AEROSPACE INFORMATION REPORT

AIR6110™	REV. A

Issued 2011-12
Reaffirmed 2020-02
Stabilized 2024-03

Superseding AIR6110

Contiguous Aircraft/System Development Process Example

RATIONALE

This technical report is being stabilized following the release of ARP4754B. Appendix E of ARP4754B contains an updated version of the contiguous example which has been coordinated with ARP4761A Appendix Q. AIR6110 is still valid for use with ARP4754A, and it is not expected to be updated in the future.

STABILIZED NOTICE

This document has been declared “STABILIZED” by SAE S-18 Aircraft and Sys Dev and Safety Assessment Committee and will no longer be subjected to periodic reviews for currency. Users are responsible for verifying references and continued suitability of technical requirements. Newer technology may exist.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

For more information on this standard, visit
https://www.sae.org/standards/content/AIR6110A/

FORWARD

ARP4754A/ED-79A contains information which places the information in this AIR in context. This AIR should be used in conjunction with the main body and the appendices of ARP4754A/ED-79A. In addition, this example shows the interrelationships with ARP4761.

1. INTRODUCTION

1.1 Scope

This AIR provides a detailed example of the aircraft and systems development for a function of a hypothetical S18 aircraft. In order to present a clear picture, an aircraft function was broken down into a single system. A function was chosen which had sufficient complexity to allow use of all the methodologies, yet was simple enough to present a clear picture of the flow through the process. This function/system was analyzed using the methods and tools described in ARP4754A/ED-79A. The aircraft level function is “Decelerate Aircraft On Ground” and the system is the braking system. The interaction of the braking system functions with the aircraft are identified with the relative importance based on implied aircraft interactions and system availabilities at the aircraft level. This example does not include validation and verification of the aircraft level hazards and interactions with the braking system. However, the principles used at the braking system level can be applied at the higher aircraft level. The methodologies applied here are an example of one way to utilize the principles defined in ARP4754A/ED-79A. The function chosen was the braking system. Other formats may be used to accomplish the documentation, so long as the principles outlined in ARP4754A/ED-79A are followed.

This example contains references to documentation that a company may use to assure itself of the safety of its products but does not include the documentation that the Original Equipment Manufacturer (OEM) would be required to submit at the aircraft level for aircraft certification. Some of these documents are submitted to the regulatory agencies for the purpose of certification (e.g. the Wheel Brake System FHA). Other documents are internal to the company and not required to be submitted for certification. No implication is made that these documents should be submitted to a regulatory agency and none should be implied, although all documents should be available for submission if requested by the regulatory agency. Safety and Certification are not synonymous terms. The example shows the systems engineering process as applied to the development of an aircraft, including some processes that are beyond certification requirements.

Figure 1 depicts the flow of activities within this example. This figure provides a guide to the structure of this AIR and should allow the reader to quickly find specific areas within the example using the cross references.

Figure 1 includes the top aircraft level tasks to provide the reader a reference point. The detailed example in Section 3 of this AIR covers only the activities related to the braking system. Figure 1 presents a sequence of activities found in a typical development program. In a real development program, the development process is usually far more complex. For example, in a real development program, development of the different levels (aircraft, system and item) often occurs concurrently, rather than serially as depicted in example flow.

The top row of Figure 1 represents the activities that will occur within the aircraft development. The middle row represents the activities that occur within the wheel brake system development. The bottom row represents the activities that are covered for the subsystem-level Brake System Control Unit (BSCU) development, as well as the integration and verification activities at the higher levels.

The Figure 1 example flow also shows where major artifacts from the System Safety Process (ARP4761) will be utilized. The example flow shows how the sections and artifacts are laid out and represents the step by step process detailed in ARP4754A/ED-79A. In a real development program, the System Safety Process occurs concurrently with ARP4754A/ED-79A, constantly receiving inputs from the ARP4754A/ED-79A process and providing feedback to ARP4754A/ED-79A processes.

Figure 1 also shows a box titled Integral Processes to illustrate to the reader that the integral processes are utilized throughout the development process. The reader is encouraged to use this example flow diagram to help navigate the example. This will allow the reader to either read the example in its entirety or use it as a quick reference guide in order to quickly find the desired section.

1.2 Document Format

This AIR contains the following sections and appendices:

Section 1 is an introduction to the document, giving the scope, format, references to other documents, an acronym list, and a description of the example aircraft function being developed.

Section 2 describes the overall example aircraft development process, focusing on activities leading to the development of the braking system. The hypothetical aircraft in this example is introduced and its basic requirements are given. Aircraft-level planning documents are identified. Top-level aircraft functions are decomposed to determine the functions required of the braking system. The aircraft level safety assessment process, including the aircraft FHA and the Preliminary Aircraft Safety Assessment (PASA), is conducted. The PASA assigns development assurance levels to aircraft functions. These functions are allocated to the braking system as part of the overall aircraft architecture. Aircraft requirements relevant to the braking system are validated. The braking system is integrated and validated with the other systems on the aircraft. (Note: PASA is introduced in ARP4754A/ED-79A, but detailed guidance for completing it awaits the release of ARP4761A. This AIR does not conduct the PASA; it just uses its results).

Section 3 contains the detailed example development process for the braking system. The system is introduced and its planning elements are identified. System functions and requirements are developed. The system safety assessment process, including the system FHA, PSSA and SSA, is conducted. The braking system architecture is developed and selected from among candidate architectures on which trade studies have been conducted. The PSSA leads to assignment of the development assurance levels for the Braking System Control Unit and the other systems and items comprising the system architecture. Braking system requirements are captured and derived requirements are identified. Interface requirements are identified both external to the system and between the items of the system. Requirements are allocated to the items, and the system requirements are validated. System integration, process assurance and configuration management examples are given.

Section 4 describes the verification of the braking system and the associated aircraft-level verification of the system as installed on the aircraft.

Appendix A is an example of an aircraft-level development plan.

Appendix B is an example of a braking system requirements management plan.

Note: For the sake of brevity, the appendices contain only a subset of the plans which would be generated for an aircraft development program.

This AIR contains a number of artifacts (documents, tables, etc.) that would be produced by following the process in ARP4754A/ED-79A. These artifacts are enclosed in boxes to distinguish them from explanatory text.

Editorial comments are provided in italics. Where necessary, the reader is directed to the appropriate section of ARP4754A/ED-79A or ARP4761 for further guidance on the process involved.

If there are any differences between this AIR and ARP4754A/ED-79A, ARP4754A/ED-79A will take precedence.

2. REFERENCES

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of the other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

The following documents are referenced in this AIR. Reference to 14CFR herein implies reference to equivalent CS regulation.

2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

ARP4754A Guidelines for Development of Civil Aircraft and Systems

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

2.2 Code of Federal regulations (CFR)

Available from the United States Government Printing Office, 732 North Capitol Street, NW, Washington, DC 20401, Tel: 202-512-0000, www.gpoaccess.gov.

14CFR 25.1309 / CS 25.1309

14CFR 25.735 / CS 25.735

2.3 EUROCAE Publications

Available from EUROCAE, 102 rue Étienne Dolet, 92240 Malakoff, France, +33 1 40 92 79 30, www.eurocae.net.

ED-79A Guidelines for Development of Civil Aircraft and Systems

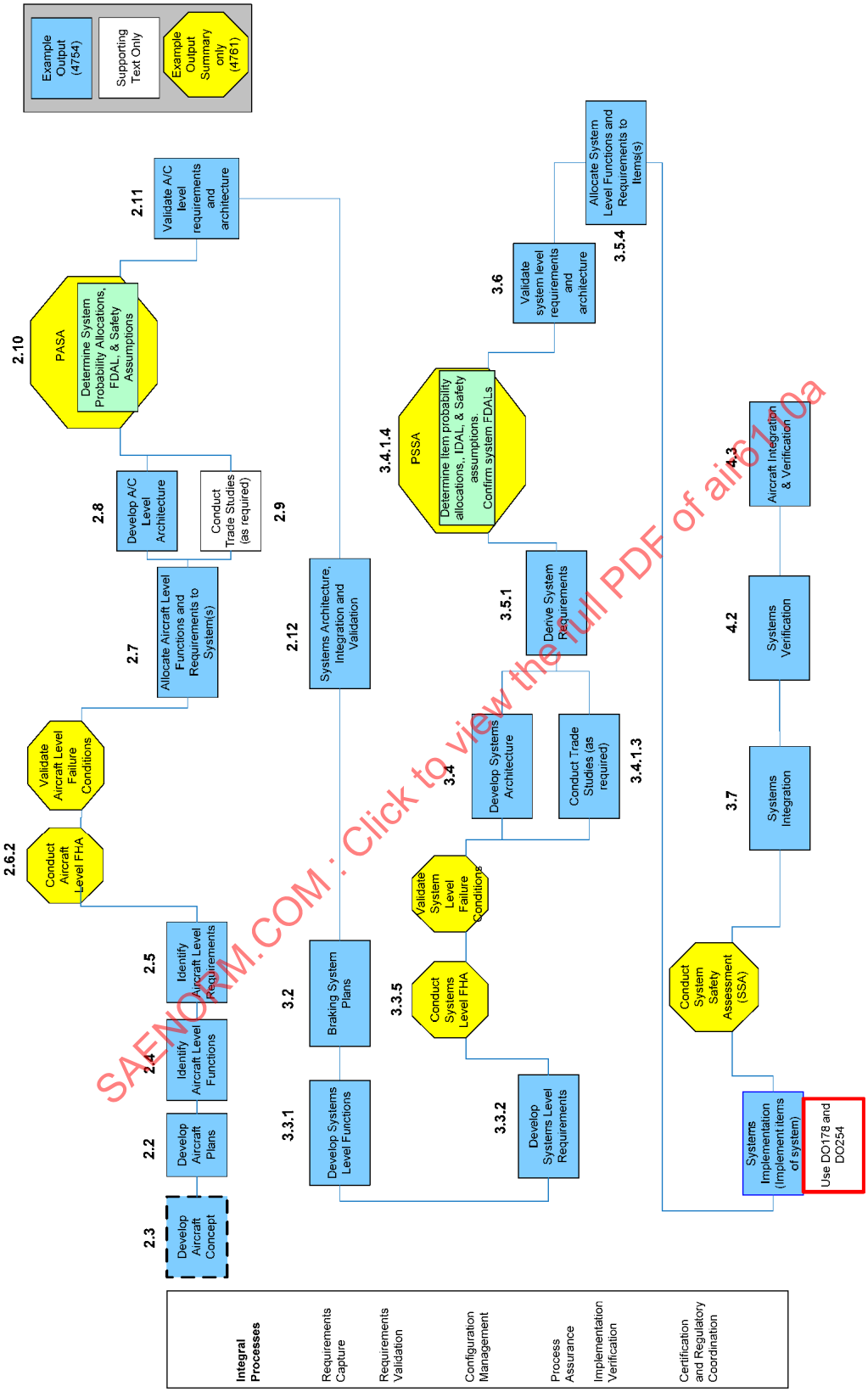


FIGURE 1 – EXAMPLE FLOW

2.4 Acronym List

A/C	Aircraft
ACCU	Accumulator
ALT	Alternate
APU	Auxiliary Power Unit
AS	Anti Skid
ASA	Aircraft Safety Assessment
B	Blue Hydraulic System
BSCU	Brake System Control Unit
C	Capacitor
CAT IIIb	Category 3b All Weather Landing System
CCA	Common Cause Analysis
CI	Configuration Item
CMA	Common Mode Analysis
CMD	Command
COM	Command (Channel)
COMP	Computation
CPU	Central Processing Unit
CSMG	Constant Speed Motor Generator
ECS	Environmental Control System
ELEC	Electric
EMI	Electromagnetic Interference
FDAL	Functional Development Assurance Level
FFS	Functional Failure Set
FHA	Functional Hazard Assessment
F.R.	Failure Rate
FTA	Fault Tree Analysis
G	Green Hydraulic System
HIRF	High Intensity Radiated Fields

HYD	Hydraulic
IC	Integrated Circuit
ICD	Interface Control Document
IDAL	Item Development Assurance Level
I/O	Input/Output
L or LH	Left or Left Hand
LRU	Line Replaceable Unit
MLG	Main Landing Gear
MON	Monitor
MT	Periodic Maintenance Task
NLG	Nose Landing Gear
NORM	Normal
OEM	Original Equipment Manufacturer
PAMB	Ambient Pressure
PASA	Preliminary Aircraft Safety Assessment
PCU	Power Control Unit
POS	Position
P/S	Power Supply
PR	Problem Report
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
PTU	Power Transfer Unit
PWM	Pulse Width Modulator
PWR	Power
R or RH	Right or Right Hand
R	Resistor
R	Right
REF	Reference
RTO	Rejected Takeoff

SIT	System Integration Test
SSA	System Safety Assessment
STBY	Standby
SYS	System
VDC	Volts Direct Current
V1	Speed above which the aircraft cannot be safely stopped on remaining runway
WBS	Wheel Brake System
ZSA	Zonal Safety Analysis

2.5 Description of the Example Function

The aircraft function analyzed is: "Decelerate aircraft on the ground (stopping on the runway)". This example acknowledges other aircraft systems involved in decelerating the aircraft, but for clarity concentrates on the aircraft braking system, the details of which are evolved through the following example approximately as they would in a real life situation.

The "Decelerate aircraft on the ground (stopping on the runway)" function, which is also used as the ARP4761 example, was intentionally selected to show the interrelationships between ARP4754A/ED-79A (system development process) and ARP4761 (system safety assessment process).

TABLE OF CONTENTS

LIST OF FIGURES

3. AIRCRAFT DEVELOPMENT PROCESS

3.1 Aircraft Introduction

The aircraft development process includes the development of the aircraft level functions, requirements, and architecture for the S18 aircraft. The purpose is to develop a complete list of aircraft requirements, determine a proposed aircraft design that can reasonably satisfy the requirements, and derive the lower level requirements to be considered in the design of the aircraft systems and lower level systems and items.

This AIR describes, in detail, a contiguous example of the design development process for the S18 aircraft braking system. In addition, the goal is to show the relationship between ARP4754A/ED-79A and ARP4761. In order to present a clear picture, some of the aircraft level tasks are provided to better understand potential interactions that may drive requirements down to the braking system level. The function “Decelerate aircraft on the ground (stopping on the runway)” is broken down into a single system and its items. A function is chosen which has sufficient complexity to allow use of all the methodologies, yet is simple enough to present a clear picture of the flow through them.

3.2 Aircraft Planning Documents

An example Aircraft Development Plan is included in Appendix A.

Other examples of planning documents are included at the braking system level (see section 3.2). In a real program all planning documents would be written at both the system and the aircraft levels as required, but only a few plans are included in their entirety in this AIR to maintain a reasonable-sized document. Other plans are referenced as necessary.

The Aircraft Development Plan defines the development process activities and integral processes of the aircraft development life cycle. Also included are the life cycle environment, including the methods and tools to be used for the activities of each life cycle process, and the development standards.

See Appendix B of ARP4754A/ED-79A for the format and content of an Aircraft Safety Program Plan.

3.3 Aircraft Description

(Editor’s Note: The following aircraft flight profile was developed from an iteration of independent market surveys, customer requests, and initial design and trade studies).

The S18 aircraft is a two engine passenger aircraft designed to carry 300 to 350 passengers up to 5000 nautical miles at 0.84 mach. The average flight duration is 5 hours.

The aircraft concept of operations led to the aircraft mission specification, which then led to preliminary aircraft sizing and preliminary aircraft design.

The S18 aircraft concept is the result of the program concept phase and is the same as that used in the ARP4761 example appendix. The S18 aircraft was developed by finalizing different high level aircraft mission profiles. The aircraft mission profiles will generally be developed from the marketing and business decisions made during these initial marketing efforts. The aircraft concept development could be the finalization of the different high level aircraft mission profiles, some of which include:

- High level aircraft requirements (payload, range, etc.)
- Tradeoff between aircraft that flies faster versus an aircraft that consumes less fuel
- Tradeoff between aircraft that predominately supports hub and spoke versus point-to-point operations

For the sake of brevity, these tradeoffs are not included in the example.

3.4 Aircraft Functions

The S18 aircraft needs to perform the following “basic” aircraft level functions as shown in Figure 2. There can be many other “customer” required functions.

The aircraft FHAs from SAE’s previous aircraft program were used as a checklist when developing the aircraft level functions. This helped the SAE team to ensure that functions were not missed and to shorten the aircraft function development time. The aircraft level functions were captured from various sources including the Aircraft Level Requirements Document, Safety Program Plan, and Aircraft Level Certification Plans.

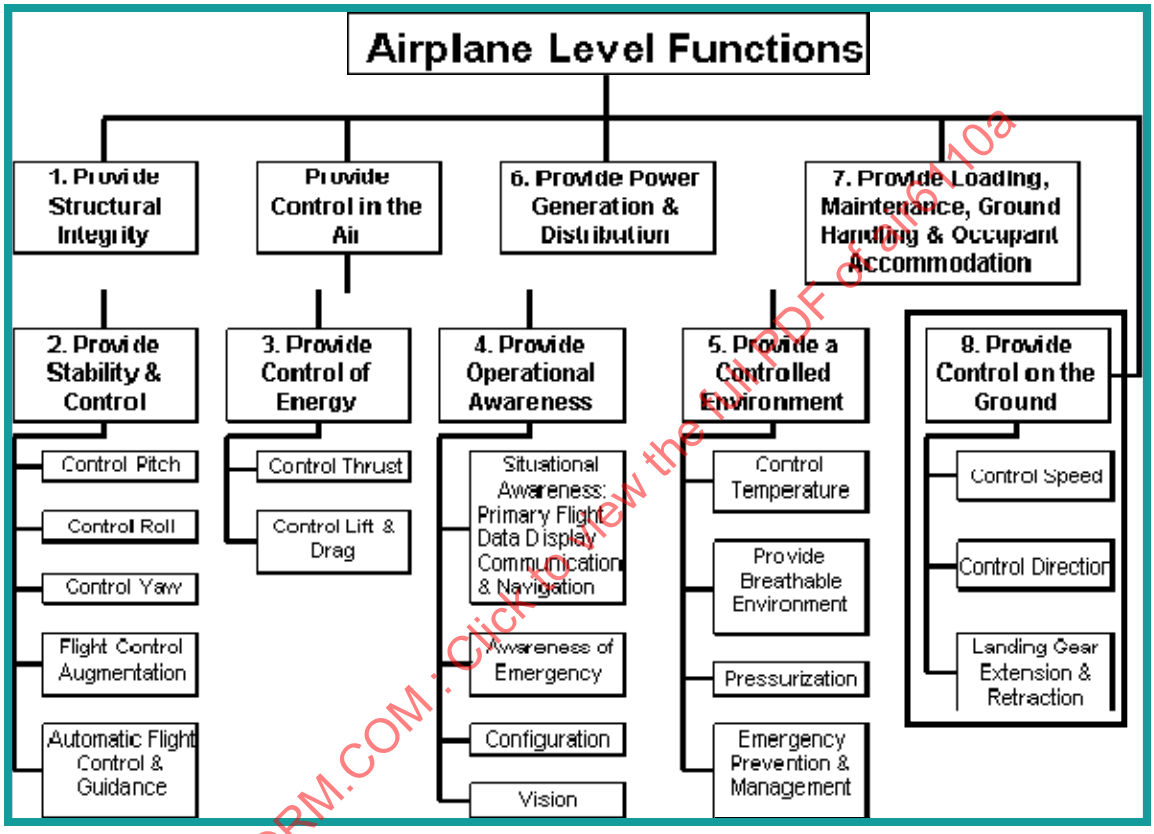


FIGURE 2 - AIRCRAFT LEVEL FUNCTIONS

(Editor’s Note: The example focuses on a sub-function of the “Provide Control on the Ground” function, specifically, the “Control Speed” function. Note that there can be more than one level of aircraft function decomposition).

3.4.1 Aircraft Functional Decomposition

The S18 aircraft level functional decomposition for “Control Speed”, which is a second level function of the first level aircraft function “Provide Control on the Ground”, is shown in Figure 3.

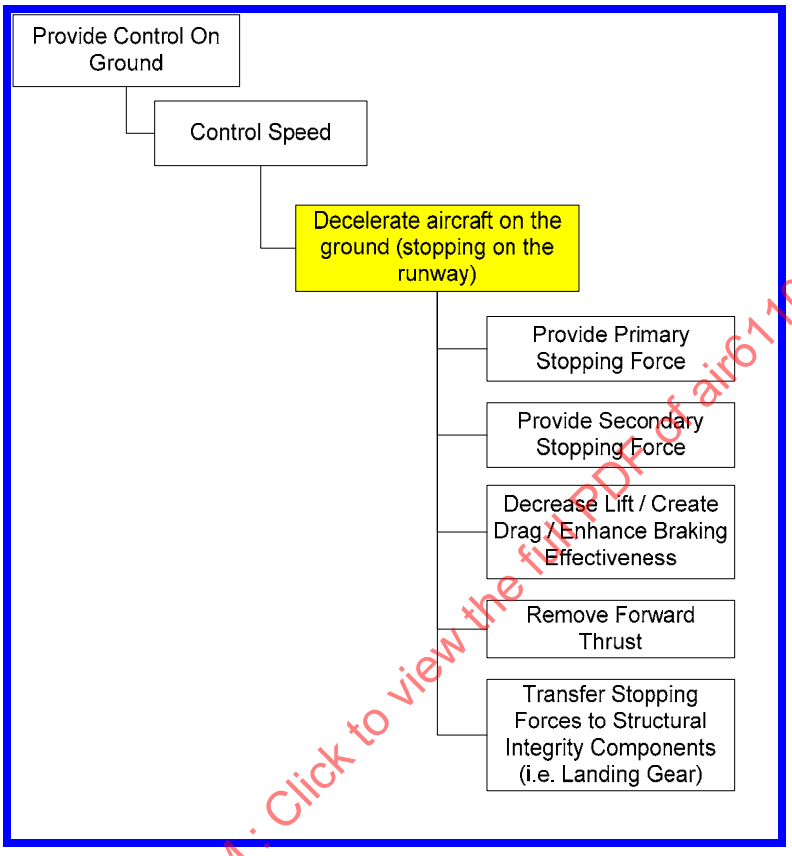


FIGURE 3 - DECOMPOSITION OF PROVIDE CONTROL ON GROUND FUNCTION

(Editor’s Note: To the maximum extent possible, the functions should be independent of the design. For example, there are several different design solutions which could be used to provide stopping forces. The determination of the allocation to the system will be completed as part of the trade studies, etc.).

3.5 Aircraft Requirements

(Editor’s Note: The development of aircraft requirements starts with the certification requirements and market/technology research. These requirements establish preliminary (initial) requirement sets. Usage of “know how” from previous programs expands this preliminary (initial) requirement sets to a degree sufficient for initial architecture trade studies. With the ongoing trade studies the requirements get enough maturity to start the safety assessment. Safety assessment results are used to derive safety requirements for the aircraft. During the requirements development life cycle special care should be focused on the validation of each requirement. As it will be explained in more detail in the following chapters, the validation activities start along with the requirement development process. This example is focused on some of the requirements related to the Wheel Brake System. It is organized to show how a requirement is flowed down with traceability from the aircraft level to the system and system interface level, and to the hardware and software item level).

3.5.1 Sizing to Landing Distance Requirements

The S18 aircraft and its systems are “sized” for the intended mission. To provide a general idea of what takes place during the high level aircraft definition, examples of the factors that translated the function “Decelerate aircraft on the ground (stopping on the runway)” into a quantified requirement included the following:

- Landing Weight
- Approach speed
- Deceleration method used
- Flying qualities of the aircraft
- Pilot technique
- Assumed environmental conditions
- Takeoff weight (for rejected takeoff)
- V1 speed

The landing distance requirements are formulated at the maximum design landing weight of the S18 aircraft.

Tradeoffs between the Landing Weight (W_L) to Takeoff Weight (W_{TO}) Ratio were made, balancing the competing interests of the landing gear and the fuel jettison systems (landing gear weight is helped by a low W_L / W_{TO}; a high W_L / W_{TO} could result in excessive fuel being required to be dumped).

In addition, trade studies were conducted to determine the systems to dissipate the kinetic energy at landing.

(Editors’ Note: Systems aircraft development, requirements development and trade studies are recursive, iterative processes. Interface decisions will influence the systems aircraft architecture; systems aircraft architecture decisions will influence interfaces).

3.5.2 Aircraft Requirements Traceability

The S18 aircraft requirements traceability is depicted in Figure 4 and was developed as follows: the top level aircraft requirements, as described in Section 3.5, were decomposed (i.e. “traced down”) to the top level system requirements. The system requirements were grouped into interface management requirements and all other system requirements. The system requirements (including the interface requirements) were flowed down to subystems and items that make up the higher level system. For this example, it is assumed the flow down and relationships between the braking system and other aircraft systems will be validated and verified at the aircraft level by the aircraft manufacturer and is outside the scope of this example.

(Editor’s Note: The other aircraft level requirements defining this aircraft would be included in this paragraph, but are not described for the sake of brevity. The requirements need to be validated to ensure that they are compatible and consistent with the aircraft concept of operations. This is an iterative, recursive process. Top level requirements will need to be validated as the lower level requirements are developed and the systems architectures are developed in further detail).

The link between the aircraft requirements and the system requirements and between the high level system requirements and the subsystems and items requires special attention in development of the S18 aircraft. In this example, the OEM is responsible for the aircraft level. Supplier A is responsible for the top-level Braking system. Finally, other suppliers are responsible for some of the lower level items and subsystems (some subcontracted by the OEM and other subcontracted by Supplier A). Therefore these links represent not only the relationship between higher level requirements and lower

level requirements, but they also indicate where major team interfaces will be needed. To ensure the right aircraft is developed in the manner intended, careful management of the requirements and the traceability between them is crucial.

