Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Design for System Safety Analysis of the Aircraft Braking System Having Normal and Emergency Wheel Braking

Rolwyn Marian Cardoza
Dept. of Mechanical Engineering
RV College of Engineering
Bengaluru, India

Dr. M. Krishna
Head of the Department
Dept. of Mechanical Engineering
RV College of Engineering
Bengaluru, India

***Abstract*— The technology is improving at a faster pace when it comes to aerospace and defense sector, this is leading to the increase in complexity of the modern system. The defense expenditure is estimated to reach US $1.9 trillion by 2020 and the commercial aircraft market is expected to reach $872 million in 2020 if there wasn't pandemic. But it is seen, lot of accidents occur during Rejected Take-off and landing phases. Any failure of the Brake system at these phases causes high speed excursion of the aircraft leading to casualties of crew, occupants and damage to the aircraft. In this context many works have focused on different safety methods on different systems but very little to none research has been done in system safety of the aircraft braking system having normal and emergency wheel braking using isograph reliability workbench tool for part 25 airplane. The objective of the work is to preform System safety analysis for the Aircraft braking system following ARP 4761 and ARP 4754A and the sensitivity analysis of the 3 architectures. It is concluded architecture 1 is the better choice since there are no single failures present in most of the failure conditions except for partial loss of the normal wheel braking but it is shown compliance to 14CFR 25.735 (b)(1), the complexity of architecture 1 is lesser than architecture 3 and there is no single failure such as main shuttle valve in architecture 2. The architecture 3 is better choice over the 2 architectures 1 and 2 for uncommanded failure conditions, which occurs due to the malfunction of the LRU's present, because of the presence of multiple BSCU which improves the possibility of failures.**

Keywords—Aircraft MLG Brake system; Normal and Emergency wheel braking; ARP 4761; ARP 4754A;

I. INTRODUCTION

A. System Safety Assessment Process

The system safety process comes under the system safety engineering which is the application of engineering and management technology, principles and criteria to achieve reasonable safety keeping in mind the design constraints through all the flight phases in the system lifecycle [1].The system safety assessment process is very widely used in the aviation industry to make the aircraft safer and to get the system certification. The federal aviation authority follows the system safety assessment as given by SAE ARP4754A and SAE 4761[2,3]. The system safety process is an integral part of the system development process. It is as shown in the figure 1.1, it is also called as "V" diagram, the first half of the process includes validation (left side of the diagram), followed by the verification (right side of the diagram) which support the safety and development of the aircraft's activities. The process starts at the Aircraft level which involves development of the Functional Hazard Analysis (FHA), this is followed by the FHA at the System level for individual sub-systems (SFHA). The purpose of the SFHA is to find the functions, find the corresponding failure conditions and classify it based on the severity. The SFHA is followed by the Preliminary System Safety Assessment (PSSA), this uses the method of fault tree analysis (FTA) to derive the requirements to the sub-systems. The fault trees are just developed at the system level in this stage. The Fault tree is a top-down approach. The top failure condition value is given as per the FAA requirement to meet, since the item requirement values are not known. The "V" process is iterative, any changes to design causes changes to the system requirements, hence, fault trees must be developed again. Once the design and architectures are finalized, the System Safety Assessment process verifies whether the implemented system meets the safety requirements. The Failure Modes and Effects Analysis (FMEA) is performed after the SSA for computing of actual failure probabilities on to the items. The verification is done by performing qualitative and quantitative analysis of the fault trees step by step, from the item level to the aircraft level after the integration of all the systems.

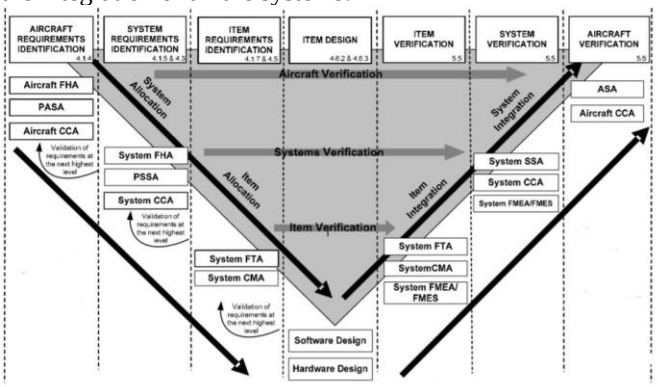

Fig 1.1 SAE ARP 4754A System Assessment Process

B. Description of Hazard Classification

The Hazard Level and the Failure Effects on the crew/occupants are provided by the United States Department of Transportation, Federal Aviation Administration based on which the Hazard levels are classified. The Failure conditions

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Hazard level for the corresponding Effects on Airplane, Occupants and Crew and the PR is shown in the Table 1.1.

Table 1.1: Hazard level and PR for Effects on airplane, crew and occupants

Hazard level	No Safety Effect	Minor	Major	Remote	Catastrophic
Probability requirement	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
		<1e-3	<1e-5	<1e-7	<1e-9
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers'	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation

C. *Description of the Braking systems in the Aircraft*

The aircraft consists of the braking for the function of deceleration or stopping the aircraft during the different flight phases. The Braking system is vigorously used during the landing, rejected take-off phases. The braking or deceleration of the aircraft can be obtained by the application of main landing gear disc brakes, spoilers, airbrakes, thrust reversers [4]. These are explained below:

1) Aircraft disc brakes system:

The Aircraft disc brakes are located in main landing gear wheels, although there have been some aircrafts which also have brakes in the nose landing gear wheels. The brakes operation has evolved from a single lever where brakes are symmetrically applied, to the incorporation of the rudder pedals which allows the left and the right brakes to be applied independently allowing the usage of differential braking to steer the aircraft for the operations on the ground as well as maintaining directional control during take-off or landing roll. The multiple disc brakes used in aircraft is shown in the Fig 1.2

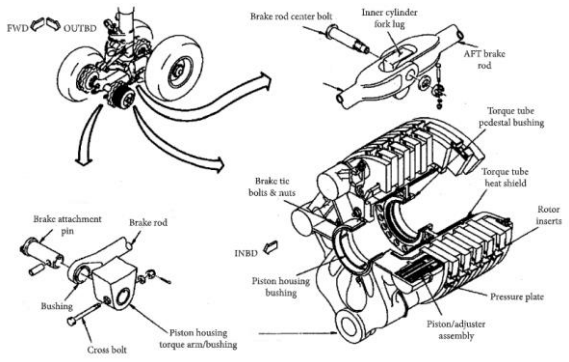

Fig I.2: Main landing gear multiple disc brakes

2) Thrust reverser system:

The Thrust reversers featured in many aircrafts are used widely for slowing down the aircraft after touch-down by temporal diversion of engine's thrust, it assists in reduction of wear on the brakes and enables shorter landing distances. The thrust reverser system provides additional safety during bad weather conditions involving snow or rain on the runway, which reduces the effectiveness of the brakes. The thrust reversers also assist in emergency situations such as rejected take-off. The Fig.1.3. shows the operation of the thrust reversers in opened and closed position.

