

CHAPTER 7

FAILURE MODE AND EFFECTS ANALYSIS AND FAULT TREE ANALYSIS OF PARACHUTE DECELERATION SYSTEM

Abbreviations

FMEA	Failure Mode and Effects Analysis
FM	Failure Mode
FTA	Fault Tree Analysis
MCS	Minimum Cut Set
MiL-STD	Military Standard
NASA	National Astronautics and Space Administration
PDS	Parachute Deceleration System
RBD	Reliability Block Diagram
RCM	Reliability Centered Maintenance
RPN	Risk Priority Number
D	Detection
O	Occurrence
S	Severity

7.1 Introduction

Although the components are designed with all precautions and using proper safety factors, the failures cannot be avoided completely, particularly in textile-made items. The reasons could be many, such as, degradation of materials, mishandling during packing or manual

operation, sharp edges, rubbing/abrasion, adverse environment, etc. To investigate the impact of these drawbacks, FMEA, FTA and reliability analysis is required to be carried out.

The intent of this chapter is to find out the root cause of failure and to provide solution for avoiding these failures using combined FTA-FMEA model. This combined methodology assesses the internal risks that may occur during the design, manufacturing and strategic operation.

FMEA was originally used by NASA to improve and verify the reliability of space program formally introduced in mid-1960, and also to examine the safety and failure modes of the components within a system. It traces the potential effects of each component failure mode on the system performance. It is basically a cause-effect model. It is a preventive approach used to design products and processes. It assures that both design and manufacturing quality objectives consistently meet the system requirements (Robert, 1993). MIL-STD-1629A (1980) consists of the detailed procedures for performing FMEA. This methodology is designed to identify potential failure modes for a product or process, to assess the risk associated with those failures, to rank the issues in terms of importance and to identify and perform corrective actions to address the most serious concerns.

On the other side, FTA is a top-down Boolean logic tool commonly used to identify possible causes for potential operating hazards or an undesired event. This technique was formerly developed by Watson in 1962 at Bell Telephone Laboratories in USA for safety evaluation of the Minuteman launch control system. FTA does not necessarily contain all possible failure modes of the components of system, but only those failure modes that contribute to the existence or occurrence of the top event.

7.2 FMEA Approach

The primary objective of a FMEA is to improve the design of the subsystem or component and system. FMEA is performed early in the design stages of a new product or system as a way of discovering failures so that necessary corrective actions could be planned. Carlson (2012) has explained the process of FMEA. The objective is to improve the design of the manufacturing process. Anthony (1996) has formulated the requirements and identification of FMEA. FMEA Task 101 (Carlson, 2012; and Robert *et al.*, 1993) explains it as the combined influence of severity classification and its frequency of occurrence can be measured using the available data. Erik (2007) defined the severity as a ranking number associated with the most serious effect for a given failure mode and is based on the criteria from a severity scale. Severity of failure is a relative measure of the consequences of the failure mode.

7.2.1 FMEA Rating Scale

FMEA rating scale differentiates the level of severity, occurrence and method of detection of any failure mode of the item. It gives rating on a scale of 1 to 10, with a number signifying a different criterion. In general, criteria of rating for levels 1 to 3 are very low, for levels 4 and 5 is low/moderate, for levels 6 to 8 is moderate/high, for levels 9 to 10 is very high (Kulkarni and Srivastava, 2013). Tables 7.1 to 7.3 show the quantitative scales used in the present work for identifying the severity, occurrence and detectability indices.

7.2.2 Risk Priority Number

The RPN is used to rank the risk for corrective actions to eliminate or reduce the potential failure modes. RPN rates the risks based upon three factors, namely, severity, occurrence

and detection. Rating of these factors is based upon a predetermined scale, low to high. To use the RPN method for assessing the risk, the analysis must have:

- (i) Rate the Severity of each effect of failure,
- (ii) Rate the likelihood of Occurrence for each cause of failure,
- (iii) Rate the likelihood of prior Detection for each cause of failure, and
- (iv) Calculate the RPN by obtaining the product of the three ratings.

