item, function, or piece part
- Determines the effects at the next higher level of design
- The detection method, if any, for failure modes is usually determined
- For a quantitative FMEA, a failure rate is determined for each failure mode

2003 FAA National Software Conference

Overview of SAE ARP 4761

FMEA

PURPOSE: Identifies the effects each failure on system being analyzed and supports the other analysis techniques of the SSA.

SCOPE: The system boundaries and the level of detail of the analysis must be carefully defined.

LIMITATIONS: Does not usually account for multiple failures. May not identify failure modes related to integration and installation.

FMEA

How Does the FMEA support the SSA ?

An FMEA supports the verification of the FTA through a comparison of the FMEA failure effects with the basic events of the fault tree. It can also provide failure rates to quantify the basic events of the fault tree.

2003 FAA National Software Conference

Overview of SAE ARP 4761

FMEA

ANALYSIS

- Determine failure modes and assign failure effect codes
 - Avoid poorly defined failure modes
- Determine detection means, if required
- Verify analysis conclusions with lab and/or aircraft data for safety related functions

Functional FMEA

- Break down the system into “functional blocks”
- Postulate the failure modes for each functional block
- Determine failure effect/detection
- Determine failure rate, if quantitative
 - Note: The entire failure rate of the associated hardware should be assumed for each functional block, unless analyzed in more detail

2003 FAA National Software Conference

Overview of SAE ARP 4761

Piece-Part FMEA

- Determine the failure modes of each individual component
- Determine failure effect/detection
- Determine failure rate, if quantitative

What is an FMES ?

Failure Modes and Effects Summary

- Grouping of failure modes with like effects
- FMES failure rate is the sum of the failure rates coming from each FMEA
- Used as an aid to quantify FTA primary events

2003 FAA National Software Conference

Overview of SAE ARP 4761

COMMON CAUSE ANALYSIS

What is a common cause?

AN EVENT WHICH BYPASSES OR
INVALIDATES REDUNDANCY OR
INDEPENDENCE, I.E.... AN EVENT
WHICH CAUSES THE
SIMULTANEOUS LOSS OF
REDUNDANT OR INDEPENDENT
ITEMS

2003 FAA National Software Conference

Overview of SAE ARP 4761

Common Cause Analysis

Establishes the need for the safety assessment process to address the impacts of potential common cause faults

Common Cause Analysis

CCA is subdivided into three areas of study:

- Zonal Safety Analysis
- Particular Risks Analysis
- Common Mode Analysis

2003 FAA National Software Conference

Overview of SAE ARP 4761

Zonal Safety Analysis

Examines each physical zone of the aircraft to ensure that equipment installation and potential physical interference with adjacent systems do not violate the independence requirements of the system under study.

Zonal Safety Analysis

- Part of aircraft development
- Based on CAD, mockups, aircraft
- Usually performed by the airframe manufacturer
- Problems fed back into design

2003 FAA National Software Conference

Overview of SAE ARP 4761

Particular Risks Analysis

Examines those common events or influences which are outside the system(s) concerned but which may violate independence requirements. These particular risks may influence several aircraft zones.

Particular Risks Analysis

- Mostly a qualitative analysis
- Drawings, models, mock-ups, aircraft
- Performed on a risk by risk basis
- Applies to the whole aircraft development process
- Some risks may be subject to specific airworthiness requirements (e.g... engine rotor burst, tire burst, etc.....)

2003 FAA National Software Conference

Overview of SAE ARP 4761

Particular Risks Analysis

Typical risks would include:

Fire	Bulkhead Rupture
Bird Strike	Hail/Ice/Snow
Tire Burst	Rotor Burst
Wheel Rim Release	Manifold Rupture

NOTE: Some events may also be analyzed as part of the Zonal Safety Analysis

Common Mode Analysis

Provides an assessment that the independence claims made in the FTA are valid. This analysis covers the effects of design, manufacturing, and maintenance errors and the effects of common component failures.

2003 FAA National Software Conference

Overview of SAE ARP 4761

Common Mode Analysis

- CMA is carried out at all levels from item design to aircraft level design
- Includes an evaluation of the components within an item
- Based on inputs from the FHA and PSSA
- Verifies that independence principles have been applied when necessary

Common Mode Analysis

SCOPE:

- For each Hazardous or Catastrophic event documented in the FHA and/or PSSA, identify each AND event (AND gate in fault tree) to determine which failure combinations must be assured to be independent.

2003 FAA National Software Conference

Overview of SAE ARP 4761

Common Mode Analysis

Alternate Approach:

- For each Hazardous or Catastrophic event documented in a Fault Tree, evaluate each element of the minimal cut set of the fault tree to determine which failure combinations must be assured to be independent.

Common Mode Analysis

Example Common Modes:

- Software Design Error
- Hardware Design Error
- Hardware Failures
- Production/Repair Flaw
- Stress Related Events (abnormal)
- Environment (Temp. , Vib. , etc.....)

2003 FAA National Software Conference

Overview of SAE ARP 4761

Preliminary System Safety Assessment (PSSA)

PSSA

DEFINITION:

A system evaluation of the proposed architecture(s) and implementation(s) based on the Function Hazard Assessment (FHA) failure condition classifications to determine safety requirements of the system.

2003 FAA National Software Conference

Overview of SAE ARP 4761

PSSA

The PSSA is:

- Imbedded within the overall development
- An iterative process associated with the design definition
- Conducted at multiple stages including system, sub-system, LRU/LRM, and hardware/software levels

PSSA

The PSSA is:

- Intended to be part of the designer's trade studies to determine system characteristics
- Coordinated with the FAA when the architecture for the final design has been determined

2003 FAA National Software Conference

Overview of SAE ARP 4761

PSSA PURPOSE

- The objective of the PSSA is to establish the safety requirements of the system and to determine that the proposed architecture/implementation can reasonably be expected to meet the safety objectives identified by the PSSA.

PSSA

- FORM
 - The PSSA can be thought of as a Fault Tree with budgets.
 - Primary Events associated with AND gates determine derived safety requirements for the protection from common-cause failures and errors.

2003 FAA National Software Conference

Overview of SAE ARP 4761

PSSA

- **OUTPUTS:**

- Safety Requirements Allocated to Items
- Installation Requirements (separation, segregation, isolation, etc.....)
- Hardware and Software Design Assurance Levels
- Safety Maintenance Tasks and Associated Non-exceed Times

System Safety Assessment (SSA)

2003 FAA National Software Conference

Overview of SAE ARP 4761

SSA

A System Safety Assessment is a systematic, comprehensive evaluation of the implemented system to be certificated to show that the qualitative and quantitative safety requirements as defined in the FHA and PSSA have been met.

SSA

- The SSA is usually based on the PSSA FTA and uses the quantitative values obtained from the FMEA/FMES.
- The SSA should verify that the FMEA effects and the FTA primary events are compatible
- The SSA should also include the Common-Cause Analysis results.

2003 FAA National Software Conference

Overview of SAE ARP 4761

Common Mode Analysis for SSA

SCOPE:

- For each Hazardous or Catastrophic event documented in the System Safety Assessment, identify each AND event (AND gate in fault tree) to determine which failure combinations must be assured to be independent.

Common Mode Analysis for SSA

Alternate Approach:

- For each Hazardous or Catastrophic event documented in a Fault Tree for the System Safety Assessment, evaluate each element of the minimal cut set to determine which failure combinations must be assured to be independent.