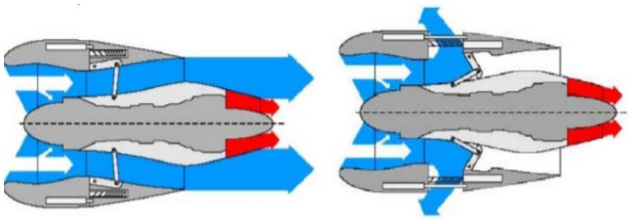

Fig 1.3 Forward and Reverse thrust in Aircraft engine

3) Spoilers

The spoiler is a device whose function is to intentionally reduce the lift component of the air foil in a very controlled way. The spoilers differ from the airbrakes in a way where the lift to drag ratio reduces, for the same reason spoilers are opened when the aircraft is approaching the runway and is about to touch-down. The airplane with spoilers actuated is as shown in the Fig. 1.4.

Fig 1.4 Spoilers

II. PROJECT OBJECTIVES AND METHODOLOGY

A. *Project Objectives*

To preform System safety analysis for the Aircraft braking system and the sensitivity analysis

- To define failure conditions based on the functions.
- Minimize failure conditions to find most critical failure condition & perform FTA
- Check if the architecture meets the FAA requirements using quantitative and qualitative analysis
- To perform sensitivity analysis.

B. *Project Methodology*

The project methodology is as shown in the Fig. 2.1. The project started with the in-depth literature survey. This involved overview of the system safety assessment, its basics, methods and tool employed to perform system safety analysis. The Architecture of the Brake system was found from literature of the aircraft from company documents.

The FCIM was derived to find out the possible failure conditions, with and without crew aware conditions, the unique and most critical failure conditions are shortlisted for SFHA. The FCIM was performed using MS Excel software.

The SFHA evaluated the failure conditions shortlisted in the FCIM at different flight phases, the effects on the airplane,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

crew and occupants are reasoned out and the corresponding hazard levels are obtained. The most critical failure condition corresponding to the flight phase and the hazard level are shortlisted for the DRM.

The DRM is the final matrix which shortlisted the failure conditions that are critical for building the fault trees. The driving failure condition and the associated hazard levels were obtained. The Fault trees were developed for the driving failure conditions of all architecture 1. The Fault trees analysis were performed to meet the requirements specified and to find the critical elements. The two novel architecture were designed, and safety assessments were performed. The shortlisted failure conditions remain the same for all the architectures, the fault trees were built for the architectures and the fault tree analysis was performed. The sensitivity analysis was performed which compares the architectures 2 and 3 with architecture 1 for all the failure conditions shortlisted in DRM.

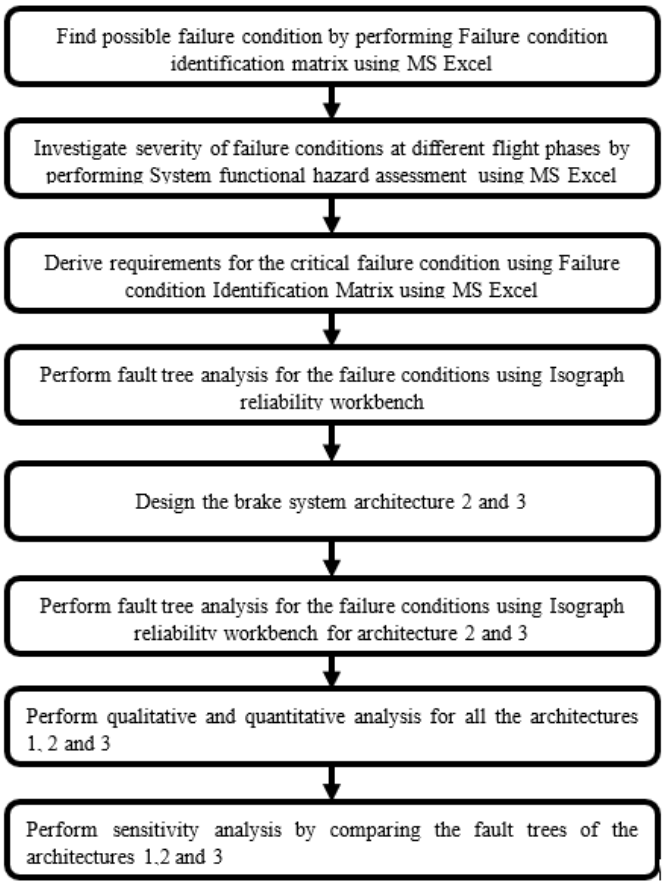

Fig 2.1 Project methodology flowchart

III. AIRCRAFT BRAKE SYSTEM ARCHITECTURES

A. Aircraft Brake System Architecture 1

The Brake System Architecture 1 as shown in the Fig. 3.1. is obtained after extensive literature survey of the company documents. The Brake System Architecture is of the aircraft MLG wheels.

It consists of the following parts:

Pilot and Co-Pilot Rudder Pedals: The top of rudder pedal is pushed for applying the brakes by the crew.

Pedal position sensor: A linear variable differential transformer (LVDT) is used as a position sensor which measures the linear displacement of the pedals and sends proportional signals to Brake system control unit.

Shut-off valve: The Shut-off valve is used to shut the hydraulic line coming from the Hydraulic system in case of failures detected. These are electrical actuated by the Brake system control unit.

Brake Control valve: The Brake control function is to control the amount of hydraulic pressure to be applied on the wheel brakes. The signals for the application of the brakes is obtained from the Brake system control unit for preventing the skidding of the brakes. Independent Brake control valves are employed for inboard and outboard brakes.

Shuttle valve: A Shuttle valve is used when there is need to take inputs from multiple channels into one output channel. It is used in for emergency purpose where if the main system fails, the emergency system pressure is used.

Hydraulic Fuse: A Hydraulic Fuse is a safety device placed at strategic and crucial location. If the sudden flow downstream is located, the fuse shuts off the fluid flow.

Brake system control unit: This is a very important part of the braking system. It performs the anti-skid operation by taking in the input from the pressure sensor and the wheel speed transducer. The purpose is to increase the traction and avoid wheel locking.

Avionics: The Avionics is the electrical systems on the aircraft. It is responsible for displaying the pressure readings from the pressure sensors, wheel speed from the wheel speed transducer, park brake handle position from the sensor, failure alerts to the crew etc.