Table 7.1: Severity rating scale for PDS

#	Description	Criteria
1	No effect	No discernible effect on parachute
2	Annoyance	Appearance, operable, parachute does not conform (< 25%).
3	Annoyance	Appearance, operable, parachute does not conform (50%)
4	Annoyance	Appearance or operable, parachute does not conform (> 75%).
5	Degradation of secondary function	Degradation of materials of secondary function parachute
6	Loss of secondary function	Loss of secondary function of parachute or items
7	Degradation of primary function	Degradation of primary function of parachute
8	Loss of primary function	Loss of primary function of parachute
9	Safety/regulatory compliance	Non-compliance with government/space regulation with warning
10	Safety/regulatory compliance	Non-compliance with government/space regulation without warning

Table 7.2: Occurrence rating scale for PDS

#	Description	Criteria
1	Very Low	Failure can be eliminated through preventative control
2	Low	No failures were observed in an identical design
3	Low	Only isolated failures were observed in an identical design
4	Moderate	Isolated failures were observed in a similar design
5	Moderate	Occasional failures were observed in a similar design
6	Moderate	Frequent failures were observed in a similar design
7	High	Failure is uncertain in the new design
8	High	Failure is likely to occur in the new design
9	High	Failure is inevitable in the new design
10	Very High	New technology/design has no history

Table 7.3: Detection rating scale for PDS

#	Description	Criteria
1	Detection not applicable	Failure cannot occur because it is fully prevented through design solutions
2	Virtual analysis	Has a strong detection capability
3	Prior to design freeze	Product validation prior to design freeze using degradation testing
4	Prior to design freeze	Product validation prior to design freeze using test to failure
5	Prior to design freeze	Product validation prior to design freeze using pass/fail testing
6	Post design freeze & prior to launch	Product verification prior to launch with degradation testing

7	Post design freeze & prior to launch	Product verification prior to launch with test to failure testing
8	Post design freeze & prior to launch	Product verification prior to launch with pass/fail testing
9	Difficult to detect	Design analysis/detection controls have a weak detection capability
10	Absolute uncertainty	No current design controls. Cannot detect or cannot be analysed.

Yahia (2018) has explained RPN goal and priority model to optimize the failure cost and RPN risk associated with the overall system. RPN is calculated using equation (7.1).

$$\mathbf{RPN = Severity (S) \times Occurrence (O) \times Detection (D)} \quad (7.1)$$

Since, each of the three factors vary from 1 to 10, RPN can get a value between 1 and 1000.

Therefore,

$$1 \leq \text{RPN} = S * O * D \leq 1000$$

If RPN is the same for any two or more components, severity and occurrence are to be given priority. One should assign a threshold RPN value to classify the failure modes. Since the space mission is a very capital-intensive program and any failure is likely to cause death of astronauts and loss of CM, a failure mode with $\text{RPN} \geq 48$ (a low value) is considered as the ones with ‘corrective action definitely required’. Failure modes with RPN in the range of 25 to 47 are classed as the ones with ‘scope for corrective action’. Based on experience and testing, the following RPN limits for the deceleration parachute system were considered.

RED RPN \geq 48

YELLOW $47 \geq$ RPN \geq 25

GREEN $24 \geq$ RPN \geq 1

The failure modes with the highest RPN should be given first priority. Once corrective action has been taken, a new RPN is determined by re-evaluating the severity, occurrence, and detection ratings. Improvement and corrective actions must continue until the revised RPN is at an acceptable level for all potential failure modes.

7.3 FMEA of Parachute Deceleration System

In the parachute decelerator system, single point failure is avoided by providing sufficient margin of safety and / or redundancy in each subsystem. Therefore, in the present research, the failure modes are identified on a single component basis. The failure mode and effects analysis of the deceleration system is ranked according to their probability of failure. It is further classified into their components.