Figure 4 is taken from the aircraft requirements specification to show the nomenclature used to identify and trace requirements.

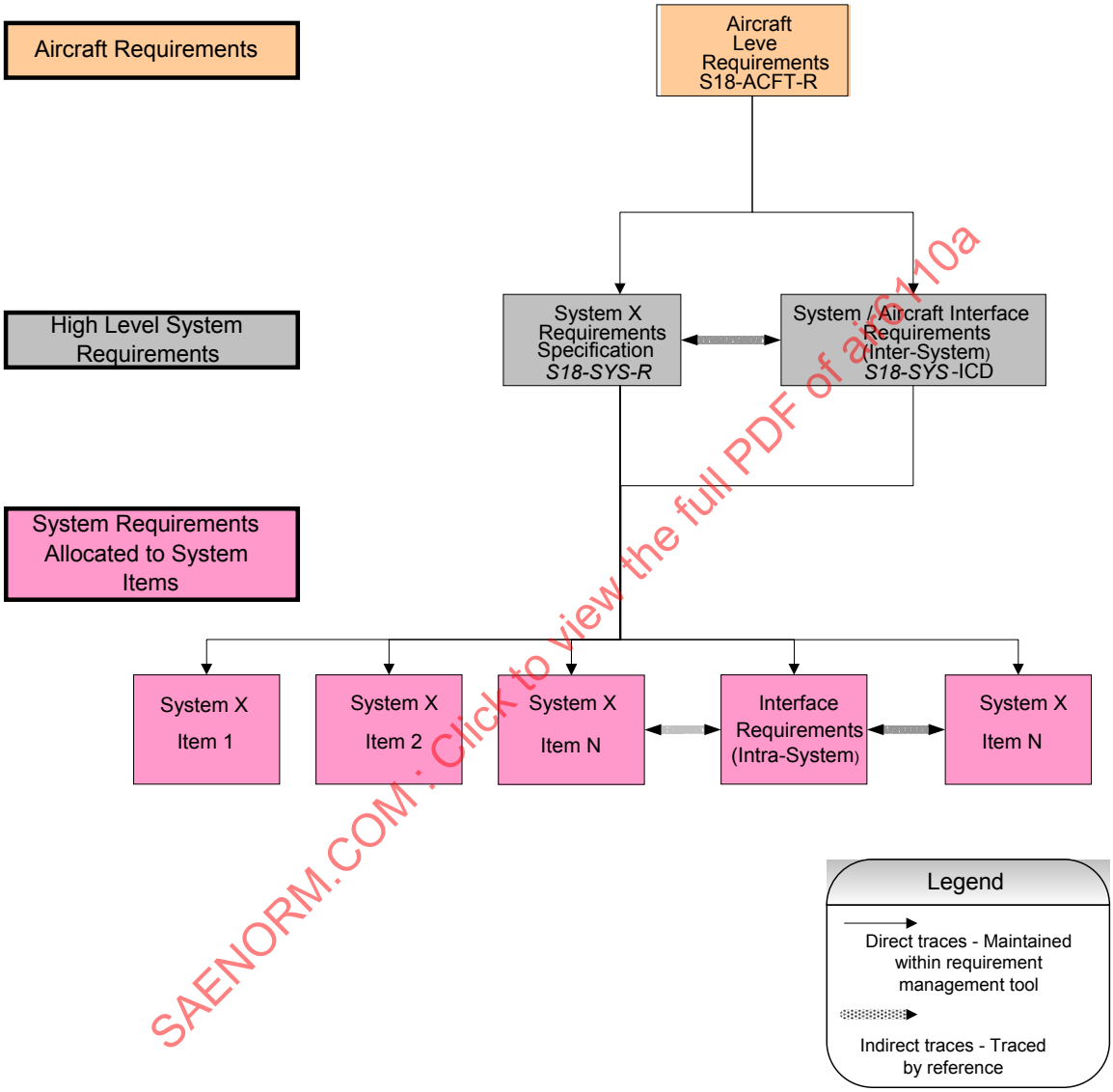


FIGURE 4 - AIRCRAFT REQUIREMENTS TRACEABILITY

3.5.3 Aircraft Requirements Specification

(Editor's Note: The following excerpt from the aircraft requirements specification shows a subset of the requirements which will be used to trace to braking system requirements).

Requirement #	Description	Traced From	Rationale
S18-ACFT-R-0009	Aircraft shall have a means to decelerate on the ground in accordance with 14CFR 25.735	14 CFR Part 25.735	Minimum standard required for aircraft certification
S18-ACFT-R-0110	Aircraft shall have autobrake function	Derived	Technological improvements in CAT IIIb auto-landing capability and market research, (report MRS18-XXX) about the customer needs
S18-ACFT-R-0135	Aircraft shall provide an anti-skid function.	Derived	All weather operation and stability of the aircraft during runway runs and market research, (report MRS18-XXX) about the customer needs
S18-ACFT-R-0184	Aircraft shall have hydraulically-driven brake function	Derived	Trade studies TS18-XXXX (not shown in the example) determined that the hydraulic drive of brake system is more economically feasible than electrical systems given the reuse of hydraulics systems from previous SAE aircraft.
S18-ACFT-R-0185	The pilot shall be allowed to override the autobrake function.	14CFR 25.735(c)(2)	Autobrake function is derived from the crew operational design requirement allowing override.

FIGURE 5 - AIRCRAFT REQUIREMENTS SPECIFICATION (EXCERPT)

3.6 Aircraft Level Safety Assessment Process

The aircraft level functions were passed to the System Safety Process (ARP4761) to be analyzed in the aircraft level FHAs. The aircraft level safety assessment process is a critical task in the overall safety assessment process, culminating in a development assurance process that establishes and drives system requirements from the top down. This requires the safety analyst to ensure the failure conditions and their associated assumptions at the aircraft level are complete and correct to gain confidence that all the critical hazards have been captured.

3.6.1 ARP4754A Inputs to ARP4761 Aircraft Functional Hazard Assessment Process

The functions which are developed as part of the aircraft function and functional decomposition in ARP4754A/ED-79A provide the inputs to the Functional Hazard Assessment process in ARP4761. For the purpose of this example, the FHA will be conducted on the "Decelerate Aircraft on the Ground" function, which was identified during the functional decomposition in 3.4.1.

3.6.2 Aircraft Functional Hazard Assessment (FHA)

An aircraft functional hazard assessment is the root of a process that is conducted for each of the aircraft first-level functions identified in section 3.4 but, as stated earlier, this example will focus on one of these aircraft functions, “Provide control on ground” and its associated second-level function “Control speed”. The functional breakdown depicted in section 3.4.1 for the second-level function “Control speed” identifies the aircraft level function “Decelerate aircraft on the ground (Stopping on the runway)” as the starting point for the failure condition identification phase.

The failure conditions identification phase for this function is conducted in accordance with ARP4761, which outlines the process for discovery of all the possible failure modes and combinations of failures, addressing both loss of or malfunction of a function. This process is aided by an understanding of the overall aircraft-level functional requirements. This is especially true when the effect of a certain failure depends on the integration and interaction of another function (such as would be the case for the “Air/Ground Determination” function where a number of aircraft-level functional failure conditions are dependent on this function). The ARP4761 assessment process is utilized to gain an understanding of all the potential failure modes, assumptions made and contributing factors influencing the effects each failure condition has on the aircraft and its occupants.

Areas/factors of consideration in the assessment of each failure condition associated with the aircraft function “Decelerate aircraft on the ground (Stopping on the runway)” would include:

- Environmental conditions (e.g. weather, runway surface)
- Emergency configuration (e.g. rejected takeoff)
- Applicable flight phases when the severity of the condition changes with different flight phases (e.g. takeoff, landing)
- Interfacing functions

The determination of the effects each failure condition imparts on the aircraft and its occupants is accomplished through analysis of accident/incident data, reviewing regulatory guidance material and by consultation with individuals with previous design and operational experience. For those failure condition effects that are not well understood, additional supporting material (e.g. simulation, studies, flight tests, etc.) should be defined to validate the classifications made. The rationale used for any assumptions in determining the effects and classification of any failure condition should be preserved to ensure traceability for future reference.

A subset of the results of the ARP4761 assessment process conducted for the aircraft-level function “Decelerate aircraft on the ground (Stopping on the runway)” are shown in the aircraft level functional hazard assessment matrix shown in Figure 6. This matrix lists the functional failure conditions assessed during this process and the agreed upon associated hazard classification and is the starting point for the generation and allocation of safety requirements.

The above process would be repeated for the remaining seven aircraft first-level functions (i.e. those functions other than “Provide Control on Ground”) depicted in the diagram in section 3.4.1 for completeness of the aircraft level functional hazards assessment matrix.

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification
Decelerate Aircraft on Ground	Loss of Deceleration Capability	Landing, RTO, Taxi	See Below	See Below
	a. Unannunciated loss of Deceleration Capability	Landing, RTO	Crew is unable to decelerate the aircraft, resulting in a high speed overrun	Catastrophic
	b. Annunciated loss of Deceleration Capability	Landing	Crew selects a more suitable runway, notifies emergency ground support, and prepares occupants for runway overrun.	Hazardous
	c. Unannunciated loss of Deceleration Capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles.	Major
	d. Annunciated loss of Deceleration Capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.	No Safety Effect

FIGURE 6 - AIRCRAFT FHA (EXCERPT)

3.7 Aircraft Function Allocation

The S18 aircraft level functional allocation for "Decelerate Aircraft on the Ground" is shown in Figure 7. The initial wheel brake system requirements given in section 4.3.2 are outputs of the allocation activity, along with the functional requirements for the other systems shown in Figure 7.

(Editors' Note: **Figure 7** ***assumes some systems will be present on the S18 aircraft, as shown in the top row (Brake System, Thrust Reverser, etc). These systems were identified from the development of the initial high level architectures. This allocation will be an important input into the Preliminary Aircraft Safety Assessment (PASA). The purpose of the functional allocation is to identify the system(s) which will implement the respective function(s). This is a recursive, iterative process. After aircraft functions have been allocated to systems by the design process, each system which integrates multiple aircraft functions should be re-examined using the system level FHA process).***

Function	S18 Aircraft	Wheel Brake System	Thrust Reverser	Spoilers	Engine Controls	Structural Integrity (Landing Gear, Fuselage, etc.)
Decelerate Aircraft on the Ground	X	X	X	X	X	X
Provide Primary Stopping Force		X				
Provide Secondary Stopping Force			X			
Decrease lift / Create drag / Enhance Braking effectiveness				X		
Remove Forward Thrust					X	
Transfer Stopping Forces to Structural Integrity Components				X		X

FIGURE 7 - AIRCRAFT FUNCTION ALLOCATION (EXCERPT)

3.8 Aircraft Architecture

The preliminary aircraft architecture decisions for the S18 aircraft considered the following:

- Overall configuration: Conventional, tail aft
- Fuselage Layout:
  - Arrangement of crew, passengers, fuel, cargo and other payloads
  - Cockpit / flight deck layout
  - Cabin layout
  - Window, door, and emergency exit layout
  - Fuel, baggage and cargo volume
  - Access for loading and unloading
  - Access for maintenance and servicing
- Propulsion type: Turbofan
- Number of engines: Two
- Integration of propulsion system: Engines in nacelles on the wing
- Wing and empennage (tail) geometry
- Selection of major systems to be employed by the aircraft
  - Flight control system, primary and secondary
  - Landing gear (including wheel brakes)
  - Thrust reverser
  - Auxiliary power unit
  - Fuel system
  - Hydraulic system
  - Pneumatic system
  - Electrical system
  - Oxygen system
  - Environmental control system
  - Anti-icing and de-icing system
  - Navigation and guidance system
  - Communication system
  - Fire control system
- Selection of structural arrangement, type of structure and manufacturing breakdown

3.9 Aircraft Architecture Trade Studies

The S18 aircraft program conducted several trade studies to analyze different methods to decelerate the aircraft on the ground. See section 4.3 of ARP4754A/ED-79A, which discusses selecting the appropriate grouping of aircraft functions to be implemented by each system within the aircraft architecture. The function “Decelerate the aircraft on the ground” has two sub-functions allocated between the brake system and thrust reverser: “Provide Primary Stopping Force (stopping on the runway)” and “Provide Secondary Stopping Force”. One trade study (S18 TS-001) looked at only using braking system (i.e. eliminate thrust reverser system) to implement the “Provide Primary Stopping Force” and “Provide Secondary Stopping Force” functions.

Trade Study	Implementing System	Provide Primary Stopping Force	Provide Secondary Stopping Force
S18 TS-001	Braking System (Only)	X	X
	Braking System	X	
	Thrust Reverser		X

FIGURE 8 - TRADE STUDY

For safety reasons, it was decided to not rely solely on brakes to implement the “Provide Primary Stopping Force” and the “Provide Secondary Stopping Force” functions. The trade study determined that brakes and thrust reverser are the optimal solution for the S18 aircraft. These two systems will become part of the S18 aircraft basic architecture.

(Editor’s Note: A detailed example of trade study methodology is beyond the scope of this example. The purpose is to highlight that the design process involves many iterations).

3.10 Preliminary Aircraft Safety Analysis (PASA)

Decomposing the top level function Decelerate Aircraft on the Ground identified the following functions which require functional independence:

- Provide Primary Stopping Force
- Provide Secondary Stopping Force

The PASA assessed how failures can lead to the associated functional hazards of the aircraft FHA by identifying the elements and interactions that contribute to the relevant failure conditions. Following are the outputs of the PASA outlining how the aircraft FHA requirements will be achieved.

Generally speaking only multi-system Failure Conditions identified in aircraft FHA should be allocated to PASA for further aircraft level studies in order to determine requirements at system level. Single system Failure Conditions identified in the aircraft level FHA can be directly allocated to system FHA without additional PASA activity

(Editors Note: The PASA activity was conducted in accordance with the guidance of ARP4761A Appendix B).

3.10.1 System Probability Allocations

The PASA in Figure 9 shows, at the aircraft level, what systems are involved in the catastrophic failure condition, namely brakes, thrust reversers, and spoilers. The aircraft level fault tree gives a preliminary set of failure conditions and associated requirements to consider for each system involved in the failure condition. For more information on FTAs, refer to ARP4761.

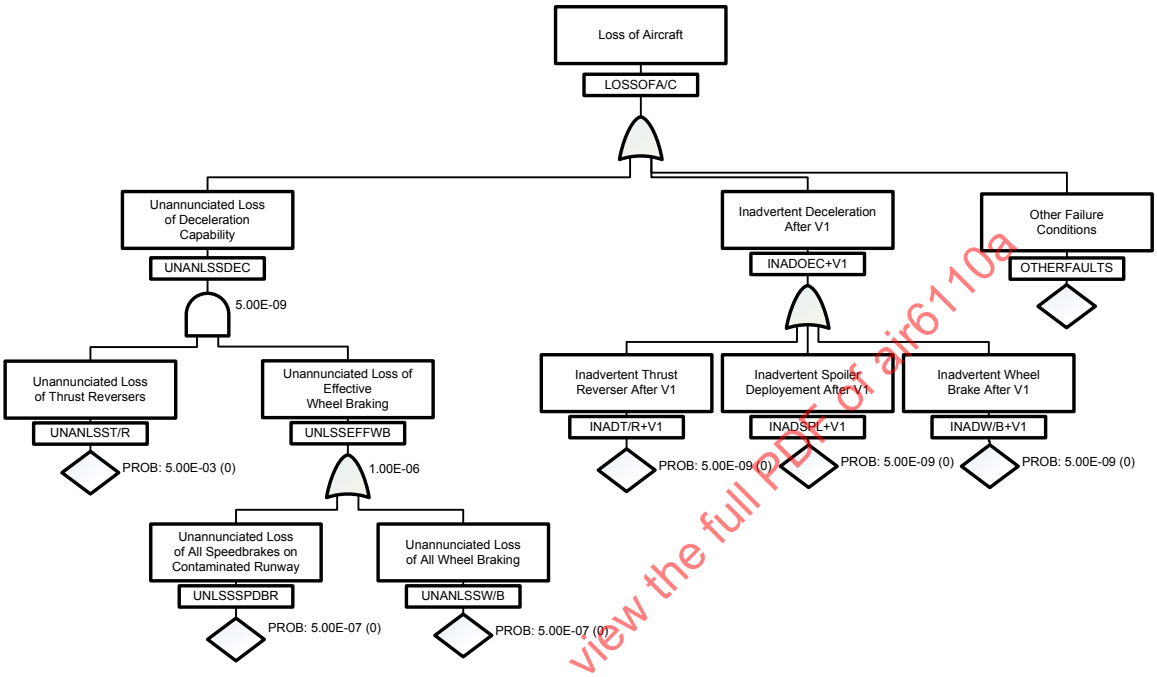


FIGURE 9 - PASA: SYSTEM PROBABILITY ALLOCATIONS

(Editor's Note: This is only a subset of the complete list of failure conditions. As one example, non detected Inadvertent deceleration before V1" would have to be considered. This failure condition can lead to an over run at high speed in case of rejected take off at V1 or to a landing gear retraction with very hot brake and risk of tire explosion in the landing bay and fire).

3.10.2 Aircraft Functional Development Assurance Level (FDAL) (Documented in PASA)

The Functional Hazard Assessment is conducted as part of the safety assessment process described in ARP4761. The outputs of the ARP4761 FHA process, which provide inputs to the ARP4754A/ED-79A process, are the failure conditions, effects, classification and safety objectives. This information is used to determine the Development Assurance Levels, as part of ARP4754A/ED-79A.

(Editor's Note: The aircraft level FHA and associated PASA fault trees give a preliminary set of failure conditions and associated requirements to consider at the system level. This example only summarizes parts of the FHA. This section only talks about the Functional Development Assurance Level assignments. For more information on Functional Hazard Assessments, refer to ARP4761).

Following the guidance of ARP4754A/ED-79A section 5.2, the aircraft functions are assigned development assurance levels that will be applied to the various development processes associated with each function.

The required FDAL for the function Decelerate Aircraft on the Ground is derived directly from the PASA as shown in Figure 6, following the criteria in Table 5.1 of ARP4754A/ED-79A. The aircraft FHA (see Figure 10) shows that the function Decelerate Aircraft on the Ground has a catastrophic event: Unannunciated Loss of Deceleration.

This fact leads to the following requirement:

The function “Decelerate Aircraft on the ground” shall be developed using a development assurance level of A as described in SAE ARP4754A/ED-79A.

(Editor’s Note: Though not shown in this example, the rest of the top level functions were evaluated using the same process. This FHA is not complete. Additional rows may be included for degraded deceleration capability but are beyond the scope of this example).

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification	FDAL
Decelerate Aircraft on Ground	Loss of Deceleration Capability	Landing, RTO, Taxi	See Below				
	a. Unannunciated loss of Deceleration Capability	Landing, RTO	Crew is unable to decelerate the aircraft, resulting in a high speed overrun	Catastrophic		S18 Aircraft Fault Tree	A
	b. Annunciated loss of Deceleration Capability	Landing	Crew selects a more suitable runway, notifies emergency ground support, and prepares occupants for runway overrun.	Hazardous	Emergency landing procedures in case of loss of stopping capability	S18 Aircraft Fault Tree	B
	c. Unannunciated loss of Deceleration Capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles.	Major			C
	d. Annunciated loss of Deceleration Capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.	No Safety Effect			E

FIGURE 10 - AIRCRAFT FHA UPDATED WITH FDAL ASSIGNMENT

3.10.3 Systems Interactions

This example focuses on the braking system, but there are interactions with interfacing systems that require integration activities to avoid surprises due to these interactions. For the sake of brevity, these interactions are not discussed in detail. Some examples are provided here.

- It is typical that the power plant, the thrust reverser, the brakes and the spoilers all need a robust air-ground indication, but may be constrained not to use the same sources, and typically may not use any one source, because of availability. With only a few available sources, it can be a challenge to avoid common modes. Not all of the sources transition at the same time during the landing, and the desired air-ground indication for some functions may or may not have to transition before others (e.g. thrust reversers may be deployed well before ground spoilers).

- There are also functional interactions (e.g. brakes will be ineffective unless the ground spoilers have already deployed, which must also be accounted for).

- For systems in general, the significance of data on system data buses requires close coordination. It can happen that a data item labeled "PAMB" on an engine bus is taken to be the engine's value, and the value taken and used to validate the air data signal. Careful review is required to ensure that the value used is not the same air data signal from the aircraft, meaning that the two values being used to vote were the same value, completely defeating the purpose of a cross check.

- Electrical or Hydraulic Power can become an undetected common mode. Besides the obvious loss of the systems powered by a power source that has failed, loads may be shed on the remaining buses, and probes which are still being read may not be anti-iced.

The general process to identify and resolve these problems is for partner personnel to create interface control documents, identifying and describing the analog, digital, power and physical interfaces between systems, subsystems and the aircraft. In addition to the characteristics of the signals, the purpose, and uses of the signals should be described. Intellectual property issues and access control should be solved such that it is easy to put the necessary information in the document.

Development of the interface definition should begin as early in the development process as possible and captured in the Interface Control Document (ICD). At early stages of the development, such as evaluating the aircraft architectures, the ICD does not need to contain a lot of information, but the information should be correct, kept current, and controlled. As the development progresses, the interface definition will become more detailed. The process of making changes to ICDs should be rapid and should make all parties to the ICD aware of a proposed change.

Referring to Figure 11 below, the functions and hazards flow down to systems; signals are identified as necessary to perform these functions on the ICDs. Integrators at both the aircraft and systems level study the signal usage for common modes or other problems. The systems are iterated until all common mode events/interactions have been accounted for. Failures should be considered at this stage at least down to the level of limited time dispatch.

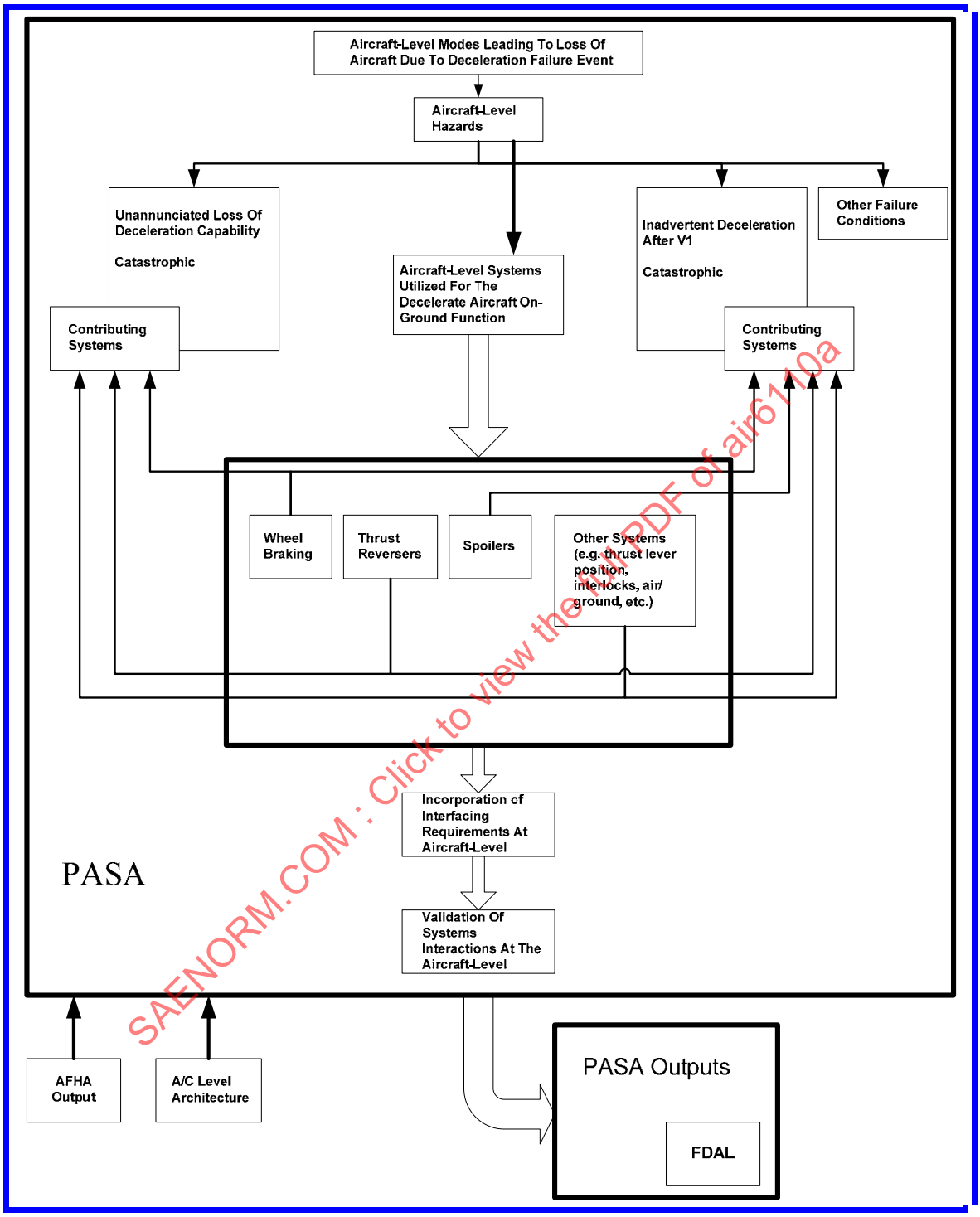


FIGURE 11 - SYSTEMS INTERACTIONS

3.10.4 Safety Derived Requirements from PASA/Aircraft FHA

The following requirements are derived from following the ARP4761 safety assessment processes.