Parking Brake: The Parking brake function is to apply pressure to the brakes during parking or during emergency wheel braking. It consists of a mechanical parking brake lever, accumulator, pressure sensor, check valve and is used to apply pressure on all the wheel through the shuttle valves. It is also used during emergency wheel braking.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

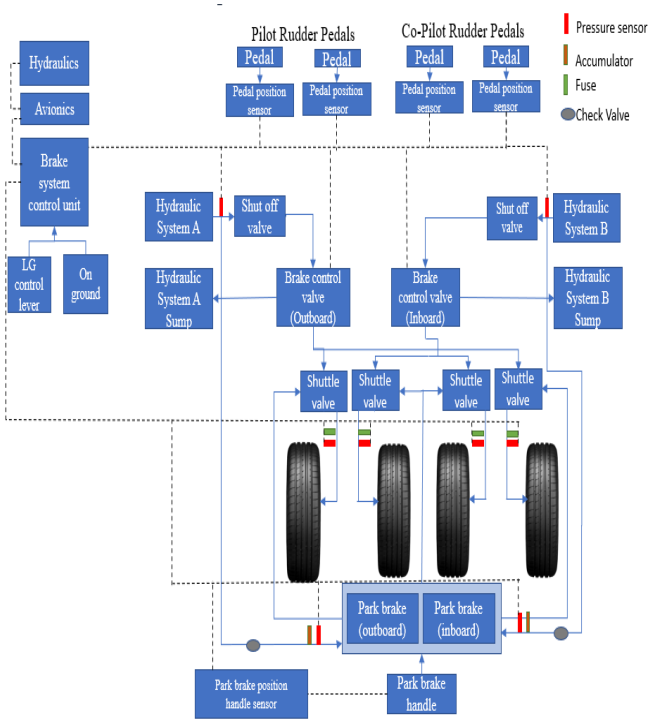

Fig 3.1 Brake System Architecture 1

B. Operation:

The operation of the aircraft braking system is divided into normal wheel braking and emergency wheel braking. The normal wheel braking doesn't consider parking brake to assist in the stoppage or deceleration of the aircraft, to make the brake system robust in the absence of the parking brake due to the following reasons:

- The parking brakes will act on all the wheels, even on the wheel brakes functioning, resulting in the loss of the available anti-skid, causing the aircraft to skid and might lead to casualty.
- When there is complete loss of the right outboard wheel brake, the application of parking brakes would apply brake on the left outboard brake along with the inboard brakes resulting in asymmetric braking leading to sliding of the aircraft away from the failed brake.
- The crew would be busy with other works for the safe landing of the aircraft such as keeping a hand on the throttle, activation of landing crew and few landing protocols, due to this the crew might not be able to apply the parking brakes.

The Emergency wheel braking also considers the parking brake for the stoppage or deceleration of the aircraft along with the normal wheel braking, during emergency that is after the loss of the inboard or outboard brakes and after receiving the CAS message about the failure of the one pair of brakes. The pilot after being alerted presses the parking brake for stopping the aircraft.

1) Normal Wheel Braking:

The crew applies the brakes by pressing the top of the rudder pedals. The position sensor detects the position and sends the signals to the Brake system control unit (BSCU). The BSCU sends the signals to the Hydraulic systems and the Brake control valve to apply pressure on the wheel. There are two independent Hydraulic systems, one for inboard and another for outboard brake systems. There are two independent Brake control valves, one supplies the pressure to the outboard brakes and other for the inboard brakes. The shutoff valve is also connected to the BSCU, it shuts off the line as per the signals obtained from the BSCU in case of detected failure. The Hydraulic fuse cuts of the line in case of sudden flow of fluid downstream and protects the system from leakage or loss of Hydraulic fluid.

Anti-skid braking is provided by the BSCU by taking the inputs from the pressure sensor and the wheel speed transducer values. If the pressure is more and wheel speed is less, it reduces the pressure to increase the traction and reduce the locking of the wheels. Anti-skid is available on all the wheels in Normal Wheel Braking.

2) Emergency Wheel Braking:

Emergency Wheel Braking is when half of the normal wheel is available, in this case either the inboard or the outboard brake system fails, then the opposite braking system either inboard or the outboard braking system is available. In the Emergency Wheel Braking, the anti-skid braking is available only in one of the functioning set of brakes.

The parking brake system is used, it is activated by pulling down the lever, the pressure sensors monitors the pressure from the accumulator. The parking brake applies the pressure on all the wheels through the shuttle valves.

C. Design of the two architectures, architecture 2 and 3 for the brake system of the main landing gear

The following 2 architectures Fig. 3.2. and Fig. 4.3. have been constructed for performing the sensitivity analysis, to realize how the safety changes or to understand how sensitive the architecture of the system is for safety.

a) Brake system architecture 2 (Arc-2)

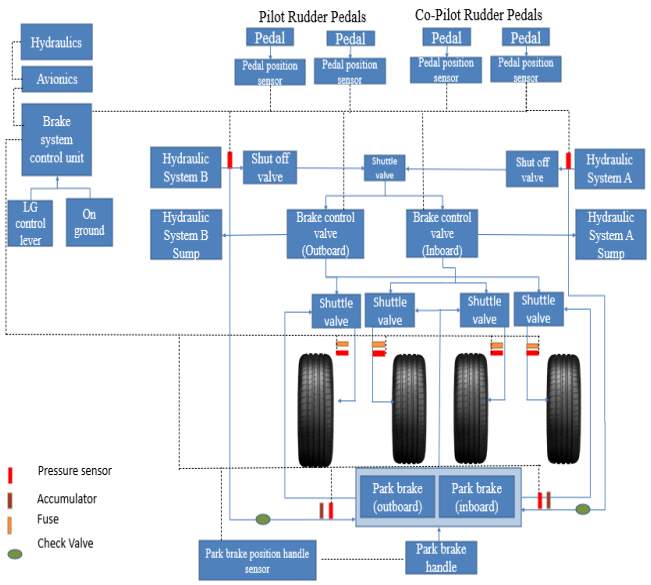

Fig 3.2 Brake System Architecture 2

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

The architecture in the Fig. 4.2. considers making the system robust by supplying the hydraulic motive power from 2 hydraulic system, in this way there is a backup motive power supply in case of failure of either one. (If hydraulic system A fails Hydraulic system B is supplies). In this brake system a shuttle valve is used to connect the hydraulic system A and B, which sends the motive power to the respective brake control valves.

2) Brake system architecture 3 (Arc-3)

The brake system architecture in the Fig. 3.3. considers making the brake system independent on the right and left side. The right side and left side are made independent by considering independent BSCU, hydraulic system i.e. Hydraulic system A to the right side and Hydraulic system B to the left side.