Major points of failure modes are identified in the following areas:

- (i) Device/ Sensor failures,
- (ii) Design related failures,
- (iii) Failures due to defective materials, and
- (iv) Interfacing with parachute and CM.

No single point failures in devices are accepted in the system. Each and every functional device is provided with redundancy. These issues are to be well addressed during the

design, manufacturing and packing of parachutes. The single point failure modes related to material are:

- (i) Failure of parachute fabric, tapes, suspension-lines and riser,
- (ii) Joint failures on gores,
- (iii) Failure of parachute anchoring pin, and
- (iv) Failure of metallic component.

Material failures are treated as a single point failure of individual parachutes and this may not lead to mission failure. But the failure of parachute anchoring pin will definitely result in the failure of the mission.

7.3.1 TCS Chute

Failure of TCS chute could lead to the failure of the mission. This system consists of two small chutes having diameter of 2.50 m. It carries away the forward heat shield of module to avoid collision with CM. Detailed FMEA of this chute is described in Table 7.4.

Table 7.4: FMEA of TCS chute

#	Item / function	Potential failure mode	Potential effect(s) of failure	S	Potential cause(s) of failure	O	Current design controls (Prevention)	Current Design Controls (Detection)	D	RPN
1	Altitude sensor -Senses the altitude during re-entry	Sensor fails	No signal to Pyro-thrusters	2	Improper orientation. Disabled by OBC	2	Testing Add one standby sensor	Display on dashboard	2	6
2	Velocity sensor – Senses the speed of the CM	Sensor fails	No signal to Pyro-thrusters	2	Improper mounting	2	Test mounting of sensor	Display on dashboard	2	8
					Disabled by OBC	2	Put one as a standby		3	12
3	Altitude & velocity sensor	Both malfunction	No separation of forward heat shield	7	Improper orientation Disabled by OBC	1	HALT SST	Inspection/ Replacement Ground testing	2	14

4	Pyro-Thrusters – to release the forward heat shield from CM	Malfunction	Sever damage of CM	8	No signal from OBC	2	Continuity test	Design as per MiL grade	2	32
					Defective pyro-bolts	2	Pre testing & Inspection		2	32
5	Mortar 1 & 2- to deploy the chutes	Ignition failure	One chute fails	3	Gas generator failure	2	Design analysis	Review the design Inspection & replacement	2	12
6	Both mortars deploy the chutes 1 & 2	Mortar not fired	Chute will not be deployed	7	Gas generator fails No signal to mortars	2	Design review	Inspection & dynamic test		
7	Apex weak-tie - attachment b/w chute and extraction bridle of TCS pack cover	Premature breakage	Improper deployment	4	Over-stress	2	Re-design	Strength test	6	48
		Weak-tie remained tied	Sabot and TCS pack cover will remain attached	5	Over-design	3			3	45
8	Pack cover - Helps in deployment of chute in sequential order	Cuts on pack cover	Chute will be damaged	5	Abrasion Ambient condition rigorously changed	2	Cater sufficient safety factor in design Select smooth material	Inspection & replacement	4	40
		Mouth weak-tie remains unbroken	Fails to deploy the chutes	8	Weak-tie is under-load	2	Re-design	Inspection & bench test	2	32
9	Chute 1 st or 2 nd – To separate the forward heat shield from CM	Fails to deploy	Forward heat shield remains attached with CM	5	Improper angle of deployment Rotation in chutes	3	Both mortars must fire in right direction	Simulated test on ground	6	90
10	Both TCS chute - To separate the forward heat shield from CM.	Chute entanglement Delay in Mortar firing	Re-contact of forward heat shield with CM	8	Material defects	2	High packing reliability Signal must pass at same time in both the mortars	Simulated test	6	96
11	Riser –It is link between the suspension-lines and forward heat shield	Riser broken	Forward heat shield free fall and may hit to CM	8	Material defect Abrasion with edge of CM	2	Re-design	Inspection & replace	2	32
12	Suspension-lines–Maintain the required shape of canopy	Breaking of suspension-lines(s)	Forward heat shield fall free	8	Over-stress Unequal length	2	Re-design	Inspection & replace	2	32
		Entanglement b/w the lines	Rotation in chutes	5	Design fault	2	Review the design Maintain equal length of suspension-lines	Wind tunnel test	3	30