Requirement #	Type of Req	Description	Rationale
S18-ACFT-R-0835	Safety	The S18 aircraft shall provide Flight Crew notification for failure conditions which could result in a runway excursion (loss of directional control, loss of speed control, loss of directional/speed control, or asymmetric loss of directional control)	Required to show compliance to Aircraft S18 FHA outputs. The requirement reduces the severity of FC a of Figure 10 if the failure is annunciated - see FC b (14CFR 25.703)
S18-ACFT-R-0933	Safety	The function responsible for 'decelerate aircraft on the ground' shall be developed using a functional development assurance level of A as described in SAE ARP4754A / ED-79A.	Aircraft S18 FHA outputs and required to show compliance to 14CFR 25.1309. Reference the catastrophic failure conditions in Figure 10. Reference FC a. Inadvertent deceleration on ground during takeoff phase
S18-ACFT-R-1322	Safety	There shall be functional independence between brakes and reverse thrust functions.	PASA outputs confirmed that interactions of contributing systems could not reduce the relative importance of the braking function below the Aircraft FHA. Independence has to be confirmed as required by Section 5.2.3.1 of ARP4754A/ED-79A. Two failure conditions have been taken into account, both Catastrophic.
S18-ACFT-R-1324	Safety	The brakes and reverse thrust functions shall be developed to functional development assurance level A as described in SAE ARP4754A/ED-79A.	The failure condition that drives the more stringent requirement (inadvertent deceleration after V1) requires both brakes and reverse thrust functions to be FDAL A. It is also required to demonstrate functional independence (at level A) otherwise there is potentially a single member that could cause this effect. See Note 1 of Table 3 and sec 5.2.3.1 of 4754A/ED-79A.

FIGURE 12 - AIRCRAFT LEVEL SAFETY DERIVED REQUIREMENTS

3.11 Aircraft Requirements and Architecture Validation

The validation process of ARP4754A/ED-79A section 5.4 is continuous throughout the development life cycle. At the aircraft-level, the main goal is to ensure that the set of requirements is complete and that each requirement is correct. A critical aspect is to ensure aircraft-level requirements are both necessary and sufficient to meet the needs of operators, maintainers and certification authorities, as well as aircraft and system developers. A Validation Matrix, shown below, is used to illustrate the outcome of the validation process.

(Editor's Note: The SAE S18 team has prepared many simulations, trade studies, and analyses in order to validate the top-level aircraft requirements. For the sake of brevity, only a sample of requirements will be shown in the validation matrix, and the actual evidence articles (e.g. the simulation methods and results) will not be shown in this example).

Following the guidance of ARP4754A/ED-79A section 5.4.7.2, Validation Tracking, Figure 13 has been created to track the status of validating each requirement and the set of requirements as a whole. The reader should note that the Associated Function and the FDAL column does not imply that each requirement has a specific FDAL assigned to it. Instead, this matrix helps the validation team remember to determine whether the validation method and evidence meets the rigor required for FDAL of the associated function.

Requirement ID	Safety	Source of Requirement	Associated Function (if applicable) and the FDAL		Validation Method and Evidence	Validation Conclusion	Open Problem Report (PR)
S18-ACFT-R-0009 Aircraft shall have a means to decelerate on the ground in accordance with 14CFR 25.735	No	14 CFR Part 25	Deceleration on the ground	A	Form XXX or PR YYY	Valid	
S18-ACFT-R-0110 Aircraft shall have autobrake function	No	Business Case Trade Study			Form XXX or PR YYY	Valid	
S18-ACFT-R-0135 Aircraft shall provide an anti-skid function.	No	Business Case Trade Study			Form XXX or PR YYY	Valid	
S18-ACFT-R-0184 Aircraft shall have hydraulically-driven brake function	No	Hydraulic-Electric Braking Trade Study			Form XXX or PR YYY	Valid	
S18-ACFT-R-0185 The pilot shall be allowed to override the autobrake function.	No	14 CFR 25.735(c)(2)			Form XXX or PR YYY	Valid	
S18-ACFT-R-0835 The S18 aircraft shall provide Flight Crew notification for failure conditions which could result in a runway excursion (loss of directional control, loss of speed control, loss of directional/speed control, or asymmetric loss of directional control)	Yes	Aircraft FHA. Assumption.				To be further analyzed and confirmed during PSSA	

FIGURE 13 - AIRCRAFT REQUIREMENTS VALIDATION MATRIX (SAMPLE)

S18-ACFT-R-0933 The function responsible for “Decelerate Aircraft on the ground” shall be developed using a functional development assurance level of A as described in SAE ARP4754A / ED-79A.	Yes	FHA			Form XXX or PR YYY	Valid	
S18-ACFT-R-1322 There shall be functional independence between brakes and reverse thrust functions.	Yes	PASA. Independence requirement		A	Form XXX or PR YYY	Valid	
S18-ACFT-R-1324 The brakes and reverse thrust functions shall be developed to functional development assurance level A as described in SAE ARP4754A/ED-79A.	Yes	PASA. Independence requirement		A	Form XXX or PR YYY	Valid	

FIGURE 13 - AIRCRAFT REQUIREMENTS VALIDATION MATRIX (SAMPLE) - CONTINUED

3.12 Aircraft Systems Architecture Integration and Validation

Systems integration takes place from requirements capture until aircraft verification. System Integration activities try to identify conflicts, as early as possible, between aircraft or system level requirements or implementations which are valid and logically consistent when considered separately, but which can't both be implemented.

This may become apparent at the requirements level, for example, in the assumption of a failsafe state for a function which is safe in one flight condition, but not for another. More often, a problem will become apparent as the aircraft and system architecture are refined. In this example, all the elements which can cause aircraft acceleration or deceleration require a robust air-ground indication. It is typical that the power plant, the thrust reverser, the brakes and the spoilers all need such a robust air-ground indication, but also as a rule, are constrained not to use the same sources and not to rely on any one source. With only a few available sources, this is a challenge. With several different suppliers involved it is more challenging. Systems integration, especially among multiple suppliers, will work better if the participants can establish close working relationships and write interface control documents that adequately describe the behavior of the systems on both sides of the interface.

The CMA, ZSA, and PRA (see ARP4761) are integration activities whose outputs should flow into the formal analyses. Systems integration focuses on the physical and data interfaces between system elements.

System elements all have behavior which is required and described by specification, but may have additional behavior which is not described in the specification. There is often no specified response to incorrect inputs. Testing systems with incorrect inputs, even informally can avoid surprises. The unexpected response of one system may excite an unexpected response in a connected system, even while both systems conform to all their stated requirements. This can happen more easily with system elements at lower development assurance levels. Findings from these activities should be used to design out the unexpected behavior, or to document it in an Interface Control Document.

The S18 aircraft system architecture is considered to be complete because the following have been completed (many more considerations are listed here than have been detailed in the example):

- Aircraft systems architecture has been identified which satisfies validated aircraft requirements (mission, safety, and certification).

- Aircraft systems architecture definition includes a description of the primary attributes of a system, such as performance, size, shape, operational capability, dispatch capability, reliability, and arrangement in the aircraft.
- The architecture definition clearly defines what functions are performed by each system.
- The architecture considered the following:
    - Availability
    - Commonality
    - Cost and schedule
    - Growth potential
    - Operational capability
    - Parts obsolescence
    - Reliability
    - Retrofit
    - Arrangement in the aircraft
    - Capacity
    - Dispatch capability
    - Bonding and grounding
    - Electrical characteristics
    - Electromagnetic effects (lightning, High Intensity Radiated Fields (HIRF), etc.)
    - Environmental (temperature, humidity, pressure, vibration, exposure to fluids, fungus, air quality)
    - Flammability and toxicity
    - Flight Regime (orientation/attitude)
    - Function
    - Functional test
    - Human-machine interface
    - Integrity
    - Interchangeability and inter-mixability
    - Maintainability
    - Materials
    - Noise
    - Performance
    - Planned options
    - Regulatory requirements
    - Safety
    - Size and shape
    - Weight
    - Corrosion
- High level schematics and other high level documentation developed for the aircraft system architecture
- Preliminary routing / system separation determined, with preliminary interfaces and spatial integration coordinated.
- Analyses and simulations, as necessary, conducted to initially size hardware
    - Preliminary hazard assessment
    - Preliminary certification plan
    - Preliminary FMEA
    - Preliminary fault tree analysis
    - Preliminary Reliability and Maintainability (R&M) analysis
    - Performance analysis
    - Preliminary physical layouts
    - System specific data
- FDAL
- Etc.

4. BRAKING SYSTEM DEVELOPMENT PROCESS

4.1 Braking System Introduction

This section describes, in detail, a contiguous example of the system architecture development for the braking system. The braking system was developed to implement the “Provide Primary Stopping Force” sub-function of the “Decelerate Aircraft on the Ground” function (see 3.10). This sub-function was analyzed using all the methods and tools described in the rest of ARP4754A/ED-79A. The methodology applied here is an example of one way to utilize the principles defined in ARP4754A/ED-79A. Other formats may be used to accomplish the documentation, so long as the principles outlined in ARP4754A/ED-79A are followed.

This example shows the interrelationships between the system safety assessment, the Development Assurance Level (DAL) assignment, the systems architecture development, system requirements validation and verification, and the intra-system and inter-system interface requirements. The purpose of this section is to illustrate that development of a system architecture involves taking system functions, requirements, results of the safety assessment analyses, interfacing systems, and other activities into account.

This example contains references to documentation that a company may use to assure itself of the safety of its products. Some of these documents are submitted to the regulatory agencies for the purpose of certification (e.g. the Wheel Brake System FHA). Other documents are internal to the company and not required for certification. No implication is made that these documents should all be submitted to a regulatory agency and none should be implied. Safety and Certification are not synonymous terms. This example shows the systems engineering process as applied to the development on an aircraft, including those processes that go beyond certification requirements.

4.1.1 Braking System Description

The braking system design team developed a top-level Design Requirements Document to capture the allocation of aircraft functions to the braking system and to describe the basic system architecture. This satisfies the “Develop System-Level Functions” block in Figure 1.”

(Editor’s Note: The following excerpt is taken from the S18 Wheel Brake System (WBS) Design Requirements Document).

The S18 Wheel Brake System (WBS) is comprised of the pedal brake control system, brake hydraulic system, anti-skid and autobrake systems, brakes/wheels/tires, brake temperature monitor system, brake cooling fans, tire pressure indication system, and tire and brake monitoring system. For brevity, the example will only show certain aspects of the systems architecture in detail.

The aircraft has two main landing gear attached to the wings and a nose gear. The Wheel Brake System is installed on the two main landing gear. The nose gear wheels are un-braked.

Braking on the main gear wheels is used to provide safe retardation of the aircraft during taxiing and landing phases, and in the event of a rejected take-off. The wheel brakes also prevent unintended aircraft motion when parked, and may be used to provide differential braking for aircraft directional control. A secondary function of the wheel brake system is to stop main gear wheel rotation upon gear retraction.

Braking on the ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application.

Pedal brake application is controlled by left and right brake metering valves located in the wheel wells. The brake metering valves are operated, through cables and linkages, from toe pedals integral to the rudder pedal assembly. Differential control of the left and right brakes is available to both the captain and first officer. The parking brake handle will be used to set the parking brake system. To set the parking brake, the brake pedals must be fully depressed. The parking brake handle can be pulled up and will latch when the pedals are released. The brake system will maintain brake clamping force without further flight crew action once the parking brake has been set. The brake pedals must be depressed to unlatch the parking brake handle.

The brake pedal position is electrically fed to a braking computer. This in turn produces corresponding control signals to the brakes. In addition, this computer monitors various signals which denote certain critical aircraft and system states, to provide correct brake functions and improve system fault tolerance, and generates warnings, indications and maintenance information to other systems. This computer is accordingly named the Braking System Control Unit (BSCU).

4.2 Braking System Planning Elements

The following planning documents for the Braking System are included as separate appendices of this AIR. In practice, the plans may be combined and/or integrated with other systems.

Appendix B – Braking System Requirements Management Plan (including Braking System Requirements Validation Plan)

Other example planning documents are included at the aircraft-level (see section 2.3). In a real program all planning documents would be written at both the system and the aircraft levels as required, but in this example duplication is avoided to maintain a reasonable-sized document.

The Braking System Requirements Management Plan identifies the scope, roles and responsibilities, processes, procedures and tools to be used to manage requirements during the system development life cycle. Roles and responsibilities include program management, configuration management, customers, verification and configuration control board. Requirements management processes include identification, recording, modification, validation and reconciliation of requirements. Requirements management tools include version and change control, linking and tracing, access control and database management. High level documentation requirements and conventions are also included.

The Braking System Requirements Validation Plan outlines how requirements will be shown to be complete and correct, and how assumptions will be managed. The plan includes descriptions of the methods to be used, the data to be gathered or generated, what should be recorded (summaries, reviews, investigations), the means for timely access to validation information, how the validation status will be maintained when changes are made to requirements, roles and responsibilities for validation activities, and schedule of activities.

The Braking System Verification Plan describes the verification methods (review, inspection, analysis, test, demonstration, and service experience) used to verify that the Brake System as designed satisfies its requirements. The Verification Plan also describes the roles and responsibilities of the verification team including independence from the system development team, the sequence and schedule of verification activities, the problem reporting system,and how credit will be taken at the system level for item-level verification.

4.3 Braking System Development

4.3.1 Braking System Functions

(Editor's Note: The following excerpt is taken from the S18 Wheel Brake System Design Requirements Document).

The wheel brake system is assigned to perform the following, separate functions;

8.1 To decelerate the aircraft on ground using wheel braking
8.2 To provide directional control on the ground through differential braking
8.3 To stop the main landing gear wheel rotation upon gear retraction
8.4 To prevent aircraft motion when parked

The wheel braking function is also supported by and/or provides support to a number of functions from different aircraft systems that the analyst must identify to ensure that cross-system failure effects are not overlooked. Failure conditions associated with these interfacing functions could affect the final determination of the braking system (as well as the interfacing systems) development assurance level. The interfacing functions associated with the wheel brake system are defined as follows;

- Provide Electrical power system
- Provide Hydraulic power system
- Provide Crew Alerting (Crew warnings, alerts, messages)
- Provide Rudder/Nose Wheel Steering for directional control
- Provide Air/ground status

Figure 14 details how the braking system function “Decelerate aircraft using wheel braking” is further decomposed into its three braking system sub-functions:

8.1.1 Apply deceleration force to wheels

8.1.2 Control wheel deceleration

8.1.3 Provide brake system annunciation

Figure 14 also depicts how the aircraft level interfacing functions, “Provide electrical power” and “Provide hydraulic power”, support the braking system sub-functions. Likewise, the braking system sub-function “Provide brake system annunciation” is identified as supporting the interfacing function “Display System Annunciation” which provides crew operational awareness to braking system status.

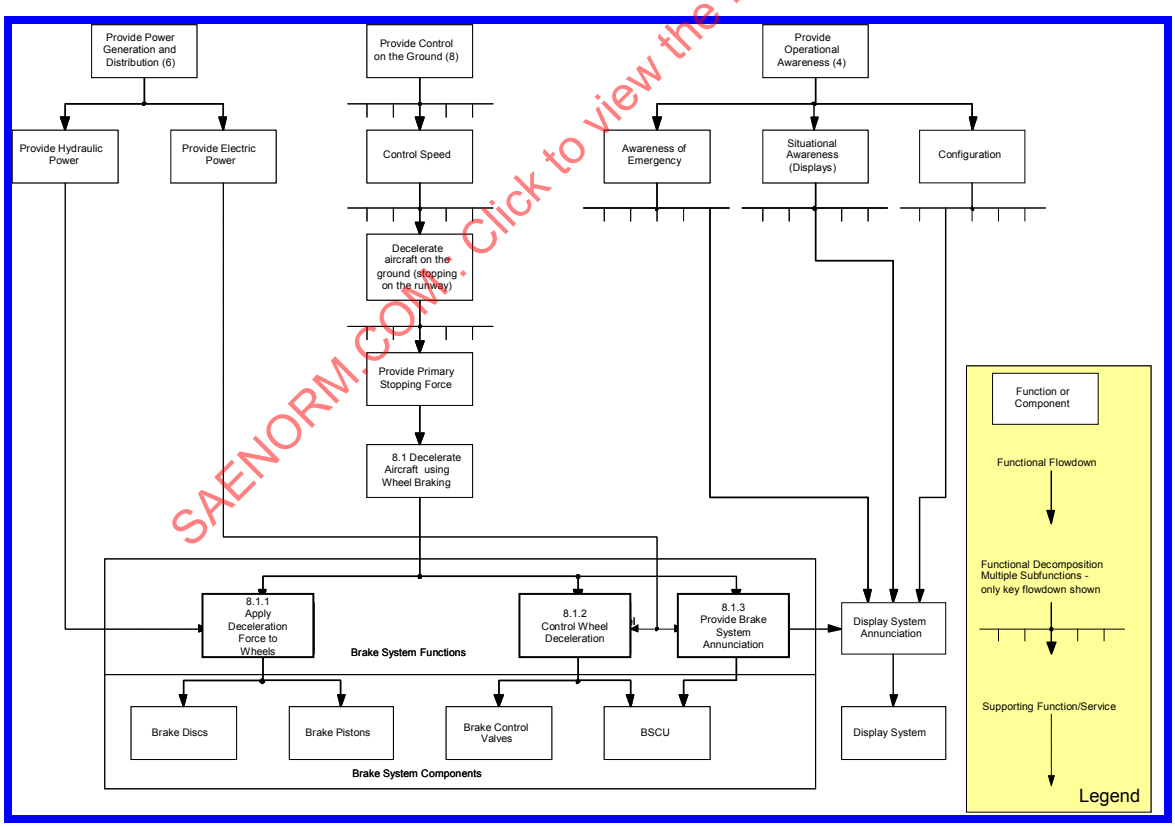


FIGURE 14 - DECOMPOSITION OF BRAKING SYSTEM FUNCTIONS

4.3.2 Wheel Brake System Requirements

(Editor's Note: Due to the complexity of the requirement capturing process as mentioned above and in section 5.3 of ARP4754A/ED-79A, not all the requirements are shown here but enough requirement sets related to deceleration of aircraft on ground function are shown to explain the process).

Initial Wheel Brake System requirements are captured by the allocation of the Wheel Brake System- related aircraft functional requirements, the derived requirements associated with these functions and the associated functional interfaces to the Wheel Brake System. The certification requirements are assigned to the Wheel Brake System either by decomposing aircraft level certification requirements or directly from the regulations. The functional safety requirements/objectives at the aircraft level are identified by the aircraft FHA and PASA where the associated functional failures are assessed. This assessment defines the aircraft requirements that are then passed down to the Wheel Brake System (See Section 3.10.4).

Figure 15 illustrates the functional and certification requirements allocated to Wheel Brake System in order to define initial system architecture for use in the safety analysis defined in ARP4761. The figure also contains design decisions from past experience and additional functions derived from the certification requirements in order to set an initial Wheel Brake System Architecture.

At this stage of requirements development the certification requirements may not be agreed upon with the certification authority. The certification requirements may be finalized after the Wheel Brake System architecture is agreed to by the OEM and applicable subcontractor.

The brake system requirement set is provided at this point in sufficient detail so that the system level FHA process can commence. For the brevity of the example, only some of the requirements related to the functions and their associated effects are shown. The requirements allocation and derivation process will continue parallel to the safety analysis.

Requirement #	Type of Req	Description	Source
S18-WBS-R-0020	Certification	Wheel Brake System shall meet 14 CFR 25.735.	FAR 25.735
S18-WBS-R-0041	Functional	Wheel Brake System shall provide directional control on ground by a differential braking function.	S18 Aircraft Requirement Specification (ref 2.5.3)
S18-WBS-R-0042	Functional	Wheel Brake System shall provide parking brake function.	S18 Aircraft Requirement Specification
S18-WBS-R-0043	Functional	Wheel Brake System shall provide autobrake function.	S18 Aircraft Requirement Specification
S18-WBS-R-0044	Functional	Wheel Brake System shall provide anti-skid function.	S18 Aircraft Requirement Specification
S18-WBS-R-0045	Functional	Wheel Brake System shall provide hydraulic brake control function.	S18 Aircraft Requirement Specification
S18-WBS-R-0047	Certification	The pilot shall be allowed to override the autobrake function.	14CFR 25.735(c)(2)
S18-WBS-R-0048	Safety	Wheel Brake System shall provide Flight Crew notification for failure conditions which could result in a runway excursion (loss of directional control, loss of speed control, loss of directional/speed control, or asymmetric loss of directional control).	S18 Aircraft FHA (ref 2.6.2)
S18-WBS-R-0049	Derived	Wheel Brake System shall be controlled and monitored by computer system called Brake System Control Unit (BSCU).	Business Case Trade Study
S18-WBS-R-0050	Derived	Each wheel brake shall have its own hydraulic circuit.	Design Architecture Decision
S18-WBS-R-0052	Derived	Each hydraulic Wheel Brake System circuit shall have metering valves, anti-skid valves and hydraulic fuses.	Design Architecture Decision
S18-WBS-R-0055	Derived	Anti-skid system shall be capable to prevent skidding of the tires by reducing the pressure applied to the brakes.	Design Architecture Decision
S18-WBS-R-0062	Derived	Wheel Brake System shall include a hydraulic accumulator to supply pressure to parking brakes.	Design Architecture Decision
S18-WBS-R-0065	Design Decision	The accumulator shall provide a minimum of 1800 PSI. (Reference Figure 38 for rationale).	Design Architecture Decision
S18-WBS-R-0122	Safety	Wheel Brake System shall be designed to preclude any common causes with Thrust Reverser System (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).	S18 Aircraft CCA

FIGURE 15 - INITIAL WHEEL BRAKE SYSTEM REQUIREMENTS (EXCERPT)

With the initial requirements set, the architecture studies and the system safety assessment process (commencing with the system functional hazard assessment) can now begin. The requirements development process is a coupled process where the system designers deriving the requirements should work closely with the safety and reliability group. The results of the requirements development and system safety assessment processes are uploaded to the requirement database simultaneously. Through the architecture development and the FHA studies the interface requirements are clarified between the Wheel Brake System and other aircraft supporting functions. Section 4.5.2 describes how these interface requirements are derived from these studies.

4.3.3 Wheel Brake System Safety Assessment Process

The Wheel Brake System safety assessment process is a critical task in the system development assurance process (see ARP4754A/ED-79A section 4.1.2) that establishes and drives system requirements from the aircraft level down to the Wheel Brake System and item level. This requires the safety analyst to ensure the failure conditions and their associated assumptions at the system level are complete and correct to gain confidence that all the critical risks have been adequately captured. The Wheel Brake System safety assessment process is iterative and dependent upon safety requirements originating at the aircraft level that lead to derived safety requirements for both the Wheel Brake System and its components.

Figure 16 depicts the inter-relationship of the Wheel Brake System preliminary safety assessment process, in the first stages of system development, with the overall safety assessment process. This diagram outlines the assessment stages undertaken and safety interfaces considered in the safety assessment process.

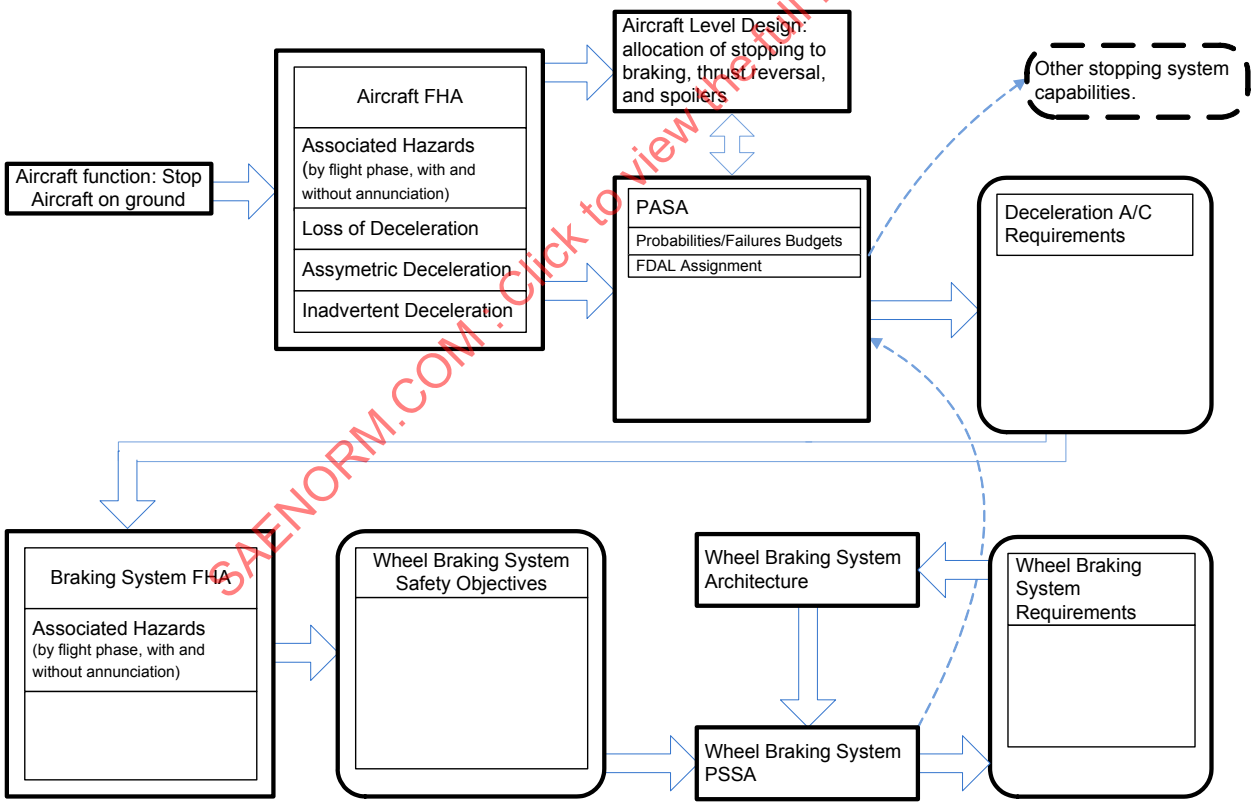


FIGURE 16 - WHEEL BRAKE SYSTEM SAFETY ASSESSMENT PROCESS

4.3.4 ARP4754A Inputs to ARP4761 System Functional Hazard Assessment Process

The functions that were developed in section 4.3.1 as part of the braking system functional decomposition in ARP4754A/ED-79A are provided as inputs to the system functional hazard assessment process in ARP4761.