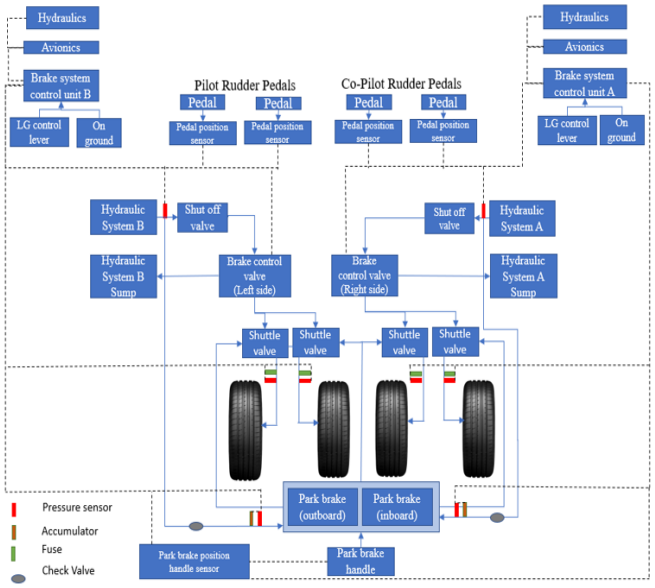

Fig 3.3 Brake System Architecture 3

D. Software Used - Isograph Reliability workbench (v14.0)

The Isograph reliability workbench with integrated Fault tree+ is the world's leading software and used extensively for system safety analysis and reliability. Reliability Workbench incorporating FaultTree+ is the world leading software suite for safety analysis of systems and reliability. It is widely used in industries such as Defense, Aerospace, Oil & Gas, Automotive, Railroads, and Nuclear Power. The software is currently being used in CERN, Switzerland for various availability and reliability calculation [5]

Reliability Workbench is an integrated environment for performing Fault Tree Analysis, FMECA, Event Tree Analysis, Reliability Prediction, Allocation and Growth, Maintainability Prediction, Reliability Block Diagram Analysis, Weibull Analysis and Markov Analysis. The integration of the different workbenches allows for ease sharing of data, entering data only once and unlimited entries. The software supports multiple standards of the system analysis including ARP 4761, ISO 26262, IEC 61508. The tool effectively predicts the electronic and mechanical components reliability using GJB299C, IEC TR 62380, Quanterion 217 Plus, FIDES, MIL-217 and NSWC.

IV. QUALITATIVE ANALYSIS

A. Failure Condition Identification Matrix (FCIM)

The Failure Condition Identification matrix is developed to find all the failure conditions corresponding to the Functions at the system level, where the crew is aware and not aware conditions. The Failure conditions are shortlisted to eliminate the redundant failure conditions, in the case we consider the failure conditions to be unique, corresponding to the functions. These failure conditions are input to the System Functional Hazard Assessment. The table 4.1. shows the few rows of how FCIM matrix is performed.

1) Possible Failure conditions considered:

The possible failure condition which might occur during the aircraft flight consisting of the various flight phases having effect on crew, occupants and aircraft are considered as shown below for the case of the normal and emergency wheel braking of the main landing gear brake system.

a) Normal wheel Braking failure conditions:

Total loss of the Normal wheel braking:

This failure condition addresses the Total loss of the ability of the normal wheel braking to provide braking. The failure condition is at system level and it considers only the landing gear brakes operation. This failure condition occurs by the loss of the both outboard and the inboard brakes of the brake system.

Partial loss of the Normal wheel braking:

The partial loss of the ability of the normal wheel braking to provide braking is considered. The failure condition occurs by the loss of the outboard brakes or the loss of the inboard brakes. The parking brakes are not considered.

Uncommanded more than commanded of the Normal wheel braking (crew doesn't apply brakes, gets full brakes):

The failure condition arises when there is uncommanded braking more than commanded by the crew i.e. brakes are applied more than required. This failure condition considers the case of, crew does not apply the brakes but gets full brakes on the main landing gear wheels. The application of brakes is against the intention of the crew. If this condition arises during the cases such as landing, the severity is not much but the application after reaching the V1 speed, would be catastrophic as seen in the qualitative analysis of SFHA. This failure condition is a question of integrity of the system.

Uncommanded more than commanded of the Normal wheel braking (crew applies light brakes, gets full brakes):

The failure condition occurs due to the malfunction of the LRU's present in the brake system. In the uncommanded more than commanded crew applies light brakes but gets full brakes, the crew's intention is to apply light brakes but the brakes are fully applied. This failure condition might result in effects on the crew, aircraft and occupants.

Uncommanded less than commanded of the Normal wheel braking:

The failure condition occurs when the crew applies the brakes but the required braking is not obtained for the deceleration of the aircraft. This failure condition results in movement of the aircraft out of the runway during landing and rejected take-off. It is a possible failure condition which would occur.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

b) Emergency wheel Braking failure conditions

The emergency wheel braking is explained in detail in the section 4.1.1. (b)

Total loss of the Emergency wheel braking:

The failure condition result in total loss of the ability to provide emergency wheel braking. This failure condition is said to occur, by considering the loss of the outboard or inboard brakes as well as the loss of the inboard or outboard parking brakes. The pilot can apply the park brakes on receiving the 50% degraded CAS message.

Partial loss of the Emergency wheel braking:

The partial loss of the emergency wheel braking is nothing but the total loss of the emergency wheel braking i.e. failure of the either inboard or outboard brakes along with failure of the parking brakes on the similar sides. This have qualitatively understood from the FCIM.

Uncommanded more than commanded of the Emergency wheel braking (crew doesn't apply brakes, gets full brakes):

The failure condition arises when there is uncommanded braking more than commanded in case of emergency wheel braking. This failure condition considers the case where crew does not apply the brakes but gets full brakes. The application of brakes is against the intention of the crew. If this condition arises during the phases such as landing, the severity is not much but the application after reaching the V_1 speed during takeoff, would be catastrophic, where the crew is neither able to reach the V_R speed nor able to stop the rejected take-off.

Uncommanded more than commanded of the Emergency wheel braking (crew applies light brakes, gets full brakes):

The failure condition arises when the crew applies the emergency brakes for decelerating or stoppage of the aircraft, but the brakes applied are less due to the malfunction of the LRU's present.

Uncommanded less than of the Emergency wheel braking:

The uncommanded emergency braking less than commanded is caused when the crew wants to apply the brakes during the phase such as landing but the brakes applied are less than anticipated which may due to the malfunction of the LRU's, error in signals sent from the pilot pedal to the signals sent from the BSCU to the mechanical items such as Brake control valve and shutoff valve.