7.3.2 Pilot Chute

FMEA of pilot chute investigates the severity of risks and their occurrence along with method of detection of the failure mode. Pilot chute system is responsible for the deployment of the drogue parachute. Therefore, FMEA of the pilot chute is to reduce/eliminate some of failures and occurrences in deployment of drogue parachute system. Failure of pilot chute cause non-deployment of drogue parachute which will results in system catastrophic failure. The detailed FMEA of pilot chute is presented in Table 7.5.

Table 7.5: FMEA of pilot chute

#	Item\ function	Potential Failure Mode	Potential Effect(s) of Failure	S	Potential Cause(s) of Failure	O	Current Design Controls (Prevention)	Current Design Controls (Detection)	D	RPN
1	Mortar 3 or 4 to deploy the pilot chute 1 or 2	Ignition failure& Signal failure	Malfunction	4	Pin remains un-sheared	2	Re-design & testing	Inspection & replacement	2	16
2	Both Mortars to deploy the pilot chutes	Ignition failure No signal	Both malfunction	9	Gas not generated Pin remain un-shear	2	Design analysis & testing	Inspection & replacement	2	36
3	Pack covers (both) - Container for chute packing & to deploy chutes in sequential order	Damage fabric	No effect	2	Material defect	2	Re-design	Inspection	4	16
		Mouth weak-tie remain unbroken	Chutes fail to deploy Tear of fabric	8	Under-stress	2	Re-design	Bench test and Inspection	3	48
4	Chute 1or 2- To deploy the Drogue parachute	Malfunction	Entanglement Redundancy will be vanished	5	Improper angle of deployment Insufficient ejection energy	3	Fire the mortar in different direction	Simulated test	2	30
5	Chute(both) – Extraction of drogue parachutes	Malfunction Material degradation	Drogue Parachute will not be deployed	9	Partial deployment	2	Faulty design Insufficient design factor	Over-load test	3	54
6	Apex weak-tie - Attachment between chute & extraction bridle of pilot pack cover	Premature breakage Improper knotting	No deployment of pilot chutes	7	Over-stress	4	Review the design	Bench test	6	168
		Weak-tie remains tied	Sabot with pack cover will remain attached with pilot chute	5	Under-load	2	Design analysis	Test	3	30

7	Riser -Attachment between suspensions lines and Drogue pack cover	Broken riser Abrasion of riser	Drogue Parachute will not be deployed Damage of CM Mission failure	9	Over-stress, Poor quality material, Rubbing with edge of CM	2	Sufficient design factor, Use steel riser or Teflon/Kevlar sheath cover over riser	Inspection and carry out Simulated tests	6	108
8	Suspension-lines - To maintain the required shape of canopy	Broken lines Entanglement of lines	Drogue Parachute will not be deployed Sever damage to CM	9	Over-stress, Uneven length of lines	2	Sufficient of design factor	Inspection	4	72
					Joint's failure Material degraded				3	4
9	Extraction bridle – interface between pack-cover & weak-ties	Defective bridle lines, Poor quality material	Main parachute will not be extracted	9	Over -tress	2	Sufficient design factor	Inspection & test	6	108

7.3.3 Drogue Parachute

Drogue parachute is the first stage decelerator consisting of a cluster of two parachutes, one functions as an active redundant. This parachute allows for tremendous drop in the descent velocity of the CM. Failures in drogue parachute will lead to severe mission operation. Therefore, the objective of FMEA for drogue parachute system is to eliminate and / or reduce the failures. The detailed FMEA carried out for the drogue parachute is presented in Table 7.6.