4.3.5 ARP4761 Outputs from Braking System Functional Hazard Assessment

The braking system functional hazard assessment process is conducted for each of the braking system functions identified in section 4.3.1 but, as stated earlier, this example focuses on one of these functions, “Decelerate aircraft on the ground using wheel braking”. The failure conditions identification phase for this function is conducted in accordance with ARP4761, which outlines the process for discovery of all the possible failure modes and combinations of failures addressing both loss and malfunction of a function. This process is aided by an understanding of the overall system-level functional requirements, especially when the effect of a certain failure depends on the integration and interaction of another function (as may be the case when considering the effects for the interfacing functions identified in section 4.3.1). The ARP4761 assessment process is utilized to gain an understanding of all the potential failure modes, assumptions made and contributing factors influencing the effects each failure condition has on the aircraft and its occupants.

The results of the ARP4761 assessment process conducted for the system-level function “Decelerate aircraft using wheel braking” are shown in the braking system level functional hazard assessment matrix (Figure 17). This matrix lists the functional failure conditions evaluated during the assessment process and their associated hazard classification, which is the starting point for the allocation of safety requirements and the determination of the braking system development assurance level.

The above process was repeated for the remaining braking system functions identified in section 4.3.1 for completeness of the braking system functional hazards assessment matrix.

(Editor’s Note: For the purposes of this example, Figure 17 analyzes the braking system function “Decelerate aircraft using wheel braking” only. Though not shown in this example, the remaining braking system functions and the associated interface functions were also evaluated in the same manner).

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification
Decelerate Aircraft using Wheel Braking	**Total Loss of wheel braking**	**Landing or RTO**	**See Below**			
	a. Unannunciated loss of wheel braking	Landing or RTO	Crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers to the maximum extent possible. This may result in a runway overrun.	Hazardous		S18 Aircraft FTA
	b. Annunciated loss of wheel braking	Landing	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for runway overrun. The crew uses spoilers and thrust reversers to the maximum extent possible.	Hazardous	Crew procedures for loss of normal and reserve modes	S18 Aircraft FTA
	Partial Symmetrical Loss of Wheel Braking	**Landing or RTO**	**See below**			
	a. Unannunciated partial symmetrical loss of wheel braking	Landing or RTO	The crew detects the failure when the brakes are used. Crew uses available wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded brakes increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.	Major to Hazardous	Additional study required to determine classification	Potentially catastrophic – to be confirmed by analysis

FIGURE 17 - WHEEL BRAKE SYSTEM FUNCTIONAL HAZARD ANALYSIS

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification
	b. Annunciated partial symmetrical loss of wheel braking	Landing	The crew is aware that there is a partial loss of braking before landing. Crew uses wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded brakes increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.	Major		
	Asymmetrical Loss of Wheel Braking	**Landing or RTO**	**See below**			
	a. Asymmetrical loss of wheel braking – brake system failure only	Landing or RTO	Decrease in braking performance. Tendency to veer off the runway. For braking performance and brake temperature the effects are the same as partial brake loss above. The crew keeps the aircraft on the runway by using rudder at high speed and nose wheel steering at low speed. Consequences are TBD pending results of the justification studies.	Potentially catastrophic – to be confirmed by analysis	Additional studies required to determine classification.	
	b. Asymmetrical loss of wheel braking and loss of rudder or nose wheel steering	Landing or RTO	Decrease in braking performance. Tendency to veer off the runway. For braking performance and brake temperature the effects are the same as partial brake loss above. The crew cannot maintain runway centerline and results in an offside excursion.	Hazardous		S18 Aircraft FTA

FIGURE 17 - WHEEL BRAKE SYSTEM FUNCTIONAL HAZARD ANALYSIS – CONTINUED

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification
	Inadvertent wheel brake application		**See below**			
	a. Inadvertent wheel brake application without wheel locking	Takeoff before V1	The crew stops the aircraft on the runway	Minor		
	b. Inadvertent wheel brake application with all wheels locked	Takeoff before V1	Potential burst of all tires and loss of braking efficiency	Hazardous		S18 Aircraft FTA
	c. Inadvertent wheel brake application with all wheels lock ed or not locked	Takeoff after V1	Crew cannot takeoff or safely RTO resulting in high speed overrun	Catastrophic		S18 Aircraft FTA
	d. Undetected inadvertent wheel brake on one wheel without locking of the wheel	Takeoff	Crew cannot detect the failure by the asymmetry which is very small. Brake temperature can reach very high temperature. Crew retract gear resulting in possible wheel fire or tire failure.	Catastrophic		S18 Aircraft FTA
	e. Inadvertent application on one wheel without locking of the wheel coupled with detected high brake temperature	Takeoff	Crew cannot detect failure by asymmetry which is very small. Brake temperature can reach very high temperature. Crew detects high brake temperature and leaves gear extended to cool brake	Minor	Crew procedure for leaving the gear down in case of detected hot brake temperatures	

FIGURE 17 - WHEEL BRAKE SYSTEM FUNCTIONAL HAZARD ANALYSIS – CONTINUED

4.3.5.1 Summary of Wheel Brake System Safety Requirements

The completion of the Wheel Brake System FHA provides the high level safety and development assurance process requirements that are passed on as inputs and guidance to the design selection process. The Wheel Brake System safety assessment process map depicted in Figure 16 can now be populated with the system safety requirements identified to be used in the design architecture trade study process. The updated Wheel Brake System safety assessment process map is shown Figure 18.

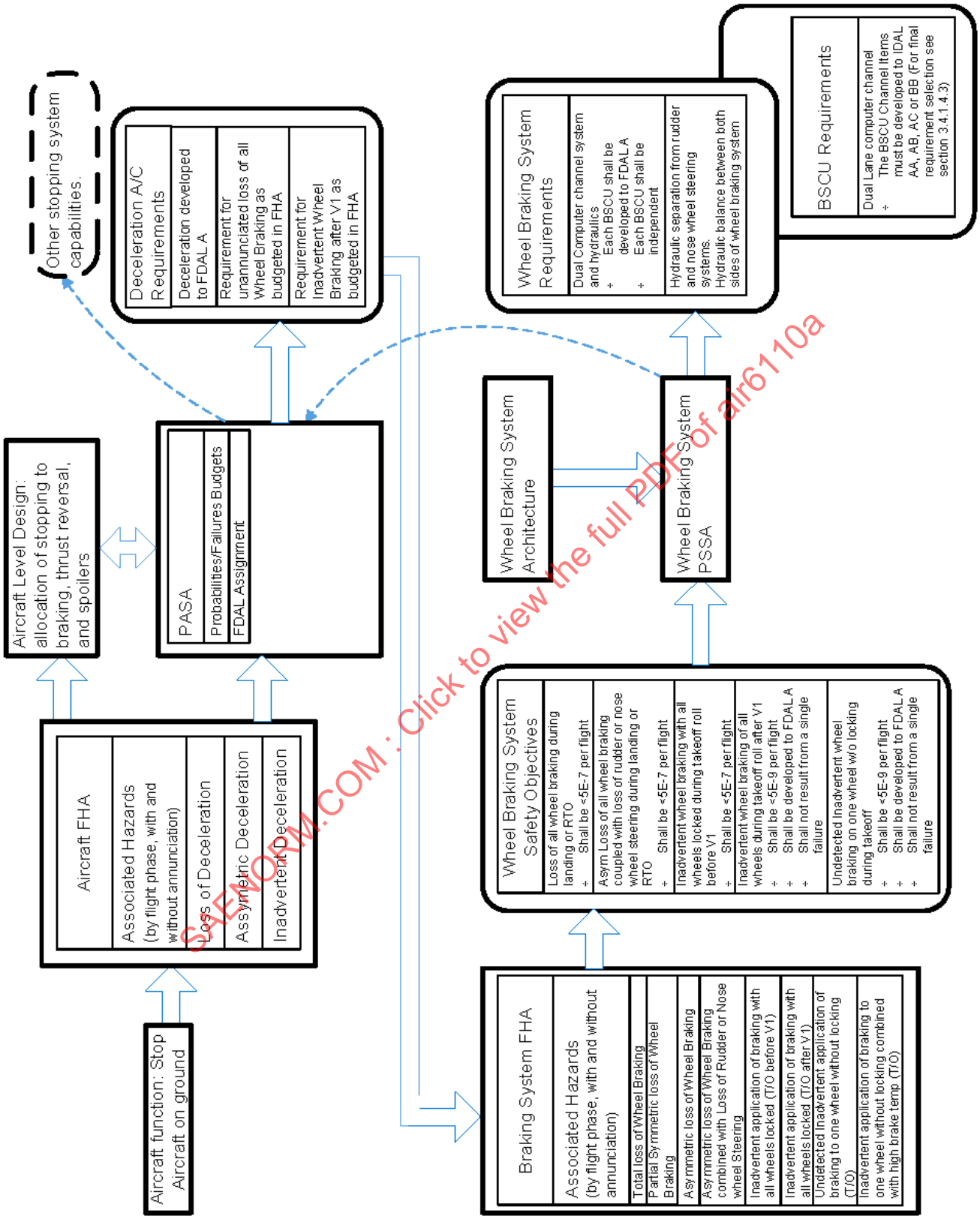


FIGURE 18 - POPULATED WHEEL BRAKE SYSTEM SAFETY ASSESSMENT PROCESS MAP

4.4 Braking System Architecture Development

(Editor's Note: This section focuses on the development of the architecture which will implement the functions for which the Wheel Brake System is responsible. The system level functions and results of the system FHA are input into this process. This process normally starts very early in the system development life cycle and is very iterative in nature. This example shows how the system architecture evolves throughout the development life cycle).

Although this section is shown prior to the system requirements section, in reality, the development of the system architecture is tightly coupled with requirements development (especially interface requirements) and is not complete until the requirements associated with the architecture have been validated.

4.4.1 Initial Architecture Concept

(Editor's Note: There is no one recommended method to capture and document the candidate system architectures. For the purposes of this example, the output of this process will consist of architecture diagrams and a system design document. Normally a system design document would include things such as a description of the system interface with other systems. Since that information is already present in other areas of this example, our system design will consist only of a high level description supported by architecture diagrams).

4.4.1.1 Preliminary System Description

When developing the initial concept for the S18 aircraft Wheel Brake System, several new technologies, such as electric brake actuation, were considered. Given schedule limitations, a high level design decision was made to implement a hydraulic Wheel Brake System architecture. The hydraulic braking system will be similar to a predecessor of the S18 aircraft, and thus most of the expertise needed to develop the braking system is already in place at SAE and leading braking system suppliers.

The system functions as shown in Figure 14 were used in conjunction with the following high level interface logic diagram, Figure 19, to help the team develop the initial architecture concept.

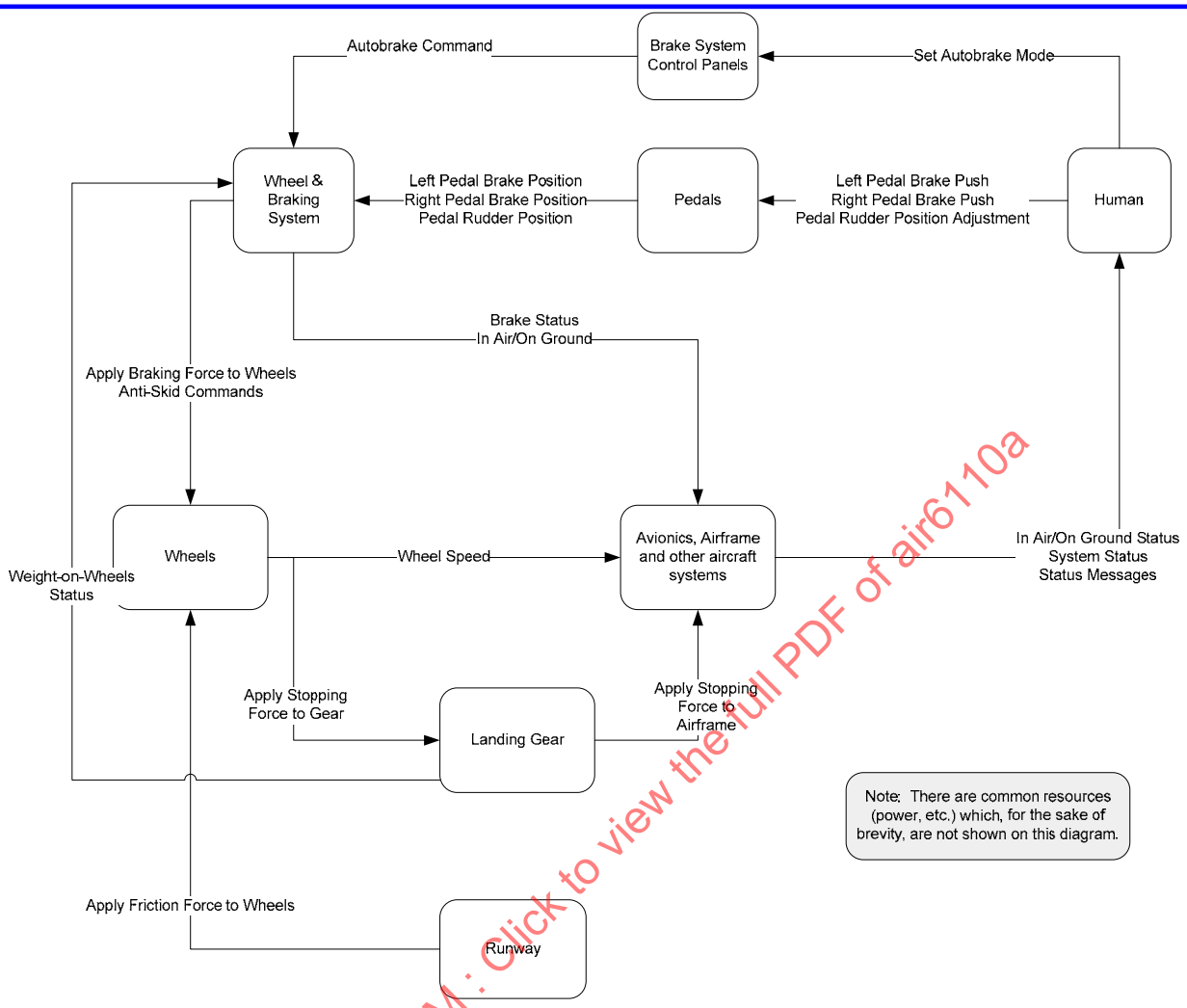


FIGURE 19 - HIGH LEVEL INTERFACE DIAGRAM

The Wheel Brake System is installed on the two main landing gear. Braking on the main gear wheels is used to provide safe retardation of the aircraft during taxiing and landing phases, and in the event of a rejected take-off. The wheel brakes also prevent unintended aircraft motion when parked, and may be used to provide differential braking for aircraft directional control. A secondary function of the Wheel Brake System is to stop main gear wheel rotation upon gear retraction.

Braking on the ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application. The Autobrake function allows the pilot to pre-arm the deceleration rate prior to takeoff or landing.

The initial Wheel Brake System architecture implementing the Wheel & Braking System block diagram in Figure 19 is shown in Figure 20. The brake pedal position is electrically fed to a braking computer. This in turn produces corresponding control signals to the brakes. In addition, this computer monitors various signals which denote certain critical aircraft and system states, to provide correct brake functions and improve system fault tolerance, and generates warnings, indications and maintenance information to other systems. This computer is accordingly named the Braking System Control Unit (BSCU).

The BSCU will be responsible for the following:

- Provide commands to control hydraulic pressure to the wheel brakes
- Anti-skid commands
- Braking commands
- Provide Brake System Annunciation for display to pilot
- Interface with other components of the Brake system
- Interface with other aircraft systems
- Provide advanced health monitoring of the brake pads and brake actuators to detect component fatigue prior to failure.

In addition to a BSCU, the Braking System will consist of:

- Shutoff Valves

The shutoff valves will respond to commands from the BSCU to apply hydraulic pressure to the braking discs.

- Metering Valves

The function of the Metering Servo Valve is to control pressure to the demanded level and to provide regulation for the Anti-Skid function.

- Gas-Charged Accumulator

The accumulator will provide an emergency reserve of hydraulic pressure. A fully charged accumulator will provide enough pressure to apply pressure for the required number of presses of the braking pedal. The accumulator will also supply pressure to the parking brake.

- Anti-Skid Valves

The Anti-Skid Valves will follow BSCU commands to control hydraulic pressure to the braking pads. These valves are used to restrict the hydraulic line pressure to the brakes in order to prevent locking of the wheels. The anti-skid system prevents wheel skids. It optimizes braking by reducing brake pressure when the pilot or autobrake system meters pressure in excess of that required to skid the tires.

- Braking Pedal

The braking pedals will provide both mechanical and electrical braking commands to the braking system. Mechanically, the pedals will be linked directly to metering valves. The braking pedals will also provide pedal force and position inputs to the BSCU. The BSCU will use these inputs to calculate commands to the shutoff and anti-skid valves.

- Wheel Brakes

The wheel brakes will provide friction force to the wheel. The brakes will also house temperature sensors which will provide brake temperature to the BSCU.

- Parking Brake

The parking brake handle will be used to set the parking brake system. To set the parking brake, the brake pedals must be fully depressed. The parking brake handle can then be pulled up and will latch when the pedals are released. The brake system will maintain brake clamping force without further flight crew action once the parking brake has been set. The brake pedals must be depressed to unlatch the parking brake handle. The parking brake has been intentionally not detailed in Figure 20 so as to not overload the schematic.

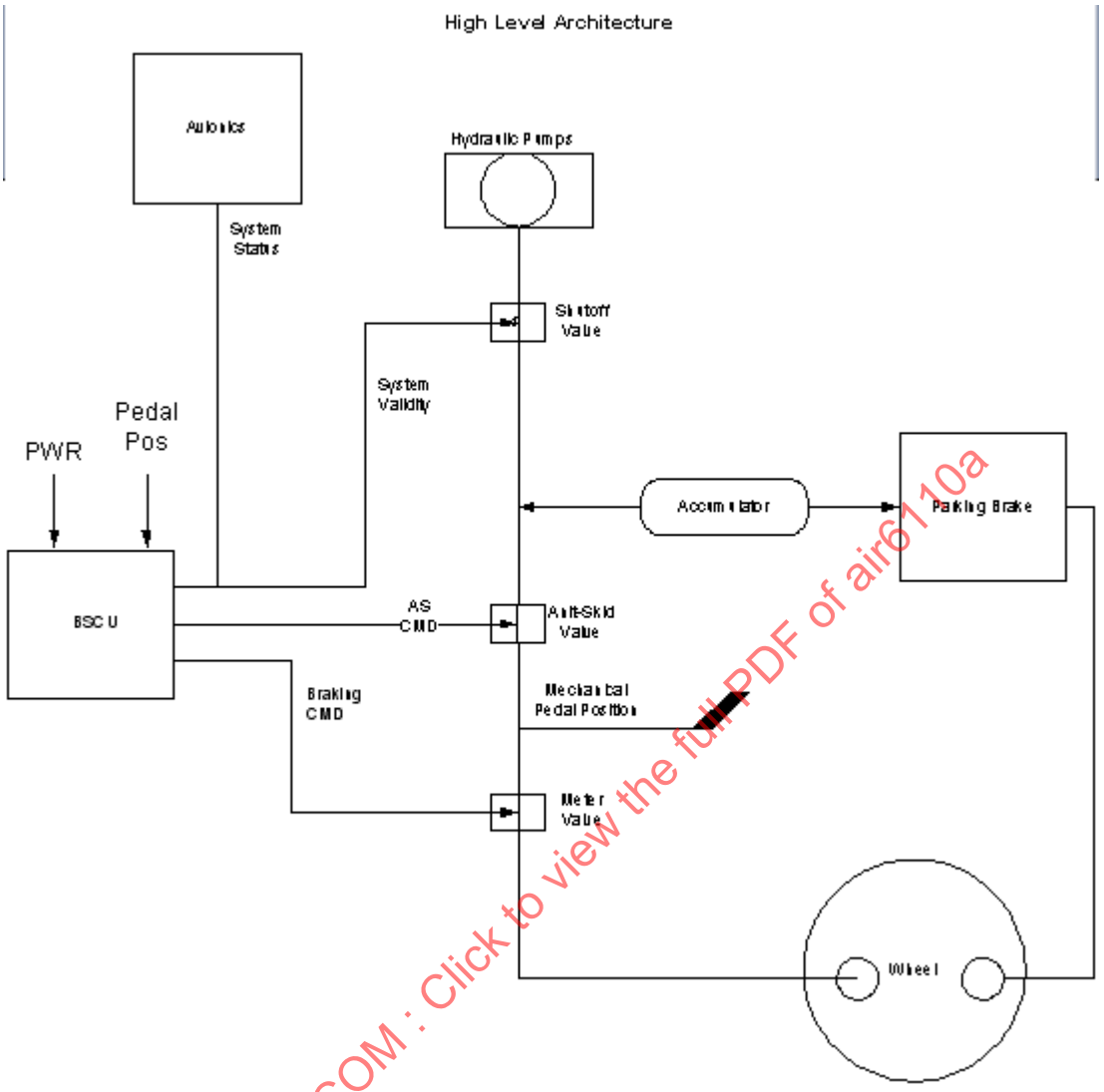


FIGURE 20 - HIGH LEVEL WHEEL BRAKE SYSTEM ARCHITECTURE

The parking brake has been intentionally not detailed in Figure 20 so as to not overload the schematic.

(Editor's Note: Now that a proposed high level architecture has been established, it must be analyzed against the system level functions, operational and safety requirements, and any design constraints that have been identified thus far).

4.4.1.2 Architectural Decisions Based on Safety Requirements

(Editor's Note: The Wheel Brake System preliminary safety assessment (PSSA) begins as soon as the SAE systems design team has an initial architecture concept. The team analyzes the initial architecture concept against the aircraft level requirements and the System and aircraft FHAs).

The paragraph below describes the feedback from this initial analysis. Though at this point there is not a formal PSSA, it is important to start documenting any design decisions which occur as a result of receiving feedback from the safety assessment process. Figure 21 lists the result of this analysis and the design decisions that the design team made based on this information:

Safety Requirement	Design Decisions	Remarks
1. Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be less than 5E-7 per flight.	More than one hydraulic system required to achieve the objective (service experience). For example, the design chosen in this example of the system design is composed of two redundant BSCUs in order to provide better availability and multimode brake operations.	The overall Wheel Brake System availability should satisfy this requirement. See PSSA FTA. (Ref. Figure 25)
2. Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing shall be less than 5E-7 per flight.	Separate the rudder and nose wheel steering system from the Wheel Brake System. Balance hydraulic supply to each side of the Wheel Brake System.	To reduce the likelihood of common causes affecting the wheel brake system, nose wheel steering and rudder systems. System separation between these systems will be shown in the zonal safety analysis and particular risk analysis.
3. Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight.	None	Requirement 4 is more stringent and hence drives the design.
4. Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 1E-9 per takeoff.	No single failure shall result in this condition. This results in the need for independent command and monitor functions in the BSCU.	None
5. Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 1E-9 per takeoff.	No single failure shall result in this condition. This results in the need for independent command and monitor functions in the BSCU.	None

FIGURE 21 - DESIGN DECISIONS BASED ON SAFETY REQUIREMENTS

As a result of the analysis, the following requirements will be added to the requirements database along with justification information from the table above:

- S18-WBS-R-0508: The wheel braking shall have at least two independent hydraulic pressure sources
- S18-WBS-R-0509: Wheel Brake System shall have dual channel BSCU and multimode brake operations to provide the required redundancy.