Table 4.1: Failure condition Identification matrix

System Function	Crew Aware (Y/N)	Total Loss	Partial Loss	Uncommanded braking (Malfunction of the LRU's)		
SRD						
Normal Wheel Braking	Y	Total loss of the capability to provide normal wheel braking to the aircraft while on the ground BS-1.1	Partial loss of the capability to provide normal wheel braking to the aircraft while on the ground BS-1.2	Uncommanded braking more than commanded due to Malfunction (crew applies light brake, gets full brakes) BS-1.3	Uncommanded braking more than commanded due to Malfunction (crew doesn't apply brakes, gets full brakes) BS-1.4	Uncommanded braking less than commanded due to Malfunction BS-1.5
	Y		Loss of Right MLG pair/Left MLG pair/Inboard or outboard brakes/ Right inboard /Left outboard / Left inboard/Right outboard brakes			

B. System Functional Hazard Assessment (SFHA)

The System Function Hazard Assessment consists of classification of the shortlisted failure conditions in the FCIM, based on the different flight phases. The qualitative analysis is done for the failure conditions, the effects of the failure conditions on the crew, occupants and aircraft are noted. Based on the effects the hazard classification is obtained to the failure condition. All the Hazards corresponding to the Failure conditions are identified and documented, Few rows of the SFHA is as shown in the Table 4.2. The highest hazard classification for each failure condition is passed on the Driver requirement matrix. These are passed on to the Driver requirement matrix. The flight phases for simplicity are made into stages as shown in the Table 5.1.

Table 5.1: Flight Phases Stages

Stage 1	Static	Taxi		
Stage 2	Prior to V1	After V1		
Stage 3	Rejected Take-off	Landing		
Stage 4	Balked Landing/ Missed Approach	Climb	Cruise	Descent

Table: System Functional Hazard Assessment

Item	Case	Failure Condition (Hazard Description)	St 1	St 2	St 3	St 4	Effect of Failure on Aircraft/Crew/Occupants	Hazard Classification
Function:		Normal wheel braking (crew aware)						
1.1	1	Total loss of the capability to control the speed of the aircraft while on the ground	X				**Aircraft:** The total loss of the normal wheel braking causes slight reduction in functional capabilities. **Flight Crew:** The total loss can be easily recognized by keeping an eye on the speed, slight increase in crew workload. **Other Occupants:** The total loss causes physical discomfort for passengers.	MIN
	2				X		**Aircraft:** The total loss of the braking results in high speed movement of the aircraft out of the runway resulting in hull loss. **Flight Crew:** The total loss suddenly increases the crew workload. The crew cannot be relied upon to perform assigned tasks effectively. **Other Occupants:** The total loss causes fatal Injury or incapacitation of the occupants.	CAT
	3			X		X	The Brakes are not used during these phases	NA

C. Driver Requirements Matrix (DRM)

The Driver requirement Matrix is also called as Preliminary System Safety Assessment Matrix, few rows of it is as shown in the Table 4.3. The critical failure condition is obtained by checking if the failure condition could drive other failure condition. Only the driver conditions are considered for performing the fault tree analysis. Since it is the worst-case condition and is most conservative. This helps us to keep a track of the failure conditions and helps us to get more accurate requirements and reduce the time by avoiding development of fault trees for all failure conditions.

Table 4.3. : Driver Requirement Matrix

Syscode.Item #.Case #	Failure Condition Description	Hazard Class	Requirement Identifier	Driving Requirement	Justification
Function:	**Normal wheel braking (crew aware) The crew awareness is ineffective**				
BS-1.1	Total loss of the ability to control the speed of the aircraft while on the ground.	CAT	PSSA-BS-1.1.2-PR1	PSSA-BS-1.2.2-PR1	Partial loss is more severe as per PR, even though Total loss meets PR, partial loss doesn't.
BS-1.1.2	Total loss of ability to provide normal wheel braking.	CAT	PSSA-BS-1.1.2-FDD1	PSSA-BS-1.2.2-FDD1	
BS-1.1.2	Total loss of ability to provide normal wheel braking.	CAT	PSSA-BS-1.1.2-NSF1	DR	Requirement for CAT event
BS-1.2.2	Partial loss of the capability to control the speed of the aircraft while on the ground.	CAT	PSSA-BS-1.2.2-PR1	DR	The partial loss PR is difficult to achieve, considering the worst-case partial loss is considered as driver.
BS-1.2.2	Partial loss of the capability to control the speed of the aircraft while on the ground.	CAT	PSSA-BS-1.2.2-FDD1	DR	
BS-1.2.2	Partial loss of the capability to control the speed of the aircraft while on the ground.	CAT	PSSA-BS-1.2.2-NSF1	DR	

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

D. Development of Fault trees for the failure condition of the architectures .

The Fault trees are developed for the failure conditions shortlisted in the Driver Requirement Matrix shown earlier. From the DRM, 6 critical failure conditions were shortlisted due to the criticality. The fault trees were developed for the same with the help of the Brake system architecture. Excessive care must be taken such that all the events are considered.

The Fault tree analysis is a top-down analysis technique in which undesired failure condition is analyzed using the Boolean logic consisting of simpler AND and OR gates to show the relationship between the failure conditions and failure modes. An AND-gate is a condition, which requires the coexistence of all the inputs to produce an output which represents the event at a higher level. An OR-gate is a condition, which requires one or more inputs to produce an output which represents the higher-level event.

V. SENSITIVITY ANALYSIS

The Fault trees are built for the architectures 1,2 and 3 using the isograph reliability workbench v14.0. The Fault tree top level gates consisting of the failure conditions is as shown in the Fig. 5.1, Fig. 5.2, Fig. 5.3 for the architectures 1,2 and 3 respectively. The isograph reliability tool gives the output as the probabilities of failure and provides the minimal cut sets of failure.