Table 7.6: FMEA of drogue parachute

#	Item\ function	Potential Failure Mode	Potential Effect(s) of Failure	S	Potential Cause(s) of Failure	O	Current Design Controls (Prevention)	Current Design Controls (Detection)	D	RPN
1	Drogue Parachute – To decelerate the CM and extract the main parachute	No deployment of parachutes Only one drogue parachute deployed	CM destabilises& falls freely, Partial recoverability	8	Packing fault Forebody wake effect Material defect	3	Sufficient design margin	No control	10	240

2	Riser – Link between the suspension-lines & PRUs	Breakage Abrasion	CM fall free Damage of CM Loss of Mission	10	Material defect Over-stress Burn cuts at riser lengths Poor stitching	2	Review the design & Replacement	Stress analysis Inspection & testing	5	100
3	Suspension-lines - Maintain the required shape of canopy	Breakage Joint fail	Reduce recoverability	8	Tight pack	2	Packing carries out as per instruction	Pre-flight inspection & lines replacement	5	80
					Material defect Burn cuts Uneven line's length	5	Material analysis Check lines dimension		3	
		Line's entanglement	CM oscillates Trajectory change	10	Rotation in parachute Incorrect line's length	5	Wind tunnel test Pack as per instruction	Pre-flight inspection Correct the line's length	5	250
4	PRUs – parachute disconnect mechanism	Breakage	No release Main Parachute will not be deployed	10	Material defect & Over-stress	2	Use rugged designed PRU	Inspection & replacement	6	120
		Premature release	Main parachute deployed above 3km altitude	10	Design fault	2	Design analysis	Testing & replacement	6	120
5	Main extraction bridle – interface between the pack-cover and weak-ties	Breakage	Main parachute will not be extracted Damage of CM	5	Over-stress, tight packing & material defects	2	Design factor QA checks	Pack as per instruction	3	60
6	Pack-cover – container in which retains the parachute to provides sequential deployment	Breakage Rough materials	High snatch force	5	Abrasion & uneven heating Tight pack	4	Faulty packing density & cotton to be used inside bag	Inspection & replace	2	40
		Mouth weak-tie remain unbroken	Parachutes failed to deploy	8	Under-load	3	Re-design weak-tie	Bench test and Inspection	3	72
7	Apex weak-ties –Connect between extraction bridle and vent lines of drogue	Premature breaking	Improper deployment	8	Over stress Material defects	3	Re-design	Inspection & replacement	4	96
		Unbroken	pack cover will remain attached with drogue	5	Under-load	2	Re-design	Inspection & replace	3	30
8	Extraction bridle – Link between pack-cover and weak-ties	Breakage	Main Parachute will not be extracted	10	Over-stress & material defect	2	Design analysis	Inspection & replacement	4	80

7.3.4 Main Parachute

The main parachute is at the final stage of PDS. It consists of cluster of two parachutes, one is kept as a, active redundant. FMEA of the main parachute system indicates the high severity and high occurrence failure mode of the component. Thus, there is a need to review the design so that RPN can be reduced to the acceptable level. The FMEA details are shown in Table 7.7.