The system description and architecture diagram are updated as follows:

Figure 22 below depicts the new architecture (ARCH 2), which implements the design decisions in Figure 20 and the derived requirements listed above. The ARP4761 process determines that redundant BSCU systems are required in order to meet safety objectives. Things to consider for trade study include, but are not limited to:

a. Where to install two LRUs

b. Cost of two LRUs versus cost of one LRU with two systems

c. Common Mode Analysis (CMA) and Zonal Safety Analysis (ZSA)

d. How will the two systems coordinate with each other

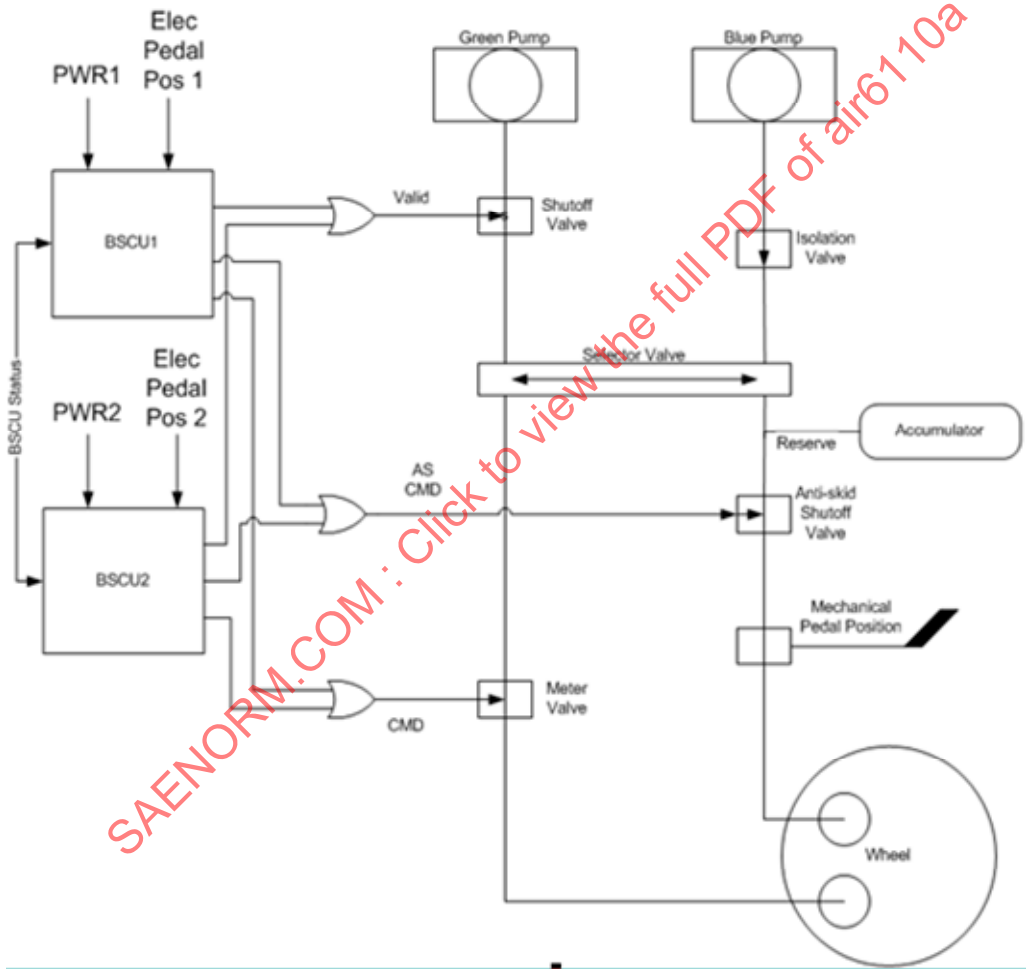


FIGURE 22 - MODIFIED BRAKING SYSTEM ARCHITECTURE ARCH 2 (DUAL HYDRAULICS, 2 BSCUS)

Modified Braking System Description

Braking on the ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application. The Autobrake function allows the pilot to pre-arm the deceleration rate prior to takeoff or landing. Autobrake is only available with the NORMAL braking system.

The eight main gear wheels have multi-disc carbon brakes. Based on the requirement that loss of all wheel braking is less probable than 5E-7 per flight, a design decision was made that each wheel has a brake assembly operated by two independent sets of hydraulic pistons. One set is operated from the GREEN hydraulic supply and is used in the NORMAL braking mode. The Alternate Mode is on standby and is selected automatically when the NORMAL system fails. It is operated independently using the BLUE hydraulic power supply and is backed by an accumulator which is also used to drive the parking brake. The accumulator supplies the ALTERNATE system in the EMERGENCY braking mode, when the BLUE supply is lost and the NORMAL mode is not available. Switch-over is automatic under various failure conditions, or can be manually selected. Reduction of GREEN pressure below a threshold value, either from loss of GREEN supply itself or from its removal by the BSCU due to the presence of faults, causes an automatic selector valve to connect the BLUE supply to the ALTERNATE brake system. An anti-skid facility is available in both the NORMAL and ALTERNATE modes, and operates at all speeds greater than 2 meters per second.

In the NORMAL braking mode, all eight wheels are individually braked from their own servo valves, which are also used to apply anti-skid. In the ALTERNATE mode, a dual metering valve provides a low pressure hydraulic braking input via four servo valves which provide the anti-skid function to four pairs of wheels. Operation of the ALTERNATE system is precluded when the NORMAL system is in use.

In the NORMAL mode, the brake pedal position is electrically fed to a braking computer. This in turn produces corresponding control signals to the brakes. In addition, this computer monitors various signals which denote certain critical aircraft and system states, to provide correct brake functions and improve system fault tolerance, and generates warnings, indications and maintenance information to other systems. This computer is accordingly named the Braking System Control Unit (BSCU). It automatically provides the following functions.

a. Takeover of manual braking (brake pedals), or automatic controls (engagement of Autobrake, autopilot commands during CAT IIIb landing)

b. Control of interfaces with other aircraft systems

(Editor's Note: Interfaces with other systems may include the hydraulic system, the brake temperature monitoring system, etc.)

c. Generation of braking commands, according to commands received and the status of the system

d. Braking regulation in order to avoid skidding of the main wheels

e. Transmission of information (indications, lights, warnings, etc.) to the flight deck and to the various aircraft computers concerning the BSCU status.

4.4.1.3 Architecture Trade Studies

(Editor's Note: There is no requirement in ARP4754A/ED-79A to perform trade studies during the development of an aircraft. However, since trade studies can often help to find and optimize solutions to design problems, the S18 Braking System Team has decided to perform one to help refine the system architecture. There are many methods and procedures for performing trade studies and ARP4754A/ED-79A does not prescribe or recommend any particular method or procedure. Therefore, we will not show the details of the trade study, instead we will show only the results and how the results were utilized to finalize the architecture with which we will continue our development. Note: the parameters in the trade study results are examples of possible parameters. The inputs to and the outputs of a real trade study will depend upon the system at hand, environment in which the development is taking place, the business, and numerous other factors).

The purpose of this section is to illustrate that development of a systems architecture involves taking system functions, requirements, business constraints, safety objectives, etc. and using these parameters to propose solutions which can then be analyzed against those parameters. There are no guidelines given in ARP4754A/ED-79A for how many architecture options to analyze or when to stop creating new architectures. The actual number of options will vary and depend on the type of system, current technologies used to implement the system, cost/schedule constraints, etc. This process should continue until a proposed architecture meets the required parameters.

Summary of Architecture Trade Study Results

(Editor's Note: Once the architecture has been selected which meets our design parameters, we can continue with the requirements development process, allocating system level requirements to system components. This architecture will continue to be analyzed and has the potential to change until the requirements have been validated. To ensure a successful development life cycle, it is important that architecture at this point is firm enough to ensure that future changes will have little or preferably no impact on other systems. Therefore the validation of interface requirements should be thorough and completed fairly early in the requirements validation process).

Figure 23 summarizes the braking system trade study. The outcome of this study is the decision to proceed with the development of Architecture 3, shown in Figure 24. This architecture consists of one BSCU which houses two independent systems. Each BSCU system has independent command and monitor channels.

S-18 Aircraft Braking System Trade Study Summary

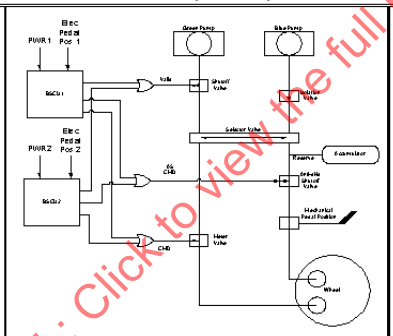
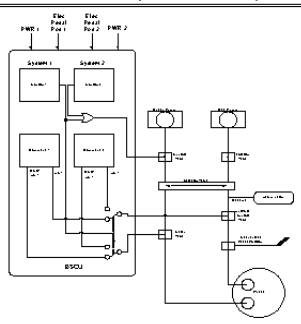
System Architecture:	**ARCH2 (2 BSCU)**	**ARCH3 (1 Dual BSCU)**
Uses the following assumptions: 1) All costs are based on system supplier rates 2) Arch 2 is based on reuse of previous S-18 aircraft braking system design.		
Cost	**ARCH2 (2 BSCU)**	**ARCH3 (1 Dual BSCU)**
OEM Cost		
Non-Recurring Cost	$X	$Y
Recurring Cost		
Price per Aircraft:	$X1	$Y1
Manufacturing per Aircraft (ROM):	$X2	$Y2
Total Recurring:	$X3	$Y3
System Characteristics	**ARCH2 (2 BSCU)**	**ARCH3 (1 Dual BSCU)**
Number of Line Replaceable Units	X	Y
System Weight in kg	X	Y
in lbs	X	Y
Power Consumption in W	X	Y
Installation Hours (Hrs)	X	Y
Difficulty of installation (1Difficult-10 easy)	3 - Note due to location of second BSCU and interconnect switches	6
Technical FAR 25.735 Compliant:	Yes	Yes
Meets Safety Objectives	Yes	Yes
Certification Risk	Low	Low
Reliability / Maintainability	**ARCH2 (2 BSCU)**	**ARCH3 (1 Dual BSCU)**
MTBF System in flight hours:	X	Y

FIGURE 23 - WHEEL BRAKE SYSTEM ARCHITECTURE TRADE STUDY SUMMARY

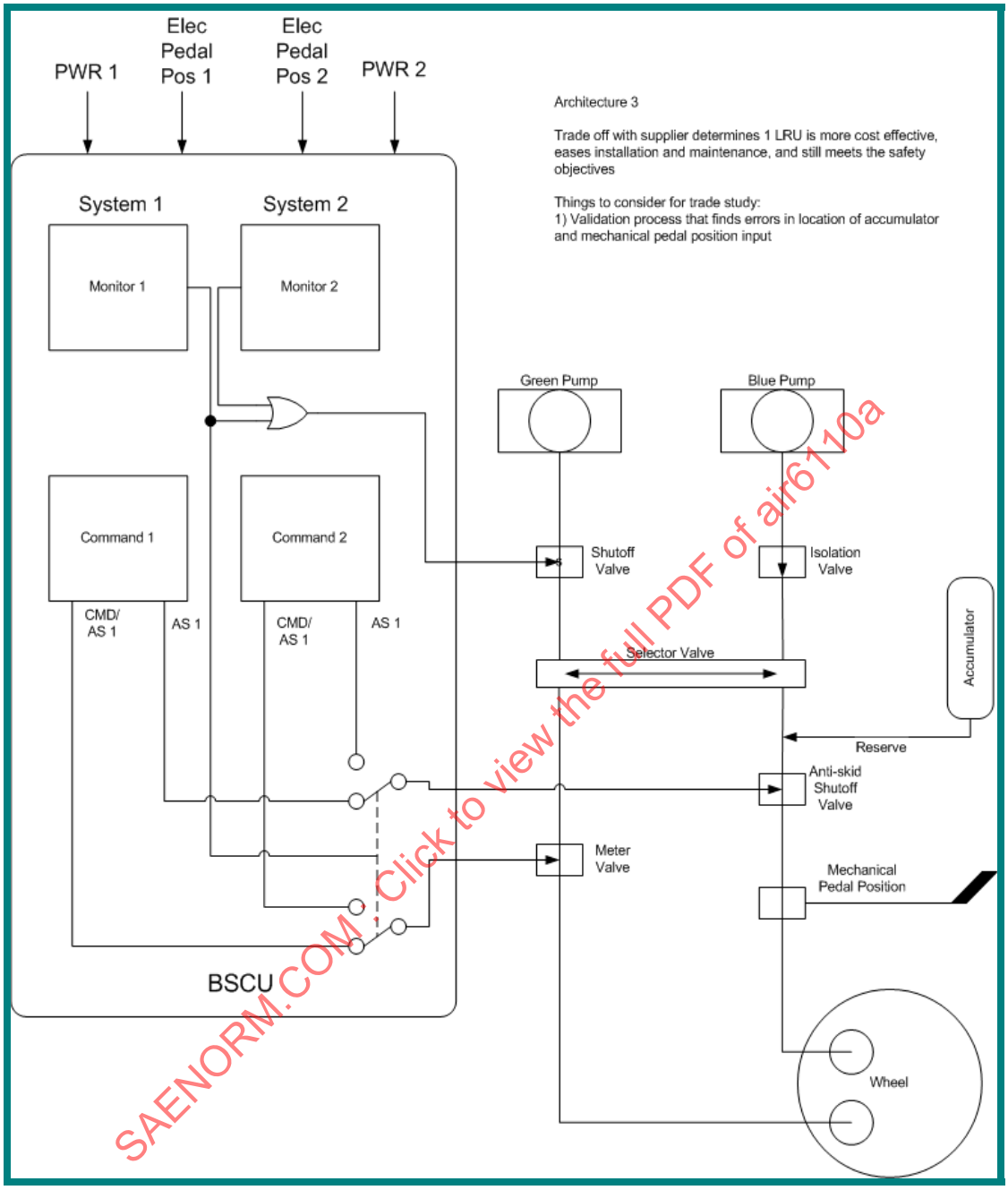


FIGURE 24 - ARCHITECTURE ARCH 3 -SINGLE BSCU WITH DUAL COMMAND/MONITOR SUBSYSTEMS

Architecture 3 will be carried forward for the rest of this example.

4.4.1.4 Wheel Brake System (ARCH 3) Preliminary System Safety Assessment (PSSA)

The Wheel Brake System PSSA is a compendium of the assessments and analyses performed during the concept and preliminary design phases of the Wheel Brake System. The elements entered into the PSSA process included a complete list of the initial safety requirements derived from the aircraft level and Wheel Brake System FHA's and common cause analyses, details from the design proposals that were reviewed to satisfy these requirements and assessment of the design decisions undertaken for establishment of derived safety requirements for systems and installations.

The design proposals presented during the design review process are detailed in section 4.4.1.1. The significant architectural changes resulting from this review that were fed into the PSSA process are as follows:

- Provide two means of applying wheel brakes by requiring normal and alternate braking system paths
- The normal and alternate brake system will meet the requirements without any reliance on the emergency braking system
- Determined that the system safety requirements could be satisfied utilizing two, separate BSCU channels contained within a single BSCU.

4.4.1.4.1 Fault Tree Analysis for the Wheel Brake System Architecture (ARCH3)

(Editor's Note: This section would normally contain the fault trees for all significant failure conditions. This example shows the evaluation of "Unannunciated loss of all wheel braking" only. The fault tree analysis approach only was used for this example).

The fault tree depicted in Figure 25 reflects the design proposal selected which incorporates the significant architecture changes stated above. The fault tree identifies the initial allocations of probability budgets to each of the three system operating modes (normal, alternate and emergency braking) with the normal mode given the most stringent allocation. The analyses performed confirmed that the derived safety requirements for the Wheel Brake System are satisfied with the architecture proposed.

4.4.1.4.2 FDAL Assignment for Wheel Brake System Functions

Following the guidance of ARP4754A/ED-79A section 5.2, the Wheel Brake System functions are to be assigned functional development assurance levels that will be applied to the various development processes associated with each function. The required FDALs for the braking system functions were derived directly from the braking system FHA (see Figure 17).

The braking system FHA output shows that the function "Decelerate aircraft using wheel braking" has the most severe failure condition resulting in a catastrophic event for the following conditions:

- Inadvertent wheel brake application with all wheels locked or not locked, or
- Undetected inadvertent wheel braking on one wheel without locking the wheel

As a result, the Wheel Brake System functions responsible for decelerating the aircraft while on the ground shall be developed using a functional development assurance level of A.

The remaining functions that are part of or interact with the Wheel Brake System function as depicted in Figure 14Figure are assessed separately to determine their respective FDAL assignments. The individual FDALs are inputs to the PASA to confirm they match their respective aircraft-level function relative importance (aircraft-level FDAL) as depicted in Figure 10. Following validation of FDAL of the system-level function at the aircraft-level, the braking system functions FDALs are used in further development of the Wheel Brake System Preliminary System Safety Assessment:

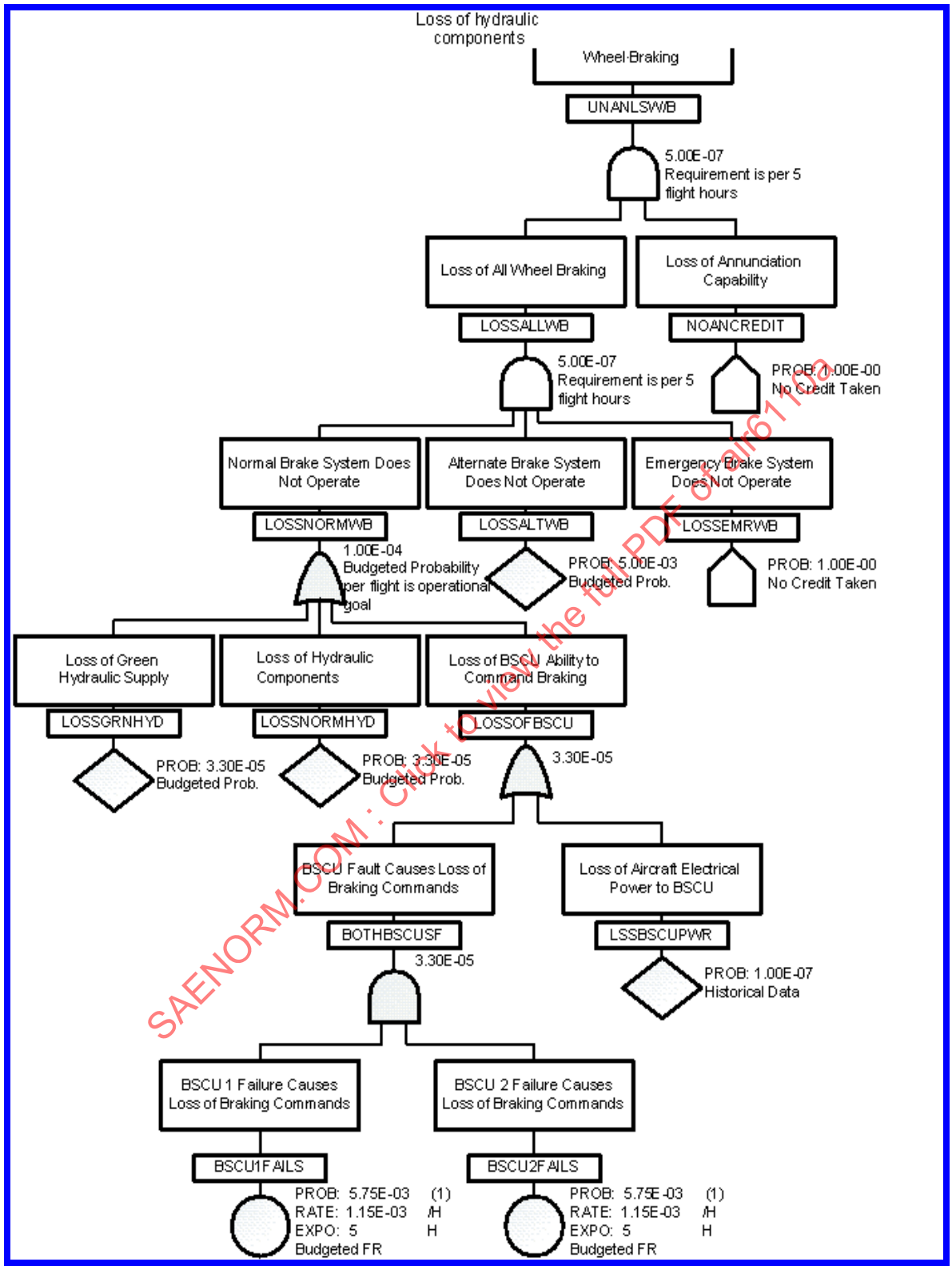


FIGURE 25 - FAULT TREE FOR “UNANNUNCIATED LOSS OF ALL WHEEL BRAKING”

4.4.1.4.3 Wheel Braking Sub-System (BSCU) Requirements

From the requirements identified at the aircraft level and Wheel Brake System FHAs and through the analyses carried out during the PSSA process, lower level derived safety requirements are identified and passed down for assessment at the BSCU sub-system level. For the braking system architecture selected, the lower level derived safety requirements are input to the Wheel Brake System requirements, resulting in a reassessment of the system architecture as depicted in Figure 26. The reassessment confirms the proposed design satisfies the lower level safety requirements identified.

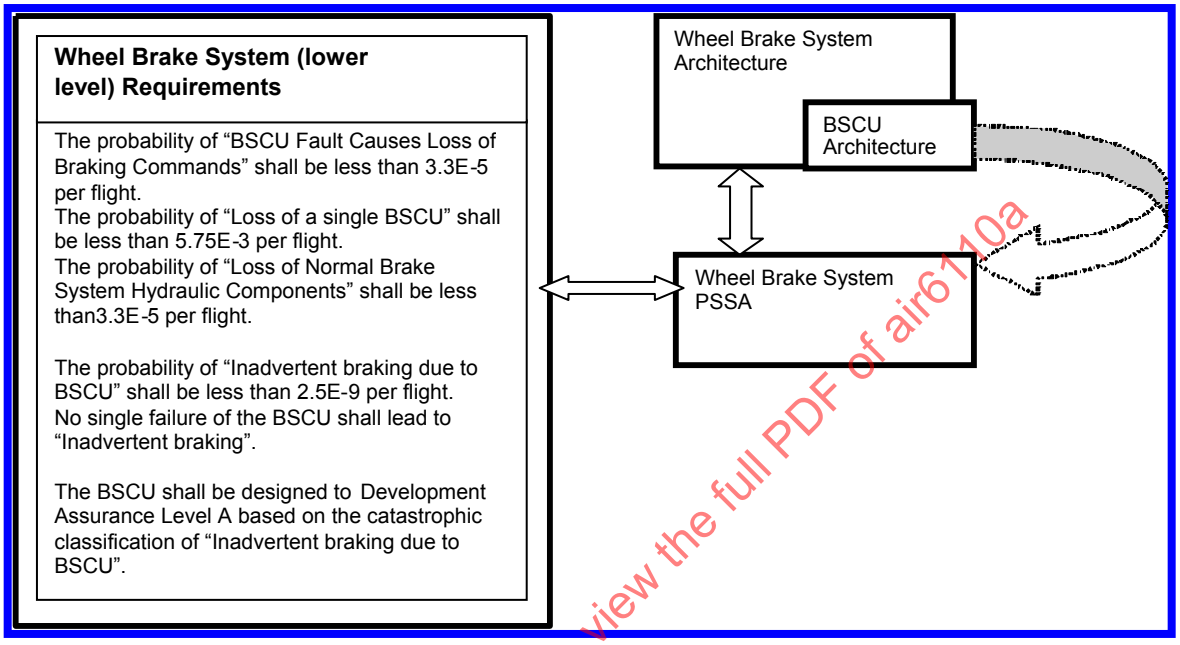


FIGURE 26 - WHEEL BRAKE SYSTEM DERIVED (LOW-LEVEL) SAFETY REQUIREMENTS

Figure 26 identifies the link back from the BSCU architecture to the wheel braking PSSA process. Thisindicates the reassessment activity required for the architectural decision, which was made late in the design process, to utilize a single, dual channel BSCU to meet the Wheel Brake System safety requirements.

4.4.1.4.3.1 Fault Tree Analysis Results for the Wheel Brake System Control Unit (BSCU)

(Editor's Note: This section contains the fault trees for the significant failure conditions associated with the BSCU only. Relevant fault trees for the remaining components of the wheel brake system were also prepared but not shown in this example. The fault tree analysis approach only was used for this example.)

The fault tree depicted in Figure 27 reflects the assessment performed specifically for the dual channel BSCU design (ARCH 3) selected in section 4.4.1.3 above. The analysis performed confirmed that the proposed architecture reasonably satisfied the derived safety requirements for the wheel brake system at the item level. Figure 27 shows that the actual predicted failure rate for "BSCU Fault causes loss of Braking Commands" is 1.5E-6 per flight, whereas the requirement in Figure 26 for this event, which derives from the fault tree in Figure 25, is 3.3E-5 per flight.