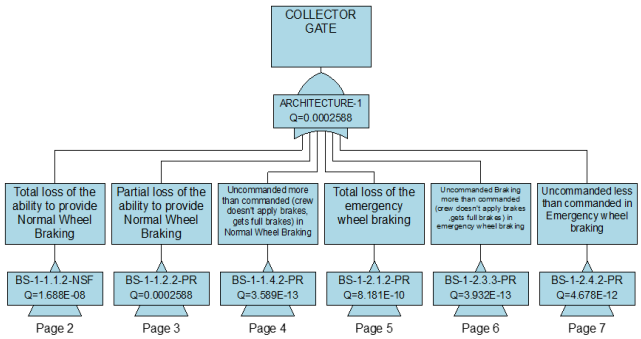

Fig 5.1 Top Level fault tree of Architecture 1

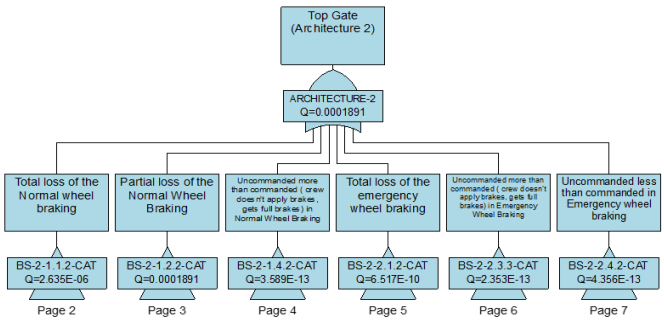

Fig 5.2 Top Level fault tree of Architecture 2

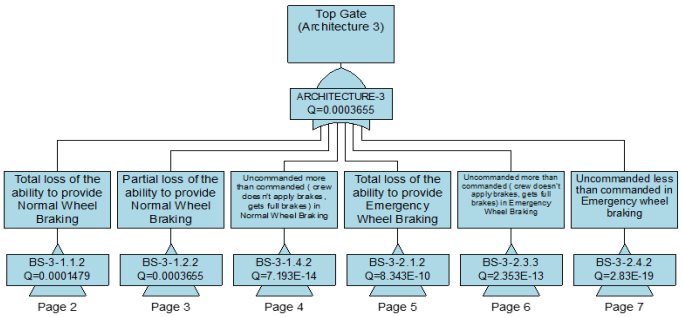

Fig 5.3 Top Level fault tree of Architecture 3

The architecture 1 of the brake system considers the ground brakes to have independent hydraulic systems with outboard and inboard brakes, where the hydraulic system A supplies power to outboard brakes and the hydraulic system B supplies power to the inboard brakes but has a single BSCU with 2 cores to operate the outboard and the inboard independently.

The architecture 2 of the brake system considers the brakes to be powered by both hydraulic system A and B of equal power with the help of a shuttle valve to allow the high pressure water from either of the hydraulics, the architecture 2 is also powered by a BSCU with 2 cores controlling the outboard and inboard brakes similar to the architecture 1.

The architecture 3 of the brake system considers the right and the left side to be fully independent considering the independent hydraulic system A to the right side and hydraulic system B to the left side brakes, independent BSCU's, the BSCU further has independent cores the inboard and the outboard brake of the right side and vice versa. Hence totally there are 4 cores in which each core controls each independent brake.

The parking brake architecture is similar in all the brake system architectures

The top-level fault tree consisting of the failure conditions is as shown along with failure of the probabilities.

A. Total loss of ability to provide normal wheel braking*:*

In the architecture 2, the probability of failure of the motive power can be seen improved as shown in the fault tree of the Fig 5.5. when compared with the fault tree in the Fig 5.6 from 4.85e-5 to 6.542e-7. The reduction in the probability of the failure of the architecture 2 is due to the presence of the single order cut set consisting of the main shuttle valve, this can be seen in the fault tree under loss of command/failure to apply brakes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

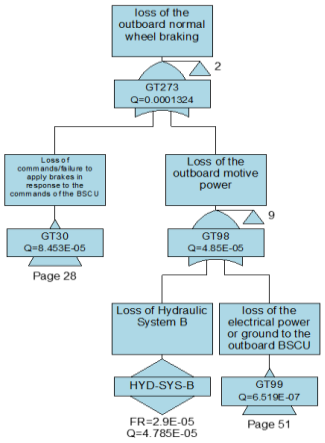

Fig 5.5 Fault tree of loss of the outboard normal wheel braking for Architecture 1

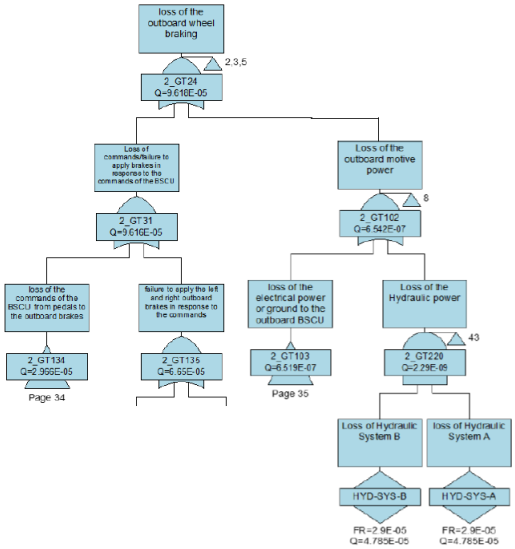

Fig 5.6 Fault tree of loss of the outboard normal wheel braking for Architecture 2

The reduction in the failure rate of the architecture 3 is owing to the failure of the hydraulic systems, hydraulic system to shutoff valve linkages, shutoff valves and the connectors, electrical fuses which supplies power to the BSCU. Since for example failure of the hydraulic system A, fails right inboard and right outboard brakes, this causes the total failure of the braking system. Similarly, failure of any of the electrical power supply components, will kill the electric supply to the BSCU which in turn kills power to the brakes.

B. Partial loss of ability to provide normal wheel braking

The probabilities of failure for Architecture 1, 2 and 3 respectively are 2.588e-4, 1.891e-4, 3.655e-4. The PR is complied to 14CFR 25.735 (b)(1) requirement, which required the aircraft to be brought to stop within twice the landing distance in the event of partial loss by using partial brakes along with other braking modes such as thrust reversers and spoilers, since the wheel braking failed to comply to 14CFR 25.1309 (b)(1). the number of single order cut sets are 71, in the architecture 2 and 3 it is 60 and 101 single failures.

In the Architecture 2 the number of cut sets have reduced, this is due to the robust hydraulics having multiple hydraulic systems, shutoff valves connection to both the outboard and inboard brakes.

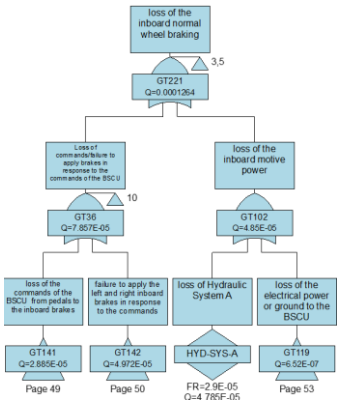

Fig V.7 Fault tree of loss of the inboard normal wheel braking for Architecture 1

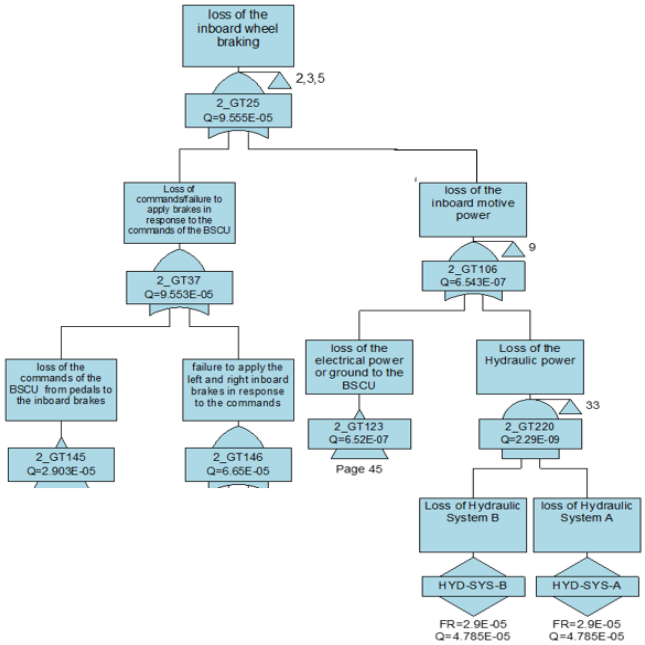

Fig V.8 Fault tree of loss of the inboard normal wheel braking for Architecture 2