Table 7.7: FMEA of main parachute

#	Item\ function	Potential Failure Mode	Potential Effect(s) of Failure	S	Potential Cause(s) of Failure	O	Current Design Controls (Prevention)	Current Design Controls (Detection)	D	RPN
1	Single parachute – Final stage retardation system	Malfunction No deployment Lines entanglement & breakage	Terminal velocity $\geq 10\text{m/s}$	8	Rotation in parachute, Apex weak-tie not broken & uneven lines' length	2	Wind tunnel test & Design review	Pre-flight inspection	5	80
2	Parachutes (both) – retard and bring safe landing < 8 m/s	No deployment, Entanglement of parachutes & Unequal inflation	CM fall with high rate of descent & Jerk on CM	10	Wrong packing, Rotation & Manufacturing fault	3	Proper packing, Wind tunnel test & Check the dimension	Inspection & drop testing	6	180
3	Reefing lines-cutter to disreefed the parachute	Premature cutting of reefing lines due to higher speed than specified	Fabric tear due to disreefed at high speed	8	Over-stress & Material defects	2	Increase delay time	Testing & Pre-flight inspection	8	128
		Failure of reefing lines-cutter	High terminal velocity	9	Failure of reefing lines & Cutter pin breakage	2	X-ray Ultra sound test & Connecting lines material test	Inspection & replace	3	54
4	Reefing lines - to reduce the size of parachute diameter	Breakage & improper reefing ratio	High opening shock force & unequal parachute opening load	6	Over-stress, material defects & design fault	2	Re-design	Sample testing & drop test	4	48
5	Riser No.1 or 2 – Attachment between the adopter and CM	Breakage & material flaws	High RoD	4	Over load, uneven length of riser & Stitching failure	2	Design review Joint test Higher MoS	Inspection & simulated test	5	40

6	Risers (both parachutes) attachment between adopter & CM	Breakage, layer friction & burning	High RoD Mission may fail Reduced recoverability	9	Rubbing with CM, Material defects & Resonance frequency	2	Design and analysis putting cotton between the layers & material test	Over-load test & check riser length position with CM to avoid edge rubbing	6	108
7	Riser loop-connect between riser end to CM	Breakage	CM falls free & high impact on ground	9	Stitching failures Material defects	2	Sufficient design margin & loop testing	Dynamic tests	3	54
8	Main PRUs – Disconnect the main parachutes	Breakage PRU not activated	CM will be dragged by parachutes	4	Material defects & no signal command to PRUs	2	Sensitivity analysis of sensors	Over-load test	3	24
9	Pack-cover – provide a safe enclosure & allow sequential deployment	Breakage & no stowing of ties	High parachute snatch load	5	Material defects, No weak-tie & human error	2	Material analysis	Inspection & fabric strength test	3	30
		Mouth weak-tie remain unbroken	Parachutes failed to deploy	8	Under-stress	2	Re-design	Bench test & inspection	2	32
10	Apex weak-ties it is tie between bridle & Vent lines	Premature breaking	Improper deployment	5	Over-stress & material fault	4	Design analysis & check the material quality	Material test & proper knotting of weak-tie	6	120
11	Adopter pin – Link between lines and riser	Breakage	Parachute detached	8	Over-stress & material defects	2	Design analysis & endurance strength	Over-load test	3	48
		Bend	No effect	8		2			2	32
12	Suspension -lines to maintain the shape of canopy	Breakage	High RoD & Reduced recoverability	8	Over-stress Material defects	2	Material test & wind tunnel test	Over-load test, inspection & replacement of lines	3	48
		Entanglement			Rotation in canopy & uneven length	3			6	144

7.4 Overall Analysis of Failure Modes

Using the data detailed in Tables 7.4 to 7.7, an overall picture needs to be drawn to visualize a macroscopic view of the failure modes from the view of their severity, occurrence and detection. Besides, it will also be desired to list out the modes that would need the corrective actions. The following sub-section shows these.

7.4.1 Distribution of Failure Modes Based on Severity Rating

The pie chart related to severity of parachute failure modes is presented in the Figure 7.1.