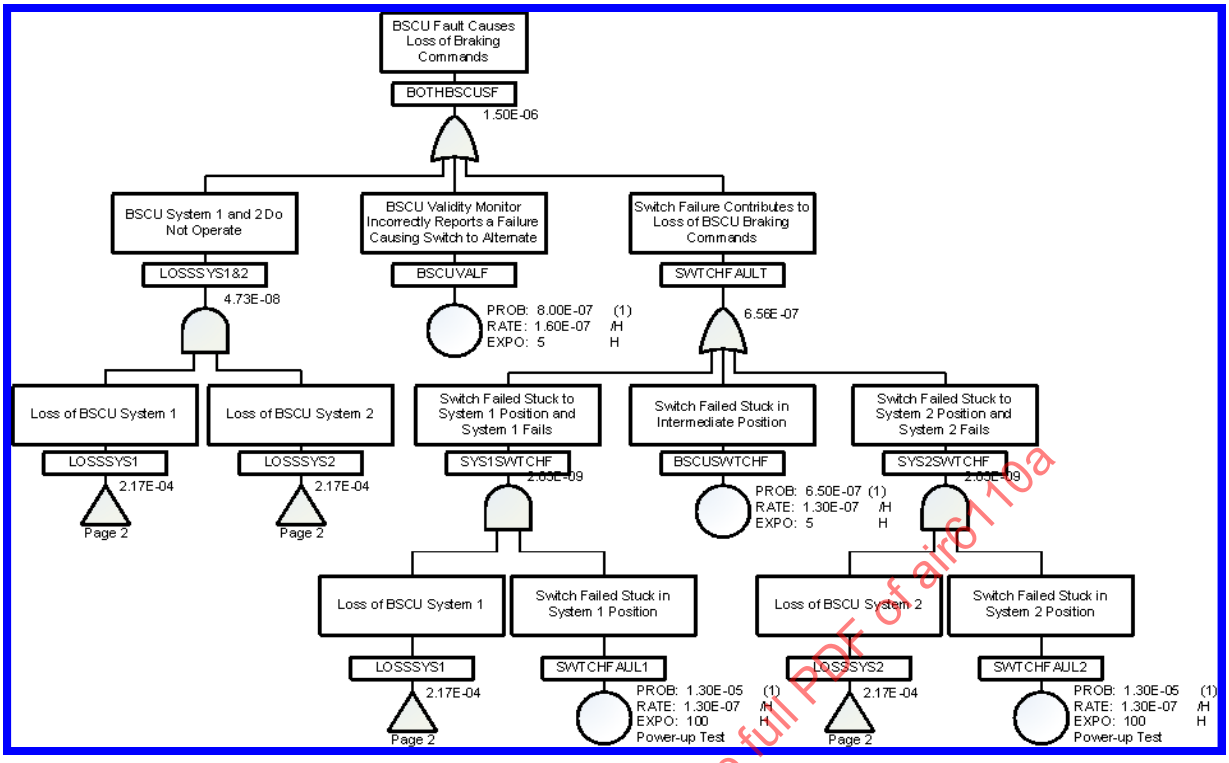


FIGURE 27 - FAULT TREE FOR DUAL-CHANNEL BSCU

(Editor's Note: Expansion of the fault tree was carried out but not included for brevity.)

4.4.1.4.3.2 BSCU Hardware and Software Item-Level Requirements

The lower level PSSA process conducted for the BSCU established the relevant item level safety requirements and the fault tree analysis conducted confirmed that those requirements were satisfied for the architecture proposed. The fault tree analysis identified the set of safety requirements that would filter down and be allocated to the hardware and software elements of the proposed BSCU design that must be satisfied in order to meet the overall safety objectives. Figure 26 outlines these key safety requirements derived from the wheel brake system level assessment will be allocated to the complex hardware and software items of the BSCU.

Apart from the BSCU complex hardware and software, items in the system can be considered as non-complex items and do not contain any software or complex electronic hardware. Therefore they may be considered to provide a level of confidence equivalent to IDAL A, provided they are appropriately fully tested and/or fully analyzed during the development cycle per section 5.2.3.3 of ARP4754A/ED-79A. In addition, the independent voting-selection logic shown in the final brake system architecture (Figure 24) is assigned an IDAL A as the result of assigning FDAL A to the entire BSCU (Figure 28). For the BSCU, the FDAL and IDAL assignment will be performed as per Section 5.2.3 of ARP4754A/ED-79A. The chosen assignment must be valid considering all hazards that can be produced by the BSCU. For instructional purposes, only three of these hazards are detailed in this example, although the BSCU is involved in all failure conditions of the System FHA shown in section 4.3.5. These hazards are:

a. Total loss of wheel braking (annunciated) at Landing, which is HAZARDOUS;

b. Inadvertent wheel brake application with all wheels locked at Takeoff after V1, which is CATASTROPHIC;

c. Undetected inadvertent wheel braking on one wheel without locking of the wheel at Takeoff, which is CATASTROPHIC.

For each one of those failure conditions the Functional Failure Sets (FFS) involving the BSCU channels have to be identified. Fault trees can be used as a tool to identify the FFSs, but caution is required as the FTA would identify the two BSCU channels as separate elements of a cut set.

The item level IDAL's determined from ARP4761 PSSA process are shown in Figure 28, below, and are used as an input to the software development assurance processes of DO-178/ED-12 or the electronic hardware assurance processes of DO-254/ED-80.

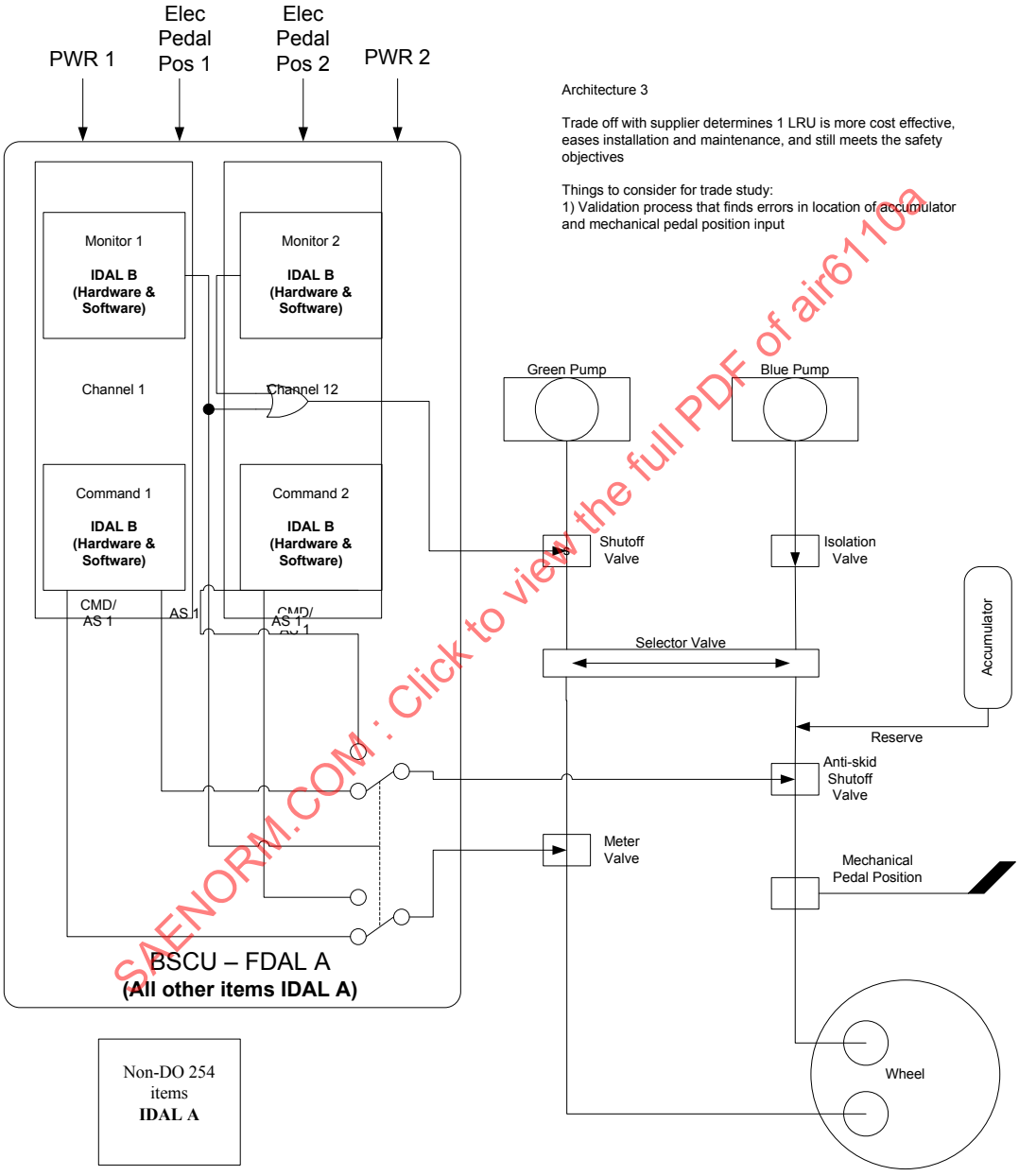


FIGURE 28 - IDAL DETERMINATION FOR BSCU

The following derived requirement was added at the BSCU level for IDAL determination:

- Item Development Assurance Level Requirements

  Complex hardware and software development for the BSCU shall be performed to an item development assurance level of at least level B for both channels, or to level A for one channel and at least level C for the other channel. (Hardware in common to both channels (e.g. voting) remains at level A.). The BSCU Safety Assessment identified that sufficient independence attributes exist to implement the system in either manner. (Case 2 in ARP4754A/ED-79A Section 5.2.3.2.3.2).

  Item Development Independence between each channel/Com-Mon shall be validated and verified to FDAL A.

The design team chose to develop the independent command and monitor in each channel to IDAL B as shown in Figure 28.

4.4.1.4.4 Derived Requirements Identified From PSSA

In addition to the wheel brake system item requirements, there are derived requirements identified from the PSSA that are to be assessed separately in the overall system safety assessment plan and include the following:

- Installation Requirements

  (i) The primary and secondary hydraulic supply systems are to be segregated or sufficiently separated and verification done in Zonal Safety Analysis and Particular Risk Analysis (ref. ARP4761).

  (ii) BSCU system 1 requires a source of electrical power independent from the source supplied to the BSCU system 2.

(Editor's Note: Additional installation requirements are developed from the fault trees but they are not shown here for brevity).

- Requirements on Other Systems

  An additional safety requirement has been identified in the wheel braking PSSA, which affects/poses a constraint on another system: "Loss of Green Hydraulic supply to the Normal brake system" shall have a probability less than 3.3E-5 per flight." This requirement is carried over and included in the hydraulic system safety assessment process.

(Editor's Note: Additional requirements on other systems are developed from the fault trees but they are not shown here for brevity).

- Safety Maintenance Requirements

  It was determined that a maintenance task to functionally check for latent failure of the ALTERNATE braking mode is necessary in order to satisfy the wheel brake system safety requirements. An Exposure time of 14,750 hours was budgeted for latent switch failures as this is the maximum exposure time which allows the top level probability requirement to be met.

(Editor's Note: Additional maintenance requirements may be developed from the fault trees but they are not shown here for brevity).

(Editor's Note: At this point in the example, it is assumed that the PSSA is sufficiently developed to enable detail design implementation).

4.5 Braking System Requirements Capture

4.5.1 Derived Braking System Requirements

(Editor's Note: The following requirements were captured from the Systems FHA and implemented to the requirements database. The requirements for a failure condition to be extremely remote or extremely improbable follow from the assignment of failures in the FHA as hazardous and catastrophic, respectively).

The safety assessment, reliability and the design team discussions about the above requirements resulted in a new architecture. The BSCU supplier declared that the past experience of the BSCU design shows that the failure rate of a single control system cannot satisfy the safety objectives of the system FHA. In response to the BSCU declaration, the Braking System supplier documented this change in Coord Memo S18 CM00XX. The following requirements are inserted into the Braking System specification.

Requirement Number	Type of Req	Description	Source
S18-WBS-R-0508	Derived Safety	The wheel braking shall have at least two independent hydraulic pressure sources	Coord Memo S18a-CM00XX
S18-WBS-R-0509	Derived Safety	Wheel Brake System shall have dual channel BSCU and multimode brake operations to provide the required redundancy.	Coord Memo S18a-CM00XX
S18-WBS-R-0510	Derived Safety	The rudder and nose wheel steering functions shall not be implemented by the wheel brake system.	Coord Memo S18a-CM00XX

FIGURE 29 - BRAKING SYSTEM SPECIFICATION

The above requirements imposed a new architecture and the architecture trade studies continued until all the requirements were validated.

The following requirements apply to the new architecture with a dual channel BSCU and two hydraulic systems as described in Section 4.4.1.2. Within the new architecture, new requirements are inserted to the database from safety assessments, certification requirements and design decisions.

Requirement #	Type of Req	Description	Rationale
S18-WBS-R-0631	Certification	Wheel Brake System shall indicate individual wheel temperature	14CFR 25.735.j
S18-WBS-R-0632	Certification	Wheel Brake System shall control individual wheel pressure	14CFR 25.735.j
S18-WBS-R-2971	Design Decision	Wheel brake system shall have one NORMAL operating mode	
S18-WBS-R-2972	Design Decision	Wheel brake system shall have one ALTERNATE operating mode	
S18-WBS-R-2973	Design Decision	Alternate system operation shall be precluded during normal operation	
S18-WBS-R-2974	Design Decision	An accumulator shall be used to back up ALTERNATE brake system operation.	
S18-WBS-R-2984	Safety	The normal and alternate operating modes shall be designed to mitigate any common threats (e.g. tire burst, tire shred, flailing tread, structural deflection).	S18 WBS PSSA
S18-WBS-R-2985	Safety	The normal and alternate operating modes shall be designed to preclude any common mode failures (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).	S18 WBS PSSA
S18-WBS-R-2986	Safety	The BSCU shall be designed to Functional Development Assurance Level A.	S18 WBS PSSA
S18-WBS-R-2997	Safety	The BSCU shall have two independent command channels.	S18 WBS PSSA

Requirement #	Type of Req	Description	Rationale
S18-WBS-R-3000	Safety	The IDAL allocation for BSCU Com shall be IDAL B.	S18 WBS PSSA
S18-WBS-R-2998	Safety	The BSCU shall have two independent monitor channels.	S18 WBS PSSA
S18-WBS-R-3001	Safety	The IDAL allocation for BSCU Mon shall be IDAL B.	S18 WBS PSSA
S18-WBS-R-2999	Design Decision	The BSCU shall have two independent power sources	
S18-WBS-R-3011	Design Decision	Brake pedals shall be independent from the rudder control	
S18-WBS-R-3213	Design Decision	Normal brake hydraulic system shall be powered from Aircraft's Right Hydraulic (Green Line) System	
S18-WBS-R-3224	Design Decision	Alternate brake hydraulic system shall be powered from Aircraft's Center/Reserve Hydraulic (Blue Line) System	
S18-WBS-R-3245	Design Decision	Alternate operating mode shall be automatically selected when the normal mode fails	

FIGURE 30 - WBS REQUIREMENTS FOR DUAL CHANNEL BSCU AND TWO HYDRAULIC SYSTEMS ARCHITECTURE

The above higher level requirements have to be further decomposed into the item level and interface requirements. The following sections describe some of these capturing processes.

4.5.2 Interface Requirements

(Editor's Note: The braking system must be integrated with other aircraft systems in order to be able to achieve the aircraft level function of decelerating the aircraft while on the ground. Managing the associated systems interface requirements is a critical part of the Wheel Brake System integration at the aircraft level. It is important to ensure that the Wheel Brake System is both receiving inputs required from other systems as well as providing outputs required by other aircraft systems functions. The development of associated interface requirements begins with the identification of which aircraft systems support the Wheel Brake System function (which in turn supports the accomplishment of system derived safety requirements). Likewise, those safety requirements for other aircraft functions that are supported by the Wheel Brake System are also highlighted. A thorough assessment of the associated functional failure conditions is performed during the PSSA process to gain an accurate understanding of the contribution each interfacing function lends to the Wheel Brake System functional failures assessed during the Wheel Brake System FHA process and the resultant hazard classifications. These interface details (e.g. hazard classifications, development assurance levels) are then passed back through their respective system safety assessment processes for consideration in their system development assurance process).

4.5.2.1 Wheel Brake System/Aircraft Interface Requirements (Inter-System)

The key system-to-system interfaces that were considered for the braking system are as follows:

- Hydraulics
- Electrical Power System
- Pilot Controls
- Flight Deck Displays
- Propulsion
- Proximity Sensing
- Earth Reference System
- Landing Gear Actuation
- Health Management System

The BSCU interface to the aircraft is comprised of two separate types of communication: those needed for the braking function and those needed for health monitoring. The following Wheel Brake System interface requirements were added:

Requirement #	Type of Req	Description	Rationale
S18-WBS-ICD-0001	Interface	The BSCU shall receive the following inputs from Pilot Controls: •Brake pedal •Parking brake lever •Autobrake selector switch •Thrust lever resolver angle •Fuel cutoff switch	Wheel Brake System architecture trade study
S18-WBS-ICD-0002	Interface	The BSCU shall receive the following inputs from the Propulsion system: • Thrust lever resolver angle • Fuel cutoff switch	Wheel Brake System architecture trade study
S18-WBS-ICD-0003	Interface	The BSCU shall receive the following inputs from the Proximity Sensing System: • Truck tilt (on-ground) • Speed brake lever	Wheel Brake System architecture trade study
S18-WBS-ICD-0004	Interface	The BSCU shall receive the following inputs from Earth Reference System: • Ground speed • Pitch attitude • Longitudinal acceleration	Wheel Brake System architecture trade study
S18-WBS-ICD-0005	Interface	The BSCU shall receive the following inputs from Landing Gear Actuation: • Landing gear lever	Wheel Brake System architecture trade study
S18-WBS-ICD-0006	Interface	The BSCU shall receive power from Electrical Power System.	Wheel Brake System architecture trade study
S18-WBS-ICD-0101	Interface	The BSCU shall transmit the following outputs to Flight Deck Displays: • Brake temperature • Tire pressure • Brake Pedal information • Brake pedal	Wheel Brake System PSSA
S18-WBS-ICD-0102	Interface	The BSCU shall transmit the following outputs to Health Management System: Fault reports	Wheel Brake System PSSA

FIGURE 31 - WHEEL BRAKE SYSTEM INTERFACE REQUIREMENTS

The brake system safety assessment and architecture trade studies are not the only sources of the requirements. Other aircraft systems can impose new requirements to Wheel Brake System. For example, the hydraulics system will be sized based on the required inputs for the flight control systems and the braking systems. In this example, the maximum hydraulic pressure is 2400 psi. This is a requirement imposed on the braking system. Moreover, the Wheel Brake System also imposes requirements to other systems. For example:

The following requirement has been sent to the ground spoiler system: The spoilers shall increase the ground contact force xx% at speeds greater than XXX on ICAO PCN XX/... runway surface.

4.5.2.2 Interface Requirements (Intra-System)

The following Wheel Brake System intra-system interface requirements were added for the interfaces between systems and items of the braking system:

Requirement #	Type of Req.	Description	Rationale
ARP-BRAKE-ICD-1001	Interface	The BSCU shall transmit the following to the brake actuator: • Total commanded clamping force • Brake temperature • Wheel speed	Wheel Brake System architecture trade study
ARP-BRAKE-ICD-1002	Interface	The brake actuators shall respond to a BSCU command within 5 ms of receiving it	Wheel Brake System timing analysis
ARP-BRAKE-ICD-1101	Interface	The brake actuator shall transmit the following information to the BSCU: • Total measured clamping force • Brake actuator power valid status	Wheel Brake System architecture trade study

FIGURE 32 - WHEEL BRAKE SYSTEM INTRA-SYSTEM INTERFACE REQUIREMENTS

(Editor's Note: An end-to-end timing analysis, coupled with simulations, was used to determine the interface timing constraints. This level of detail is left out for the sake of brevity).

4.5.3 Braking System Requirements Specification

The final Braking Systems Requirements Specification contains the derived requirements from the architecture development, derived Safety requirements from the PSSA and the intra-system and inter-system interface requirements.

The following table identifies the origin of these requirements (operational or safety-derived) and a traceability roadmap back to the aircraft and/or braking system level requirements, as appropriate. These requirements then flow down to the braking system and sub-systems developers as design specifications.

(Editor's Note: Due to the complexity of the requirement integrity and size, not all requirements developed for the braking system are shown. Those requirements which trace back to the aircraft requirements shown in section 3.5 or to the system-level requirements shown in section 4.5.4.1 are shown here, as well as requirements shown in the braking system validation and verification matrices).

Requirement #	SFTY	Description	Traced From	Traced to	Source
S18-WBS-R-0009	N	The wheel brake system shall be capable of decelerating the S18 aircraft to a complete stop/ to taxi speed in XXXX feet on a wet runway when wheel brakes, high lift speed brakes and reverse thrust are available, including when at maximum landing weight.	APR-ACFT-R-0010	S18-WBS-R-1613	S18 Aircraft Requirements Specification
S18-WBS-R-0020	N	Wheel Brake System shall be designed in accordance with 14CFR 25.735.	S18-ACFT-R-0009	S18-WBS-R-0631 S18-WBS-R-0632	14CFR 25.735
S18-WBS-R-0043	N	Wheel Brake System shall provide autobrake function.	S18-ACFT-R-0110	S18-WBS-R-3110 S18-WBS-R-1613 S18-WBS-ICD-0003 S18-WBS-ICD-0004 ...and others	S18 Aircraft Requirements Specification
S18-WBS-R-0049	Y	Wheel Brake System shall be controlled and monitored by a computer system called Brake System Control Unit (BSCU).	S18-WBS-R-0020 S18-WBS-R-0047 S18-WBS-R-0048 ....and others	S18-WBS-R-0509 S18-BSCU-R-0012 ...and others	Design Decision made to decrease the pilot workload and fulfill the brake functions like autobrake, annunciation, anti-skid, etc...
S18-WBS-R-0321	Y	Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be extremely remote as defined in 14CFR 25.1309.	S18-WBS-R-0040	S18-WBS-R-0508 S18-WBS-R-0509 S18-WBS-R-2971 S18-WBS-R-2972 S18-WBS-R-2984 S18-WBS-R-2985	S18 WBS FHA
S18-WBS-R-0322	Y	Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing or RTO shall be extremely remote as defined in 14CFR 25.1309.	S18-WBS-R-0051	S18-WBS-R-0510 S18-WBS-R-3011	S18 WBS FHA

FIGURE 33 - WHEEL BRAKE SYSTEM REQUIREMENTS SPECIFICATION

Requirement #	SFTY	Description	Traced From	Traced to	Source
S18-WBS-0323	Y	Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be extremely remote as defined in 14CFR 25.1309.	S18-WBS-R-0040	S18-WBS-R-0508 S18-WBS-R-0509 S18-WBS-R-2971 S18-WBS-R-2972 S18-WBS-R-2984 S18-WBS-R-2985	S18 WBS FHA
S18-WBS-R-0324	Y	Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be extremely improbable as defined in 14CFR 25.1309.	S18-ACFT-R-0934	S18-WBS-R-0509	S18 WBS FHA
S18-WBS-R-0325	Y	Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be extremely improbable as defined in 14CFR 25.1309.	S18-ACFT-R-0834	S18-WBS-R-0631 S18-WBS-R-0632	S18 WBS FHA
S18-WBS-R-0508	Y	The wheel brake system shall have at least two independent hydraulic pressure sources.	S18-WBS-0321 S18-WBS-0322	S18-WBS-R-2971 S18-WBS-R-2972	WBS CCA
S18-WBS-R-0509	Y	WBS shall have dual channel BSCU and multimode brake operations to provide the required redundancy.	S18-WBS-R-0324 S18-WBS-R-0049	S18-WBS-R-2997 S18-WBS-R-2998 ...and others	Coord Memo S18a-CM00XX
S18-WBS-R-0631	N	WBS shall indicate individual wheel temperature	N/A	S18-WBS-ICD-1001 ...and others	14CFR 25.735.j
S18-WBS-R-0632	N	WBS shall control individual wheel pressure	N/A	S18-WBS-ICD-0101 and others	14CFR 25.735.j
S18-WBS-R-1613	N	Hydraulic pressure shall be controlled for weight, autobrake mode, ground speed, wheel rotation, wheel temperature and deceleration rate in accordance with graphs given in S18 Brake Force Analysis AAS18-XXX	S18-WBS-R-0009 S18-WBS-R-0010 S18-WBS-R-0020 S18-WBS-R-0036 S18-WBS-R-0037 S18-WBS-R-0038 S18-WBS-R-0043		S18 Brake Force Analysis AAS18-XXX

FIGURE 33 - WHEEL BRAKE SYSTEM REQUIREMENTS SPECIFICATION - CONTINUED

Requirement #	SFTY	Description	Traced From	Traced to	Source
S18-WBS-R-2975	Y	The accumulator shall be attached to the blue hydraulic line between the isolation valve and the selector valve.	S18-ACFT-R-0184 S18-WBS-R-0508		Trade studies TS18-XXXX (not shown in the example)
S18-WBS-R-2986	Y	The BSCU shall be designed to Functional Development Assurance Level A.	Derived	S18-BSCU-R-0001	S18 WBS PSSA
S18-WBS-R-6104	Y	The probability of "BSCU Fault Causes Loss of Braking Commands" shall be less than 3.3E-5 per flight.	Derived	S18-BSCU-R-0002	S18 WBS PSSA
S18-WBS-R-6105	Y	The probability of "Loss of a single BSCU" shall be less than 5.75E-3 per flight.	Derived	S18-BSCU-R-0003	S18 WBS PSSA
S18-WBS-R-6106	Y	The probability of "Inadvertent braking due to BSCU" shall be less than 2.5E-9 per flight.	Derived	S18-BSCU-R-0004	S18 WBS PSSA
S18-WBS-R-6107	Y	No single failure of the BSCU shall lead to "Inadvertent braking".	Derived	S18-BSCU-R-0005	S18 WBS PSSA
S18-WBS-R-6108	Y	The probability of "Loss of Normal Brake System Hydraulic Components" shall be less than 3.3E-5 per flight.	Derived		S18 WBS PSSA

FIGURE 33 - WHEEL BRAKE SYSTEM REQUIREMENTS SPECIFICATION - CONTINUED

4.5.4 Allocation of Subsystem-Level Requirements

The following sampling of subsystem-level requirements are flowed down to the braking system sub-tier suppliers as the result of the final system architecture and interface requirements determined in sections 4.4 and 4.5.2. For brevity, only the BSCU sub-system requirements are shown in this example. Safety requirements allocated to the BSCU were determined by the fault tree analysis of the BSCU shown in section 4.4.1.4.3.1. The BSCU requirements are traced from their corresponding braking system requirements in the braking system specification.

4.5.4.1 BSCU Subsystem Requirements

The following is a sample of the requirements for the Brake System Control Unit, which shows traceability back to the Wheel Brake System requirements.