From the fault tree in the Fig 5.6 and Fig 5.8 it is clearly seen that the motive failure probability had improved from 4.85e-5 in the Arc 1 to 6.543e-7 in Arc 2.In the Architecture 3, the number of cut sets are very high at 101 because of having independent system for each brake, loss of each independent systems at each brake is going to be partial loss failure condition and having independent BSCU's with independent connectors which failure could result in partial loss. The possible way of reducing single order cut sets is by providing multiple systems or components performing the same function. This helps to prevent single order cut sets.

C. Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) in Normal wheel braking

There is no single order cut sets present in any of the architecture 1,2 and 3. Hence the No single failure requirement is met by the failure condition. The probabilities of failure of the architecture 1,2 and 3 for the failure condition

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

respectively are 3.589e-13, 3.589e-13 and 7.193e-14.Error in the command of the shutoff valve, the architecture 2 has two shutoff valves and 2 hydraulic systems. Hence the chances of the uncommanded application of the normal wheel braking must be more, hence there is a slight increase in failure i.e. 2.087e-6 in architecture 1 and 4.17e-6 in architecture 2, The top level probability of failure of arc 2 is same as arc 1 this is because the uncommanded application of the LVDT coils of pedal position sensor is more than the uncommanded application of the additional shutoff valves and the hydraulic systems in both architecture 1 and 2 The architecture 3 failure probability is better than the other architectures as shown in Fig 6.16. The reason for this is the presence of the independent BSCU's for each BCV, shutoff valve left and right operation. The uncommanded application of the inboard is considered only if both inboards uncommanded more than commanded application occurs similarly to the outboard. The uncommanded application is only from the malfunction of the LVDT pedal position sensor.

D. Total loss of ability to provide emergency wheel braking

The probability of occurrence of the architecture 1 is worse than architecture 2 but better than architecture 3. The architecture 2 has better probability because it is having multiple hydraulic systems, shutoff valves connection to both the outboard and inboard brakes i.e. failure of the one hydraulic system or the shutoff valve doesn't lead to the failure condition. The architecture 3 probability is slightly worse because of having just one power supply connection to the BSCU whereas Arc 1, Arc 2 BSCU has multiple power supply connection. The one power supply is provided as a trade-off for having independent BSCU. The Fig 6.9 and Fig 6.10 shows architecture 1 powered by 2 supplies and architecture 3 powered by one supply.

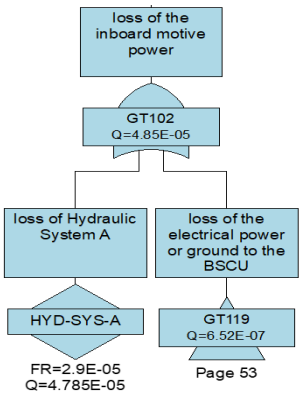

Fig V.9 Loss of the inboard motive power for Architecture 1

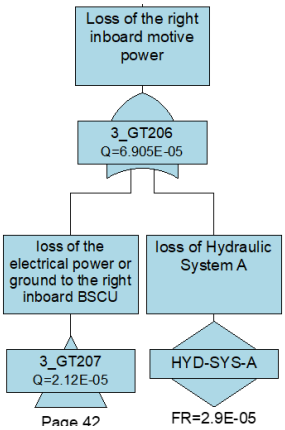

Fig V.102 Loss of the inboard motive power for Architecture 3

E. Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) in Emergency wheel braking

The probability of occurrence is almost same in all the above architectures, this is because the probability LVDT coil i.e. 2.682e-7 is more than any other uncommanded application since the hardware monitor is present to prevent BSCU faults as shown below in Fig 6.11, 6.12 and 6.13 for architecture 1, 2 and 3 respectively.

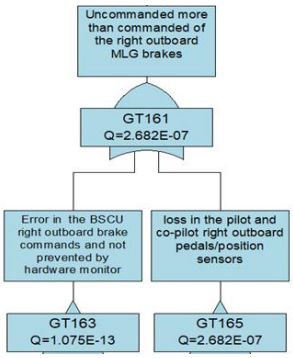

Fig V.11 Fault tree for right OB Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) in Emergency wheel braking for Architecture 1

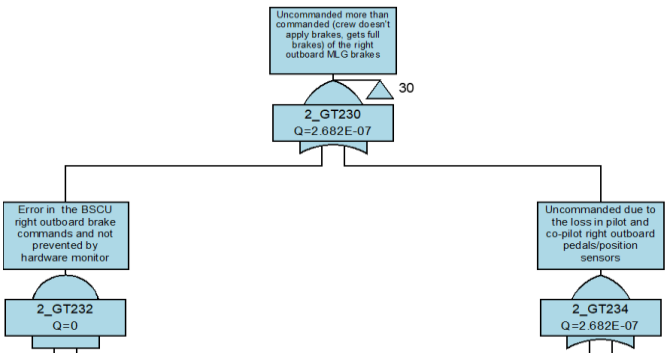

Fig V.12 Fault tree for right OB Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) in Emergency wheel braking for Architecture 2

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

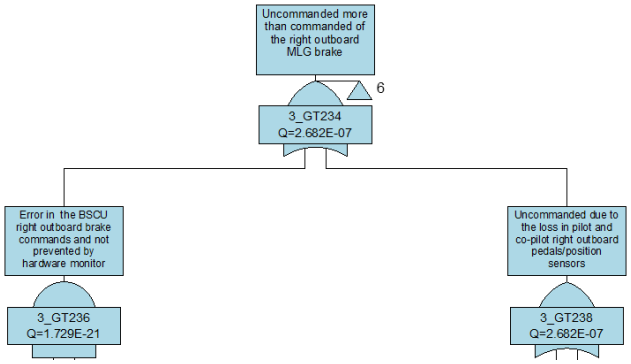

Fig V.13 Fault tree for right OB Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) in Emergency wheel braking for Architecture 3

F. Uncommanded less than commanded in emergency wheel braking

The probability of failure of architecture 1,2 and 3 respectively are 4.67e-12, 4.35e-13 and 2.83e-19. The number of second order cut sets present are 4,12 and 0.