- 1 - No Effect: Qty 0 (0 %)
- 2 - Annoyance: Qty 3 (5.67 %)
- 3 - Annoyance: Qty 1 (1.89 %)
- 4 - Annoyance: Qty 4 (7.55 %)
- 5 - Degradation of Secondary Function: Qty 11 (20.75 %)
- 6 - Loss of Secondary Function: Qty 1 (1.89 %)
- 7 - Degradation of Primary Function: Qty 3 (5.67 %)
- 8 - Loss of Primary Function: Qty 16 (30.19 %)
- 9 - Safety and/or Regulatory Compliance: Qty 8 (15.10 %)
- 10 - Safety and/or Regulatory Compliance: Qty 6 (11.32 %)

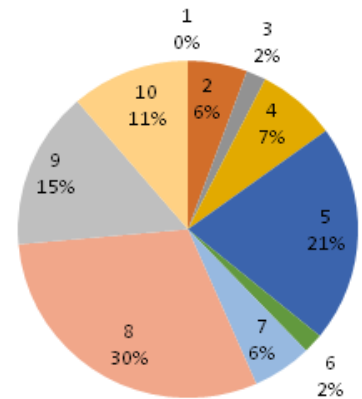


Figure 7.1: Severity effect pie-chart

From Figure 7.1, it can be noticed that most severe failure modes are related to safety compliance and /or regulatory compliance. These put together constitute 26.42% of the total failure modes. These failure modes will not be a big issue by ensuring strict adherence to the system. The other less severe failure modes are 30.19 % in the category of loss of primary function and 20.75 % in the category of degradation of secondary function. These modes require more attention during designing and manufacturing to curb the problem due to severity.

7.4.2 Distribution of Failure Modes Based on Occurrence Rating

From the view point of frequency of occurrence of the failure modes, their level was determined. Based on the level of occurrence, the failure modes were identified and their distribution is shown in Figure 7.2.

- 1 - Very Low: Qty 1 (1.73 %)
- 2 - Low: Qty 43 (74.14 %)
- 3 - Low: Qty 9 (15.52 %)
- 4 - Moderate: Qty 3 (5.17 %)
- 5 - Moderate: Qty 2 (3.44 %)
- 6 - Moderate: Qty 0 (0 %)
- 7 - High: Qty 0 (0 %)
- 8 - High: Qty 0 (0%)
- 9 - High: Qty 0 (0%)
- 10 - Very High: Qty 0 (0%)

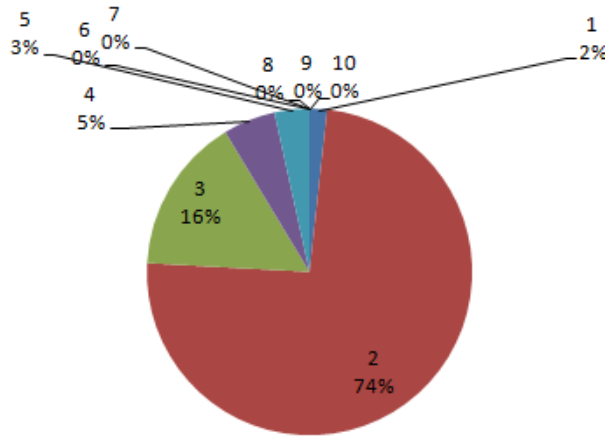


Figure 7.2: Occurrence effect pie-chart

From Figure 7.4, it can be seen that 74.14 % items are in low occurrence of failure probability range and no item is in high-risk side. Thus, the occurrence of risk is not a serious issue.

7.4.3 Distribution of Failure Modes Based on Detection rating

Based on FMEA, the initial detection ranking has been shown in Figure 7.3.

- 1-Detection Not Applicable- Failure Prevention: Qty 0 (0 %)
- 2 - Virtual Analysis - Correlated: Qty 16 (27.59 %)
- 3 - Prior to Design Freeze: Qty 16 (27.59 %)
- 4 - Prior to Design Freeze: Qty 7 (12.07 %)
- 5 - Prior to Design Freeze: Qty 5 (8.62 %)
- 6-Post Design Freeze and Prior to Launch: Qty 12 (20.69 %)
- 7 - Post Design Freeze and Prior to Launch: Qty 0 (0 %)
- 8 - Post Design Freeze and Prior to Launch: Qty 1 (1.72 %)
- 9 - Difficult to Detect: Qty 0 (0 %)
- 10 - Absolute Uncertainty: Qty 01(1.72)