Requirement #	SFTY	Description	LRU Allocation	Traced From
S18-BSCU-R-0001	Y	The BSCU shall be designed to Functional Development Assurance Level A based on the catastrophic classification of “Inadvertent braking due to BSCU”.	BSCU	S18-WBS-R-2986
S18-BSCU-R-0002	Y	The probability of “BSCU Fault Causes Loss of Braking Commands” shall be less than 3.3E-5 per flight.	BSCU	S18-WBS-R-6104
S18-BSCU-R-0003	Y	The probability of “Loss of a single BSCU” shall be less than 5.75E-3 per flight.	BSCU	S18-WBS-R-6105
S18-BSCU-R-0004	Y	The probability of “Inadvertent braking due to BSCU” shall be less than 2.5E-9 per flight.	BSCU	S18-WBS-R-6106
S18-BSCU-R-0005	Y	No single failure of the BSCU shall lead to “Inadvertent braking”.	BSCU	S18-WBS-R-6107
S18-BSCU-R-0006	N	BSCU shall calculate the required braking force as per graphs given in S18-WBS-R-1613	BSCU	S18-WBS-R-1613
S18-BSCU-R-0008	N	BSCU shall control the metering valves.	BSCU	Derived
S18-BSCU-R-0009	N	BSCU shall control the anti-skid valves.	BSCU	S18-WBS-R-0044
S18-BSCU-R-0012	Y	BSCU shall control the shut off valves.	BSCU	S18-WBS-R-0045 S18-WBS-R-0049
S18-BSCU-R-0027	Y	BSCU shall have two channel single LRUs.	BSCU	S18-WBS-R-0509
S18-BSCU-R-0051	Y	Each BSCU channel shall have a monitoring unit.	BSCU	S18-WBS-R-00509
S18-BSCU-R-0075	Y	Each BSCU channel shall have a control unit.	BSCU	S18-WBS-R-0509
S18-BSCU-R-0099	Y	Each BSCU channel shall have independent power.	BSCU	Derived
S18-BSCU-R-0123	Y	Each BSCU channel shall have independent pedal input to both control and monitoring units.	BSCU	Derived
S18-BSCU-R-0124	Y	The command units of each BSCU channel shall be independent.	BSCU	S18-WBS-R-2997 S18-WBS-R-0509
S18-BSCU-R-0125	Y	The monitoring units of each BSCU channel shall be independent.	BSCU	S18-WBS-R-2998 S18-WBS-R-0509
S18-BSCU-R-0126	Y	The command channel hardware and software of each BSCU shall be developed to IDAL B.	BSCU	S18-WBS-R-3000

FIGURE 34 - BSCU SUBSYSTEM REQUIREMENTS

4.6 Braking System Requirements Validation

(Editor's Note: This section focuses on the activities which took place during the requirements validation of the Wheel Brake System Requirements. Requirements validation involves performing activities which provide sufficient evidence that each requirement is correct and that the requirements as a whole are complete).

As described in ARP4754A/ED-79A Section 5.4, there are numerous methods for validating the requirements. For this example, the following activities were performed:

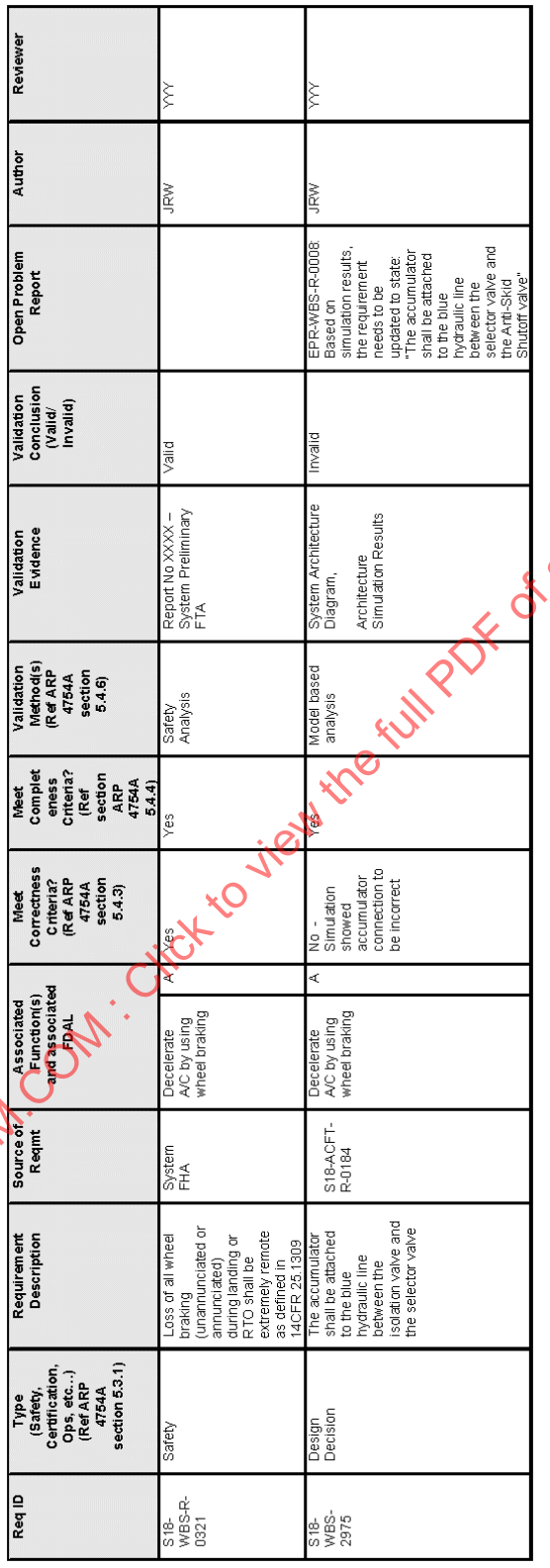
- System simulation model to validate the system architecture and safety objectives of system components
- Formal peer review of each requirement
- Formal peer review of validation method for each requirement
- Formal peer review of validation method evidence

4.6.1 Braking System Validation Matrix

The matrix given below is a sample of how to validate the requirements (and assumptions) throughout the Braking System development process.

(Editor's Note: A validation matrix or other adequate approach is desirable to track the status of the requirements validation process. The specific format is left up to the developer. This matrix should contain all of the system requirements; only two are shown here.

Example of some requirements are given in this matrix. All requirements defined in ARP4754A/ED-79A para. 5.3.1 (safety requirements, functional requirements, customer requirements, operational requirements, performance requirements, etc.) related to braking system should be validated by using the same methodology. This model is also used to validate groups of requirements. Traceability between top level requirements and lower level requirements should be established).



Req ID	Type (Safety, Certification, Ops, etc...) (Ref ARP 4754A section 5.3.1)	Requirement Description	Source of Reqmt	Associated Function(s) and associated FDAL		Meet Correctness Criteria? (Ref ARP 4754A section 5.4.3)	Meet Completeness Criteria? (Ref section ARP 4754A 5.4.4)	Validation Method(s) (Ref ARP 4754A section 5.4.6)	Validation Evidence	Validation Conclusion (Valid/ Invalid)	Open Problem Report	Author	Reviewer
S18-WBS-R-0321	Safety	Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be extremely remote as defined in 14CFR 25.1309	System FHA	Decelerate A/C by using wheel braking	A	Yes	Yes	Safety Analysis	Report No XXXX – System Preliminary FTA	Valid		JRW	YYY
S18-WBS-2975	Design Decision	The accumulator shall be attached to the blue hydraulic line between the isolation valve and the selector valve	S18-ACFT-R-0184	Decelerate A/C by using wheel braking	A	No - Simulation showed accumulator connection to be incorrect	Yes	Model based analysis	System Architecture Diagram, Architecture Simulation Results	Invalid	EPR-WBS-R-0008: Based on simulation results, the requirement needs to be updated to state: "The accumulator shall be attached to the blue hydraulic line between the selector valve and the Anti-Skid Shutoff valve"	JRW	YYY

FIGURE 35 - BRAKING SYSTEM VALIDATION MATRIX

*These requirements are created by the Aircraft manufacturer and flowed down to system supplier. Validation of the requirements will be done by the Aircraft manufacturer with assistance from the system supplier.

(Editor's Note: This matrix should be updated regularly during the development and included in the validation summary. This matrix will be finalized when all validation conclusions become valid or justified in an open problem report. Because the example does not contain a complete set of requirements, it is not possible to include a requirements completeness check.

Requirements, validation methods and validation evidence should be independently reviewed. Needs for independent review depends on the development assurance level of the function related to requirements (see ARP4754A/ED-79A section 5.4.5 for the needs for independency of validation). To ensure the independence of validation the braking system supplier used the process shown in* Figure 36, *which was documented in their Requirements Validation Plan. Other methods than this process flow may be used to satisfy independence. The objective of independence is to ensure that if errors are made during requirements development, they are visible in the validation evidence).

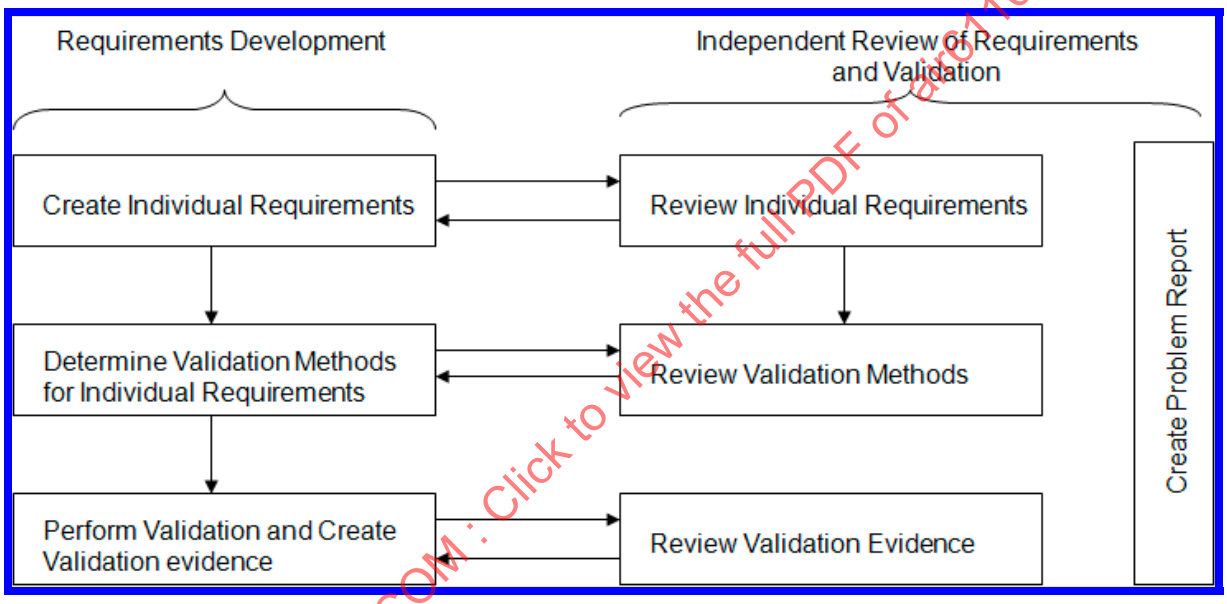


FIGURE 36 - VALIDATION INDEPENDENCE (TAKEN FROM REQUIREMENTS VALIDATION PLAN)

Editor's Note: Problem reports were established starting after the first baseline of requirements was created and continued to be generated throughout the requirement validation process. The braking system supplier's internal non-conformance control procedure was used to capture and maintain the problem reports during the validation process.

***Editor's Note: Correctness checks of the requirements should be carried out at each level of the requirements hierarchy. The correctness checklist may be performed in accordance with ARP4754A/ED-79A paragraph 5.4.3. For brevity's sake, only a subset of the ARP4754A/ED-79A correctness check is included in* Figure 37.**

Editor's Note: The following checklist was used by the system supplier to validate correctness of the braking system requirements).

Correctness Check Críteria	Results (Yes/No)	Problem Report No
Does the requirements have a unique interpretation (unambiguous)?	Y	
If it is a derived requirement supported by a rationale?	N	EPR-WBS-R-0007 EPR-WBS-R-0008
Is the source(s) of the requirement identified and correct?	Y	
Is failure condition classification justified? Are all system failure conditions identified and classifed correctly?	Y	
Does the requirement set correctly reflect the safety analyses?	Y	

FIGURE 37 - BRAKING SYSTEM REQUIREMENTS CORRECTNESS CHECK

(Editor's Note: Below is an example of a validation problem report description).

EPR-WBS-R-0007

The requirement "S18-WBS-R-0065: The accumulator shall be capable of providing 2000 PSI (assumption that 2000 PSI will be sufficient to stop aircraft) needs to be further analyzed. There should be a rationale for determining the 2000 PSI value. Therefore, the following methods may be used for justification;

a) simulation of the architecture
b) airframer provided the following information:
- need to be able to apply the brakes 6 times during an emergency landing deceleration (need to be able to press and release to avoid skidding when anti-skid is not available).
- the design of the brake actuator uses approximately 300 psi per full depress of the mechanical pedal (source of information is brake actuator supplier and is based on volume of actuator versus volume of accumulator plus hydraulic line).
- design margin of X%

All information has been evaluated about accumulator and we decided that we need accumulator capable of at least 1800 PSI. And requirement is corrected as below;

S18-WBS-R-0065: The accumulator shall provide a minimum of 1800 PSI.

FIGURE 38 - EXAMPLE VALIDATION PROBLEM REPORT

(Editor's Note: Completeness checks should be performed by reviewing outcome of validation process (templates, checklists, reports, etc.). These checks may be performed by customers, users, maintainers, certification authorities and developers. Checklists may be used for completeness checks and prepared in accordance with ARP4754A/ED-79A Para.5.4.4.1. The following checklist was used by the system supplier to validate completeness of the braking system requirements).

Completeness check criteria	Results (Yes/No)	Problem Report No
Are the procedures /templates developed and the system established for traceability of requirements	Y	
Is traceability with supporting rationale established from aircraft level to item level?	Y	
Are all requirements (performance, operational, customer, etc.) from contract fully covered?	Y	
Are all higher level functions allocated to this system fully covered?	Y	
Are all safety requirements represented in the requirements set (from FHA, previous safety assessments, in service lessons learned, novelties, etc.)?	Y	
Are all regulatory standards and guidelines represented in the requirements set?		
Industry and company design standards represented in the requirements set?	Y	
Flight operations and maintenance scenarios represented in the requirements set?	Y	
Are validation methods defined for each requirement (simulation/modelling, bench test, flight test, etc.)?	Y	
Are open reports developed for any non-conformance determined during validation of requirements?	Y	
Does the set of requirements completely define the system/item?	N	EPR-WBS-R-0009
Are all interface requirements to other systems, people and processes identified and agreed?	Y	
Are the constraints associated with each interface defined in sufficient detail for the interface to be realized?	Y	
Are the functional requirements set fully allocated and traced to the system architecture?	Y	
Are safety requirements checked using experience from previous programs and novelties of the current program?	Y	

FIGURE 39 - BRAKING SYSTEM REQUIREMENTS COMPLETENESS CHECK

(Editor's Note: After the completeness check of the requirements it was determined that the set of requirements defining brake temperature was not sufficient. Brake temperature is very important data to prevent possibility of a fire hazard. The following requirements were identified to be added to the Wheel Brake System requirements specification to satisfy the completeness check).

- Wheel Brake System shall control individual wheel temperature.
- The brake system shall have a temperature monitoring system.
- The brake system shall indicate the brake temperatures to the crew through the flight deck indications.

The Brake temperature indications and warnings should be available to the flight crew to ensure:

- the brakes are not above the maximum temperature prior to take-off,
- brake temperature differentials are within limits,
- the delay of the retraction of the gears when the brakes are above a specified brakes hot temperature

4.6.2 Validation Results

There are two requirements that need further analysis. Model base analysis has been established to finalize validation of these requirements.

System requirement to be validated is:

S18-WBS-R-2973 Operation of the alternate system shall be precluded when the NORMAL system is in use.

Derived system requirement from Arch.3 to be validated is:

The accumulator shall be attached to the blue hydraulic line between the selector valve and the Anti-Skid Shutoff valve.

Validation method used is;

Model based analysis (i.e. Simulation)

Results of model based analysis;

Architecture 3 has been simulated and the behavior model for each system component has been established. Results of the modeling are that the schematic of the braking system architecture does not work and there are some mistakes in the schematic. Risk of hydraulics supply to brakes is possible in normal mode by accumulator. Therefore accumulator position needs to be changed to meet the requirement S18-WBS-R-2973. Derived system requirements from arch.3 are not correct and needs to be changed.

Corrected requirement is: The accumulator shall be attached to the blue hydraulic line between the isolation valve and the selector valve. (Architecture 4)

Requirement derived from the architecture 4 is correct, complete and valid. Correctness and completeness of the requirement has been performed by using the checklist.

Design change according to validation process from arch.3 to arch.4 is given below:

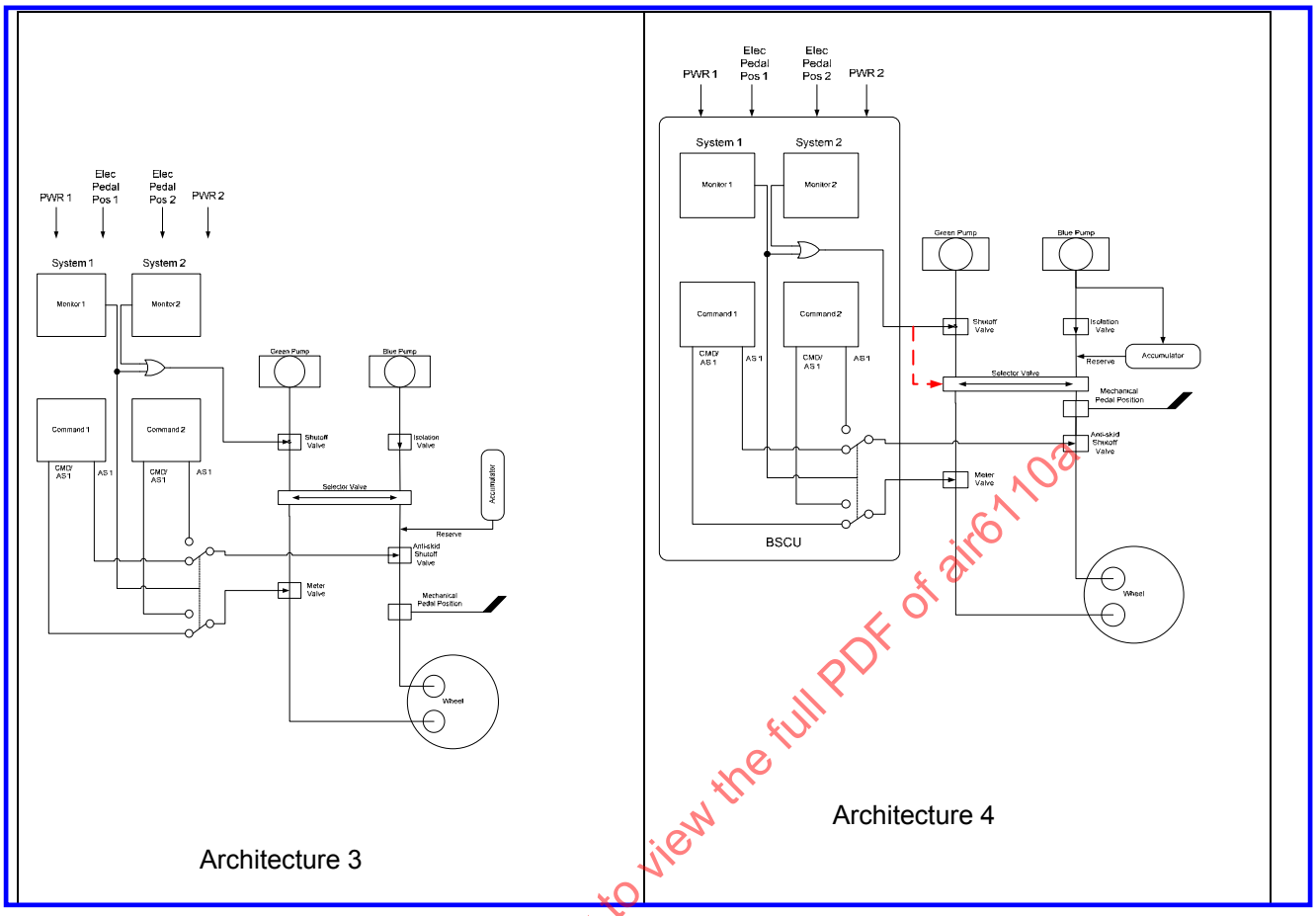


FIGURE 40 - ARCHITECTURE COMPARISON

4.6.3 Validation Summary

The applicable requirements were reviewed, analyzed and validated for Braking System of S18 Aircraft. The validation of the requirements has been performed in compliance with the Braking System Requirement Management Plan. Additional analyses were done to determine the required rigor. The validation status of all requirements was raised to “valid”. Model based analysis has been used to support the validation of requirements.

4.7 Braking System Integration

This example focuses on the braking system but there are interactions with interfacing systems that require integration activity to manage these interactions. For clarity in the example these interactions are not discussed in detail in the rest of the example, but some examples are provided here.

All the elements which can cause aircraft acceleration or deceleration require a robust air-ground indication. It is typical that the powerplant, the thrust reverser, the brakes and the spoilers all need such a robust air-ground indication, but may be constrained not to use the same sources, and typically may not use any one source. With only a few available sources, it can be a challenge to avoid common modes. Additionally, brakes will be ineffective unless the ground spoilers have deployed. An erroneous air ground indication for the both the thrust reversers and either the brakes or spoilers would violate their independence.

4.8 Braking System Process Assurance

4.8.1 Braking System Process Assurance Plan

The process assurance plan for the Braking System was developed during the project planning phase of the development life cycle. For more information on process assurance, refer to ARP4754A/ED-79A, section 5.7.

4.8.2 Evidence of Process Assurance

Throughout the development life cycle, evidence was collected to document that the processes planned were adequately followed. This evidence allowed auditors to assess the level of rigor that was carried out for each development process and determine whether that rigor was appropriate for the relative importance of the system.

Each of the plans developed for the Braking System included information about the process that was to be followed. For example, WBS-0001-105, the Wheel Brake System Requirements Management Plan (see Appendix B) states that the individuals who reviewed the validation methods and validation evidence must be independent from the individuals who created the validation evidence. The process assurance activities included audits that verified that this independent review of the methods and evidence took place as shown below.

Requirement Inspection Issue Log

Inspection ID:		WBS System Requirements Inspection			Date of Inspection:	2-Dec-08
Inspector	Item #	Line	Type of Issue	Checklist Rule	Brief Description	Problem Report (if opened)
MLS	1	ARP-BRAKE-R-0632	Minor		The requirement states "WBS shall control individual wheel pressure" but should probably state "WBS shall control the hydraulic pressure to each wheel individually."	
MLS	2	ARP-BRAKE-R-0043	Major		The requirement states "The braking system shall provide an auto brake system/" Is "auto brake system" meant to be separate sub-system or just a function that the braking system should implement?	
JPS	3	ARP-ACFT-R-0184	Major		Based on the simulation results, the requirement needs to be updated to state: "The accumulator shall be attached to the blue hydraulic line between the selector valve and the Anti-Skid Shutoff valve"	EPR-BRAKE-R-0008
	4					
	5					
	6					
	7					
	8					
	9					

FIGURE 41 - BRAKING SYSTEM REQUIREMENTS INSPECTION LOG

The development process included major phase reviews. At the end of each major development phase, a project wide design review was held to ensure that the program's objectives were being met. Below is the review checklist sign-off sheet indicating that the Wheel Brake System Systems Requirements Review phase was adequately completed and the evidence reviewed.

REQUIRED PARTICIPANTS	
Design Lead _____	Date _____
Systems Engineering _____	Date _____
	Date _____
Safety_____	Date _____
OPTIONAL PARTICIPANTS	
Contracts _____	Date _____
New Business Development _____	Date _____
Reliability _____	Date _____
Mfg Planner _____	Date _____
Test _____	Date _____
Service Center _____	Date _____
Other _____	Date _____
Other _____	Date _____
APPROVALS	
Design Mgr _____	Date _____
Team Ldr _____	Date _____

FIGURE 42 - BRAKING SYSTEM REQUIREMENTS REVIEW ARTIFACT

4.9 Braking System Configuration Management

4.9.1 Configuration Identification

The following table shows the braking system, hardware and software configuration items (CI's) and their associated data items identified from the final system architecture shown in Figure 2Figure 0 and the item-level architecture shown in Figure 24. The braking system itself, along with its associated data items, is at the top-level of configuration. The BSCU COM and MON hardware and software are separate configuration items. The associated BSCU data items include the required DO-178/ED-12 and DO-254/ED-80 data items for the assigned IDAL of these software and hardware configuration items. Some data items have been omitted from this example for brevity. All other configuration items are non-complex hardware items for which DO-254/ED-80 is not required.

All CI identifiaction numbers are assigned by the braking system integrator, who maintains a cross-reference between the system ID number and the individual supplier part numbers.