The architecture 3 probability of failure is very much better than that of architecture 1 because of having 2 shutoff valves and brake control valves, hydraulic systems etc. for the inboard and the outboard brake. For e.g. the right inboard brake has hydraulic system A, right shutoff valve and right brake control valve whereas the left inboard brake has hydraulic system B, left shutoff valve and left brake control valve, similarly for outdoor brakes. Hence both must fail partially for uncommanded less than to happen. In arc 1 and arc 2 the IB are connected to one shutoff valve and OB to the other.

If we just perform analysis for architecture 3 and 1 considering the avionics only. From fault tree in the figure 6.14 and 6.15 the probability of failure is 8.984e-22 in architecture 1 and 1.334e-28 in architecture 2 respectively. This is due to the presence of 2 BSCU with 4 channels existing in the architecture 3.

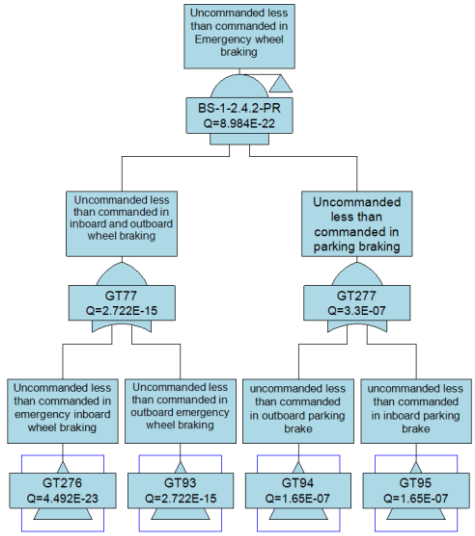

Fig V.14 Fault tree of Uncommanded less than commanded in emergency wheel braking for Architecture 1 without mechanical failures

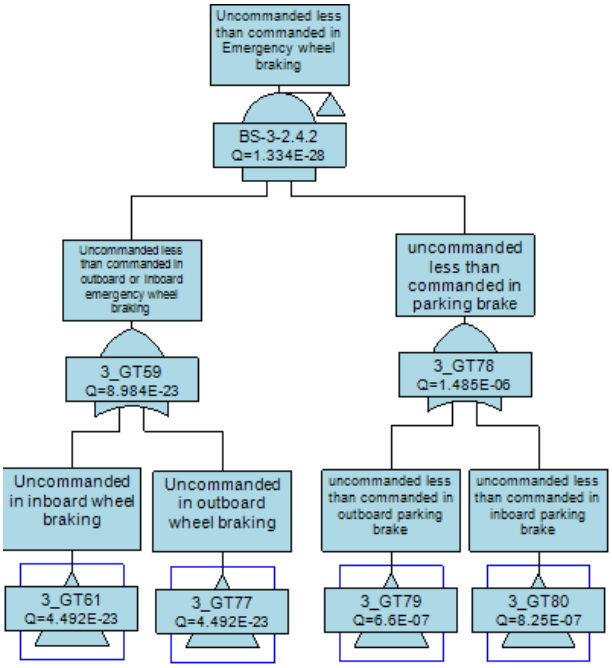

Fig V.15 Fault tree of Uncommanded less than commanded in emergency wheel braking for Architecture 3 without mechanical failures.

VI. CONCLUSIONS

The system safety analysis was performed for the aircraft braking system having normal and emergency wheel braking. The safety analysis was performed as per the ARP 4671 and ARP 4754A guidelines. The safety assessment was initially performed for the architecture 1 following ARP 4754A process consisting of FCIM, SFHA and DRM, FTA was performed for architecture 1. The similar iterative procedure was performed for the architecture 2 and 3. The sensitivity analysis was performed which compared the architectures 1, 2 and 3. The following conclusions were arrived at:

- The Crew not aware case comes under crew aware, since all the failure conditions are inherently detectable
- The analysis was performed for the entire flight phase without considering the time at risk, this means the actual probability of failure is better than the probability of failure obtained in the software. The brake failure is applicable to only one flight as it is always checked during takeoff and previous landing
- For the total loss failure condition of the normal wheel braking, the architecture 1 is a best choice because there is No single failure present and the probability of failure is 1.668e-8 when compared to 2.635e-6 and 1.479e-4 of the architecture 2 and 3 respectively.
- For the partial loss failure condition of the normal wheel braking the architecture 1,2 and 3 are not meeting the NSF and the PR. The single order failure and the probabilities of failure of architecture 1,2 and 3 respectively are 71, 60, 101 and 2.588e-4, 1.891e-4, 3.655e-4. The architecture 1 wasn't meeting the PR and NSF, but the failure condition was complied to 14CFR 25.735 (b)(1) which required the aircraft to be brought to stop within twice the landing distance in the event of partial loss by using partial brakes

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

along with other braking modes such as thrust reversers and spoilers. This requirement was met.

- The Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) failure conditions in Normal wheel braking, all the architectures met PR and NSF conditions.
- The Total loss of ability to provide emergency wheel braking failure condition, all the architectures met the PR and NSF conditions.
- The Uncommanded more than commanded (Crew doesn't apply brakes, gets full brakes) in Emergency wheel braking failure condition has met all the PR, NSF requirement.
- The Uncommanded less than commanded in emergency wheel braking, all the architectures met PR and NSF requirement.
- The critical system found is the hydraulic system in all the architectures, the main shuttle valve is the critical element in architecture 2.
- The DAL allocation was performed and the IDAL were found from the FDAL for all architectures Failure conditions.
- The study on how the failures impact design changes in terms of reliability, how system safety directs design features, how multiple resource systems design affect system design
- Cost to develop or change
- It can be concluded that architecture 1 is the better choice since there are no single failures present in most of the failure conditions except for partial loss of the normal wheel braking but it is complied to 14CFR 25.735 (b)(1), the complexity is lesser than architecture 3 and no single failure such as main shuttle valve in architecture 2.The architecture 3 is better choice over the 2 architectures 1 and 2 for uncommanded failure conditions, which is due to the malfunction of the LRU's present, this is due to the presence of multiple BSCU which improves the possibility of failures.

REFERENCES

[1] M. Allocco, G. McIntyre, and S. Smith, The Application of System Safety Tools, Processes, and Methodologies within the FAA to Meet Future Aviation Challenges, in Proc. 17th International System Safety Conference, (1999).

[2] SAE International, ARP 4761, Guidelines and Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment, (1996)

[3] SAE International, ARP4754-A, Guidelines for Development of Civil Aircraft and Systems, (2010)

[4] Shruti Nair, Shreya Nair, Aircraft Braking System, International Journal of Research in Mechanical Engineering & Technology (2014) Vol. 4, Issue 1.

[5] E. Blanco, S. Karstensen, T. Ladzinski, J. Lindkvist, T. Lensch, A. Marqueta, D. McGinnis, A. Nordt, et al., Workshop on PLC Based Interlock Systems for Accelerators and Other Large Research Installations, ESS Accelerator Division. (2013).