CI Identification Number	CI Name	CI Identification Number	Associated Data Item Names
WBS-0001-001	WBS (Wheel Brake System)	WBS-0001-101	Diagram – Interface - WBS
		WBS-0001-102	BOM - WBS
		WBS-0001-103	WBS SRD (System Requirements Document)
		WBS-0001-104	WBS SDD (System Design Document)
		WBS-0001-105	WBS Requirements Management Plan
		WBS-0001-106	WBS Validation Data
		WBS-0001-107	WBS Validation Summary
		WBS-0001-108	WBS Verification Plan
		WBS-0001-109	WBS Verification Data
		WBS-0001-110	WBS Verification Summary
		WBS-0001-111	WBS Certification Summary
		Etc.	Etc.
WBS-1000-001	BSCU COM (Hardware)	WBS-1000-101	Drawing - BSCU COM
		WBS-1000-102	BOM - BSCU COM
		WBS-1000-103	BSCU COM PHAC (Plan for Hardware Aspects of Certification)
		WBS-1000-104	BSCU COM HRD (Hardware Requirements Document)
		WBS-1000-105	BSCU COM HDD (Hardware Design Document)
		WBS-1000-106	BSCU COM HVP (Hardware Verification Plan)
		WBS-1000-107	BSCU COM HVR (Hardware Verification Results)
		WBS-1000-108	BSCU COM HAS (Hardware Accomplishment Summary)
		Etc	Etc
WBS-1010-001	BSCU MON (Hardware)	WBS-1010-101	Drawing - BSCU MON
		WBS-1010-102	BOM - BSCU MON
		WBS-1010-103	BSCU MON PHAC (Plan for Hardware Aspects of Certification)
		WBS-1010-104	BSCU MON HRD (Hardware Requirements Document)
		WBS-1010-105	BSCU MON HDD (Hardware Design Document)
		WBS-1010-106	BSCU MON HVP (Hardware Verification Plan)
		WBS-1010-107	BSCU MON HVR (Hardware Verification Results)
		WBS-1010-108	BSCU MON HAS (Hardware Accomplishment Summary)
		Etc	Etc
WBS-1100-001	BSCU COM (Software)	WBS-1100-101	BSCU COM PSAC (Plan for Software Aspects of Certification)
		WBS-1100-102	BSCU COM SRD (Software Requirements Document)
		WBS-1100-103	BSCU COM SDD (Software Design Document)
		WBS-1100-104	BSCU COM Source Code
		WBS-1100-105	BSCU COM Executable Object Code

FIGURE 43 – WHEEL BRAKE SYSTEM CONFIGURATION ITEMS

CI Identification Number	CI Name	CI Identification Number	Associated Data Item Names
		WBS-1100-106 WBS-1100-107 WBS-1100-108 Etc.	BSCU COM SVP (Software Verification Plan) BSCU COM SVR (Software Verification Results) BSCU COM SAS (Software Accomplishment Summary) Etc.
WBS-1110-001	BSCU MON (Software)	WBS-1110-101 WBS-1110-102 WBS-1110-103 WBS-1110-104 WBS-1110-105 WBS-0110-106 WBS-1110-107 WBS-1110-108 Etc.	BSCU MON PSAC (Plan for Software Aspects of Certification) BSCU MON SRD (Software Requirements Document) BSCU MON SDD (Software Design Document) BSCU MON Source Code BSCU MON Executable Object Code BSCU MON SVP (Software Verification Plan) BSCU MON SVR (Software Verification Results) BSCU MON SAS (Software Accomplishment Summary) Etc.
WBS-2000-001	Shutoff Valve	WBS-2000-101 WBS-2000-102	Drawing – Shutoff Valve BOM – Shutoff Valve
WBS-2100-001	Isolation Valve	WBS-2100-101 WBS-2100-102	Drawing – Isolation Valve BOM –Isolation Valve
WBS-2200-001	Selector Valve	WBS-2200-101 WBS-2200-102	Drawing – Selector Valve BOM – Selector Valve
WBS-2300-001	Anti-Skid Shutoff Valve	WBS-2300-101 WBS-2300-102	Drawing –Shutoff Valve - Anti-Skid BOM –Shutoff Valve - Anti-Skid
WBS-2400-001	Metering Valve	WBS-2400-101 WBS-2400-102	Drawing – Metering Valve BOM – Metering Valve
WBS-3000-001	Brake Pedal Position Sensor	WBS-3000-101 WBS-3000-102	Drawing – Sensor –Position BOM – Sensor –Position
WBS-4000-001	Accumulator	WBS-4000-101 WBS-4000-102	Drawing – Accumulator - Hydraulic BOM – Accumulator - Hydraulic

FIGURE 43 – WHEEL BRAKE SYSTEM CONFIGURATION ITEMS - CONTINUED

4.9.2 Configuration Baseline Establishment

The following table describes the established braking system configuration baselines and their purpose. A configuration baseline is a snapshot of the system configuration consisting of a released version of each configuration item. Major baselines (x.0) correspond to major system releases for major project milestones. Minor baselines (x.1,2,…) correspond to iterations between major baselines. During system integration, minor baselines serve to highlight stages of integration, as shown in the table.

WBS Baseline	CI Name	CI Version	Purpose
1.0	BSCU COM HW BSCU COM SW BSCU MON HW BSCU MON SW	1.0 1.0 1.0 1.0	Requirements compliance substantiation baseline
2.0	BSCU COM HW BSCU COM SW	2.0 2.0	First system integration baseline (BSCU COM only)
2.1	BSCU COM HW BSCU COM SW BSCU MON HW BSCU MON SW	2.1 2.1 2.0 2.0	2nd system integration baseline (BSCU COM+MON)
2.2	BSCU COM HW BSCU COM SW BSCU MON HW BSCU MON SW Shutoff Valve Isolation Valve Selector Valve Anti-Skid Shutoff Valve Metering Valve Brake Pedal Position Sensor Accumulator	2.2 2.2 2.1 2.1 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Final system integration baseline (BSCU + hydraulics)
3.0	BSCU COM HW BSCU COM SW BSCU MON HW BSCU MON SW Shutoff Valve Isolation Valve Selector Valve Anti-Skid Shutoff Valve Metering Valve Brake Pedal Position Sensor Accumulator	3.0 3.0 3.0 3.0 2.0 2.0 2.0 2.0 2.0 2.0 2.0	Flight Test baseline
4.0	BSCU COM HW BSCU COM SW BSCU MON HW BSCU MON SW Shutoff Valve Isolation Valve Selector Valve Anti-Skid Shutoff Valve Metering Valve Brake Pedal Position Sensor Accumulator	4.0 4.0 4.0 4.0 3.0 3.0 3.0 3.0 3.0 3.0 3.0	Certification baseline

FIGURE 44 - WHEEL BRAKE SYSTEM CONFIGURATION BASELINES

4.9.3 Change Control and Problem Reporting

As an example of the Wheel Brake System change control and problem reporting procedures, consider the problem report EPR-WBS-R-0007 shown in Figure 38. This problem report was written against Wheel Brake System requirement S18-WBS-R-00XX. As a result of the recommendation of this problem report, a change notice was raised against the baseline 1.0 of WBS-0001-103, the Wheel Brake System Requirements Document. This and other changes resulting from the requirements validation process were incorporated into a minor baseline 1.1 of WBS-0001-103. The example engineering change notice (ECN) is shown below.

```
    ECN # : 12345-67    Class : I                    Date : 03-DEC-08
     Entered by : jsmith
 Eng Resp : 01               Urgent : N                    Program : 12345
           Released by : JSMITH
           Customer Approval Reqd : Y        Cust. Approval Date : 03-DEC-2008
=============================================================================
  Ref Op Code Item Number      E/C Rev Qty    Requested By
 1     100       WBS-0001-103      New      1       JSMITH
DESCRIPTION:    Delete requirement S18-WBS-R-00XX and replace by requirement S18-WBS-R-00YY.
                S18-WBS-R-00XX:    The accumulator shall capable of providing 2000 PSI.
                S18-WBS-R-00YY:    The accumulator shall capable of providing 1800 PSI.
REASON:         The requirement has been adjusted based on additional information provided by the airframer.
SUBSTANTIATION: See problem report EPR-WBS-R-0007.
```

FIGURE 45 - WHEEL BRAKE SYSTEM ENGINEERING CHANGE NOTICE

5. BRAKING SYSTEM AND AIRCRAFT-LEVEL VERIFICATION

This section describes the verification process for the aircraft-level braking requirements given in section 2.5 and shows the braking system-level and aircraft-level verification artifacts generated by this process.

5.1 Braking System Control Unit Verification

When developing the Braking System Requirements, the system supplier chose to create the validation and verification matrices at the same time. Their implementation method was to use the requirements database to also store the validation and verification matrices. For each requirement the required verification attributes are stored. The company tried to determine the method of verification at the time of generating the requirement. This was not possible in all cases, but the verification method was determined and reviewed prior to the verification activities being performed. Figure 47 shows some of the BSCU-level requirements, their associated braking system-level functions, the methods to be applied to verify each requirement, references to the verification procedures, verification results and any problem reports generated, and the verification conclusion (pass/fail).

(Editor's Note: The verification matrix is based on the BSCU-level requirements shown in 4.5.4.1. For each requirement, appropriate verification method(s) are chosen. Since the FDAL of the Decelerate Aircraft on Ground aircraft function is A (see requirement # S18-ACFT-R-0933), according to Table 5.4 of ARP4754A/ED-79A the verification methods must include Analysis, Modeling or Test for Level A functions. Test of unintended functions is also required. If it is not feasible to perform a test to verify the requirement, then an analysis method is chosen. Verification of safety requirements, particularly those dealing with failure rates or to show that a particular failure condition is extremely remote, is typically performed by an SSA).

Once the verification method(s) for each requirement are reviewed and determined to be adequate for the FDAL and specifics of the requirement, the company begins to develop verification methods. In most cases, this involves formal test procedures. For formal test procedures, the company has chosen to develop a test setup and test procedures to run on that setup. The company has called these tests their System Integration Tests (SITs). The formal SITs test procedures were documented on test procedure forms as shown in Figure 46. Each test procedure is traced to one or more requirements depending on how many requirements the test exercises. After all of the identified test cases have been identified, the test procedures were reviewed using the following checklist:

Test Procedure Inspection Checklist

- Does each test have a header that identifies the author, revision date, test objectives, required configuration, and initial setup?
- Is each test traceable to a specific requirement defined in the requirements?
- Does the test procedure define the exact sequence of steps required to execute the test?
- For each test, are the expected results clearly defined?
- Are the expected results consistent with the requirements?
- Are the test objectives achievable?
- Is test specimen configured and does it match data from manufacturer?
- Is test platform representative and calibrated?
- …

After all of the identified verification procedures were written, the verification matrix was again reviewed. This time, each requirement was reviewed using the following checklist.

Requirement Verification Checklist

- Do the verification methods allocated to this requirement fully verify the requirement?
- Are any limits specified within the requirement accurately tested?
- …

System Integration Test (SITs) Procedure
Test No: S18-BSCU-SIT-0068 Date:

Test Procedure Name: Maximum Braking Force Calculation

Requirements Coverage: S18-BSCU-R-0006
S18-BSCU-R-0008
S18-BSCU-R-0009
S18-BSCU-R-0012
Add ARP_BRAKE_XXXX
Add ARP_BRAKE_XXXX
Add ARP_BRAKE_XXXX

Test Description:

This test demonstrates the proper determination of braking force required given varying wheel speed and air speed inputs. This test is performed for each condition defined S18 Brake Force Analysis AAS18-XXX.

Test Setup:

Figure NN.N depicts the test setup for S18-BSCU-SIT-0068. The aircraft simulation (located in the test station) provides simulated wheel speed and airspeed to the BSCU. The test station loops through the various conditions defined in S18 Brake Force Analysis AAS18-XXX and provides the appropriate inputs for each test case. It also records the output of the BSCU to determine if the BSCU matches expected results.

Test Steps and Success Criteria:

Test Step	Test Step Description	Expected Results	Actual Results	Pass /Fail
1	Wt: XXX,XXX lbs Autobrake mode: AUTO Wheel Speed: XX rpm CAS: XX knots Wheel Temperature: XX degrees F	XXX psi Green Meter Valve Actuation		
2	Wt: XXX,XXX lbs Autobrake mode: AUTO Wheel Speed: YY rpm CAS: XX knots Wheel Temperature: XX degrees F	YYY psi Green Meter Valve Actuation		
3				

NOTE: the test station records the inputs from the BSCU and flags a test failure if it does not meet these criteria. The recorded data is stored on the test station for post processing after the test is complete.

Test Results: PASS FAIL

Failure Description:

Failure Resolution:

FIGURE 46 – BSCU SYSTEM INTEGRATION TEST PROCEDURE

Below is an example of the verification matrix with procedures and results partially completed.

Requirement #	SFTY	Description	Associated Function(s) (Ref. Section 2.5)	Verification Method(s)	Verification Procedure/Results	Problem Report	Conclusion (Pass/Fail)
S18-BSCU-R-0012	Y	BSCU shall control the shut off valves		Analysis, System Integration Test	System Integration Test: S18-BSCU-SIT-0070 Software: DO-178B verification results for BSCU software.		Pass
S18-BSCU-R-0126	Y	The command channel hardware and software of each BSCU shall be developed to IDAL B.		BSCU SSA (CMA)	Hardware: DO-254 verification results for BSCU hardware (HAS) Software: DO-178B verification results for BSCU software (SAS)		Pass

FIGURE 47 – BRAKING SYSTEM CONTROL UNIT VERIFICATION MATRIX (EXCERPT)

5.2 Wheel Brake System Level Verification

The verification matrix (Figure 40) shows the Wheel Brake System-level requirements flowed down to the BSCU, their associated system-level functions, the methods to be applied to verify each requirement, references to the verification procedures, verification results and any problem reports generated, and the verification conclusion (pass/fail).

(Editor's Note: The verification matrix is based on the system-level requirements shown in section 4.5.3***. For each requirement, appropriate verification method(s) were chosen. Since the FDAL of the Decelerate Aircraft on Ground aircraft function is A (see requirement # S18-ACFT-R-0933), according to Table 5.4 of ARP4754A/ED-79A the verification methods must include Test and one or more others for Level A functions. Test of unintended functions is also required. Note that testing of certain system-level requirements must be deferred to the aircraft-level (see for example S18-WBS-R-0020. If it is not feasible to perform a test to verify the requirement, then an analysis method is chosen. Verification of safety requirements, particularly those dealing with failure rates or to show that a particular failure condition is extremely remote, is typically performed by an SSA).***

Figure 48 below is an example of a system integration test procedure form.

System Integration Test (SITs) Procedure
Test No: S18-WBS-SIT-0099 Date:

Test Procedure Name: Autobrake Function

Requirements Coverage: ARP_BRAKE_0043

Test Description:

This test demonstrates the proper operation of the autobrake function. This function automatically engages pressurized wheel braking at the pilot-selected pressure level upon touchdown to the landing surface. The aircraft automatically decelerates at the selected level regardless of other factors, such as aircraft drag and other deceleration methods (such as deployment of thrust reversers or spoilers)….

Test Setup:

Figure NN.N depicts the test setup for S18-WBS-SIT-0099. The aircraft simulation (located in the test station) provides the touchdown indication, the pressure level selected by the pilot, simulated wheel speed and airspeed to the BSCU. The test station receives…

Test Success Criteria

1) For each condition listed above, the Wheel Brake System shall ….
2) ….
3) ….

NOTE: the test station records the inputs from the Wheel Brake System and flags a test failure if it does not meet these criteria. The recorded data is stored on the test station for post processing after the test is complete.

Test Results: PASS FAIL

Failure Description:

Failure Resolution:

FIGURE 48 – WHEEL BRAKE SYSTEM INTEGRATION TEST PROCEDURE

Requirement #	SFTY	Description	Associated Function(s) (Ref. Section 2.5)	Verification Method(s)	Verification Procedure/Results	Problem Report	Conclusion (Pass/Fail)
S18-WBS-R-0020	N	Wheel Brake System shall meet 14CFR 25.735	8.1	Test / Analysis			To Be Verified at the aircraft level
S18-WBS-R-0043	N	Wheel Brake System shall provide an autobrake function	8.1	Test	System Integration Test: S18-WBS-SIT-0099		Pass
S18-WBS-R-0321	Y	Loss of all wheel braking (un-annunciated or annunciated) during landing or RTO shall be extremely remote as defined in 14CFR 25.1309	8.1, 8.13	Analysis	Wheel Brake System SSA (FTA)		Pass
S18-WBS-R-0322	Y	Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing or RTO shall be extremely remote as defined in 14CFR 25.1309.	8.2	Analysis	Wheel Brake System SSA (FTA)		Pass
S18-WBS-R-0323	Y	Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be extremely remote as defined in 14CFR 25.1309.	8.1	Analysis	Wheel Brake System SSA (FTA)		Pass
S18-WBS-R-0324	Y	Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be extremely improbable as defined in 14CFR 25.1309.	8.1	Analysis	Wheel Brake System SSA (FTA)		Pass

FIGURE 49 - WHEEL BRAKE SYSTEM VERIFICATION MATRIX (EXCERPT)

Requirement #	SFTY	Description	Associated Function(s) (Ref. Section 2.5)	Verification Method(s)	Verification Procedure/Results	Problem Report	Conclusion (Pass/Fail)
S18-WBS-R-0325	Y	Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be extremely improbable as defined in 14CFR 25.1309.	8.1, 8.1.3	Analysis	Wheel Brake System SSA (FTA)		Pass
S18-WBS-R-0508	Y	The wheel braking shall have at least two independent hydraulic pressure sources	8.1, 8.2, 8.3, 8.4	Analysis	Wheel Brake System CCA		Pass
S18-WBS-R-6104	Y	The probability of "BSCU Fault Causes Loss of Braking Commands" shall be less than 3.3E-5 per flight.	8.1, 8.2, 8.3, 8.4	Analysis	BSCU SSA (FTA)		Pass
S18-WBS-R-6107	Y	No single failure of the BSCU shall lead to "Inadvertent braking".	8.1, 8.2, 8.3, 8.4	Analysis	BSCU SSA (FTA) BSCU CCA		Pass
S18-WBS-R-6108	Y	The probability of "Loss of Normal Brake System Hydraulic Components" shall be less than 3.3E-5 per flight.	8.1, 8.2, 8.3, 8.4	Analysis	Wheel Brake System SSA (FTA)		Pass
S18-WBS-R-2986	Y	The BSCU shall be designed to Function Development Assurance Level A.	8.1, 8.2, 8.3, 8.4	Analysis	Wheel Brake System SSA (CMA)		Pass

FIGURE 49 - WHEEL BRAKE SYSTEM VERIFICATION MATRIX (EXCERPT) - CONTINUED

5.3 Aircraft Level Braking Verification

The verification matrix shows the aircraft-level requirements flowed down to the braking system, their associated aircraft-level functions, the methods to be applied to verify each requirement, references to the verification procedures, verification results and any problem reports generated, and the verification conclusion (pass/fail).

When developing the aircraft-level braking requirements, the company chose to create the validation and verification matrices at the same time. Their implementation method was to use the requirements database to also store the validation and verification matrices. For each requirement the required verification attributes are stored. The company tried to determine the method of the verification at the time of generating the requirement. This was not possible in all cases, but the verification method was determined and reviewed prior to the verification activities being performed.

(***Editor's Note: The verification matrix is based on the aircraft-level requirements shown in section 2.5. For each requirement, appropriate verification method(s) were chosen. Since the FDAL of the Decelerate Aircraft on Ground aircraft function is A (see requirement S18-ACFT-R-0933), according to Table 5.4 of ARP4754A/ED-79A the verification methods must include Test and one or more others for Level A functions. Test of unintended functions is also required. If it is not feasible to perform a test to verify the requirement, then an analysis method is chosen. Verification of safety requirements, particularly those dealing with failure rates or to show that a particular failure condition is extremely remote, is typically performed by an SSA).***

Below is an example of an aircraft-level test procedure form.

Aircraft Test Procedure
Test No: AAS18-Test-007 Date:

Test Procedure Name: Maximum Weight Landing

Requirements Coverage:
S18-ACFT-R-0010

S18-ACFT-R-0011

S18-ACFT-R-0012

Test Description:

This test demonstrates the proper maximum weight aircraft deceleration rates and landing distances.

Test Setup:

Figure NN.N depicts the test setup for AAS18-Test-007.

Test Success Criteria

1) For each condition listed above, the aircraft shall ….
2) ….
3) ….

NOTE: the test station records the inputs from the aircraft and flags a test failure if it does not meet these criteria. The recorded data is stored on the test station for post processing after the test is complete.

Test Results: PASS FAIL

Failure Description:

Failure Resolution:

FIGURE 50 – AIRCRAFT LEVEL TEST PROCEDURE FORM

Below is an example of an updated verification matrix with procedures and results partially completed.

Requirement Number	SFTY	Description	Associated Function(s) (Ref. Section 2.5)	Verification Method(s)	Verification Procedure/Results	Problem Report	Conclusion (Pass/Fail)
S18-ACFT-R-0001	N	The S18 aircraft shall accommodate 300-350 passengers.	5,7	Analysis	Market research report MRS18-002 AAS18-Analysis-002: Passenger Arrangement Layout Analysis AAS18-Analysis-003: Digital Interior Mockup		Pass
S18-ACFT-R-0007	N	The maximum design landing weight shall be 135,000 lbs.	1,8	Analysis	AAS18-XXX analysis report AAS18-Analysis-008 Structural Analysis	EPR-ACFT-P-0004	Fail
S18-ACFT-R-0008	N	The S18 aircraft, at maximum takeoff weight, shall be capable of takeoff in a distance of 9,800 (TBD) feet.	3,8	Analysis, Test	AAS18-XXX analysis report		Pass
S18-ACFT-R-0009	N	Aircraft shall have a means to decelerate on the ground in accordance with 14CFR 25.735	8	Analysis	AAS18-XXX analysis report		Pass
S18-ACFT-R-0010	N	The S18 aircraft, at maximum landing weight, shall be capable of decelerating in a distance of TBD feet.	8	Analysis, Test	AAS18-XXX analysis report AAS18-Test-007-Maximum Weight Landing		Pass
S18-ACFT-R-0011	N	The aircraft shall be capable of a mean landing deceleration of at least 10 fps^2, including when at maximum landing weight.	8	Analysis	AAS18-XXX analysis report AAS18-Test-007-Maximum Weight Landing		Pass

FIGURE 51 - AIRCRAFT LEVEL BRAKING SYSTEM VERIFICATION MATRIX

Requirement Number	SFTY	Description	Associated Function(s) (Ref. Section 2.5)	Verification Method(s)	Verification Procedure/Results	Problem Report	Conclusion (Pass/Fail)
S18-ACFT-R-0012	N	The S18 aircraft shall have a minimum required landing length of TBD feet.	8	Analysis	AAS18-XXX analysis report AAS18-Test-007 – Maximum Weight Landing		Pass
S18-ACFT-R-0013	Y	Individual braking system failure conditions shall not cause catastrophic condition at the aircraft level.	1-8	Analysis	ASA-18-XXX Aircraft Safety Assessment		Pass
S18-ACFT-R-0014	N	Provide control on ground	8		First Flight Simulation Profile		
S18-ACFT-R-0015	N	Provide speed control on ground	8		First Flight Simulation Profile		
S18-ACFT-R-0016	N	Provide deceleration of aircraft on ground	8		First Flight Simulation Profile		
S18-ACFT-R-0017	N	Provide deceleration of aircraft on ground by wheel brakes	8		First Flight Simulation Profile		
S18-ACFT-R-0018	N	Provide deceleration of aircraft on ground by thrust reversers	8		First Flight Simulation Profile		
S18-ACFT-R-0019	N	Provide reduced touchdown speed	3,8		First Flight Simulation Profile		
S18-ACFT-R-0020	N	Provide forward thrust removal	3,8		First Flight Simulation Profile		
S18-ACFT-R-0021	N	Provide structural integrity during deceleration	1		First Flight Simulation Profile		
S18-ACFT-R-0022	N	Provide direction control on ground	8		First Flight Simulation Profile		
S18-ACFT-R-0023	N	Provide direction control on ground by nose wheel steering	8		First Flight Simulation Profile		
S18-ACFT-R-0024	N	Provide direction control on ground by rudder control	8		First Flight Simulation Profile		
S18-ACFT-R-0025	N	Provide direction control on ground by differential braking	8		First Flight Simulation Profile		
S18-ACFT-R-0026	N	Provide retractable landing gear	8		First Flight Simulation Profile		

FIGURE 51 - AIRCRAFT LEVEL BRAKING SYSTEM VERIFICATION MATRIX - CONTINUED

Requirement Number	SFTY	Description	Associated Function(s) (Ref. Section 2.5)	Verification Method(s)	Verification Procedure/Results	Problem Report	Conclusion (Pass/Fail)
S18-ACFT-R-0028	Y	Provide warning and cautions to the flight crew	4		First Flight Simulation Profile		
S18-ACFT-R-0085	N	Provide acceleration of aircraft on ground	8		First Flight Simulation Profile		
S18-ACFT-R-0110	N	Aircraft shall have auto brake system	8		Technological improvements in CATIIIb landing capability and market research ,(report MRS18-XXX) about the customer needs are the rational the requirement		
S18-ACFT-R-0135	N	Provide anti-skid system	8		All weather operation and stability of the aircraft during runway runs necessitates the requirement		
S18-ACFT-R-0184	N	Aircraft shall have hydraulically-driven brake function			Trade studies TS18-XXXX (not shown in the example) show the hydraulic drive of brake system is more economically feasible than electrical systems given the reuse from electrical system from previous SAE aircraft.		
S18-ACFT-R-0185	N	The pilot shall be allowed to override the autobrake function.			Autobrake function is a customer demand. If the function is provided, it must meet the regulation.		

FIGURE 51 - AIRCRAFT LEVEL BRAKING SYSTEM VERIFICATION MATRIX – CONTINUED