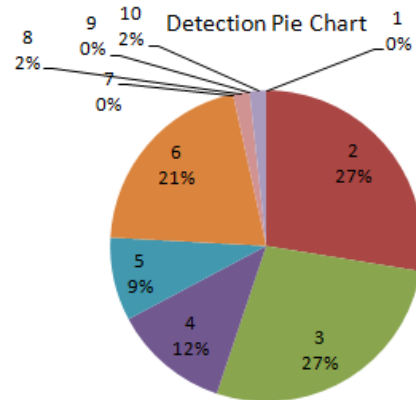


Figure 7.3: Initial detection effect pie-chart

The detection ranking (Figure 5.6) shows that 1.72 % of items are very difficult to detect, 27.59 % items require virtual analysis to find the failure causes and 20.69 % items are required to be checked before the launch. This figure shows that most of the failure model can be averted by being very cautious.

7.4.4 Ranking of Failure Modes with “Corrective Action Required”

Considering the exorbitant cost, time and involved human life, space mission requires practically a very low risk. For this reason, as mentioned in Section 7.2.2, failure modes with $RPN \geq 48$ were considered critical and needed corrective action. Success of mission will depend upon the successful operation of sequence as detailed in Section 7.3.1 to Section 7.3.4. The critical modes identified in these sections have been collated and are shown in Figure 7.4 along with their ranking based on their RPN values.

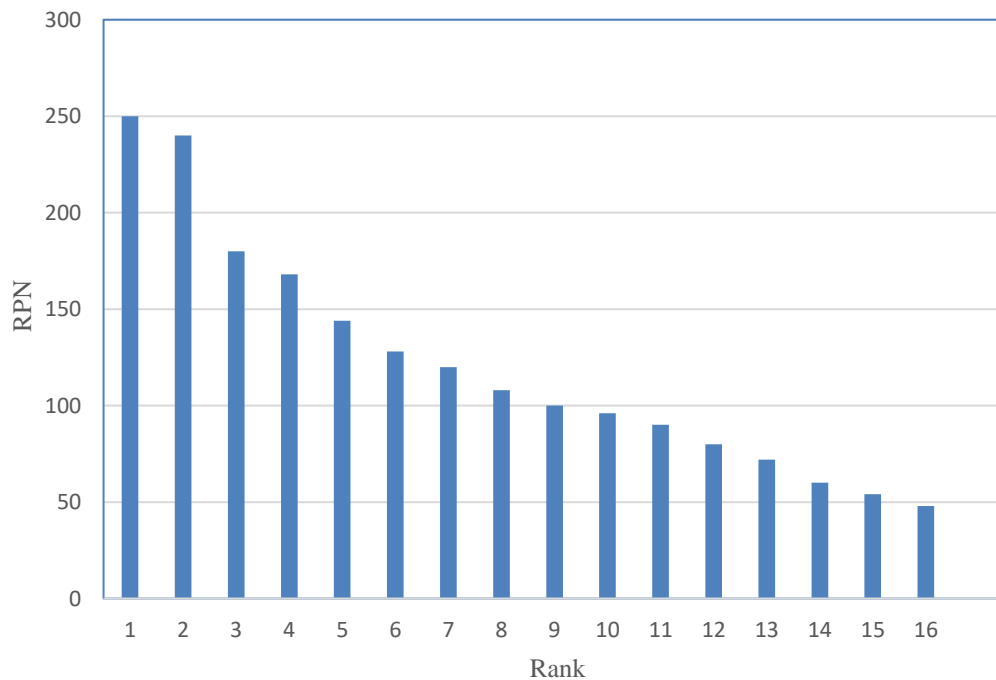


Figure 7.4: Ranking of failure modes

RPN RANKING

- 1: *RPN* = 250 – Entanglement of suspension-lines: rotation in parachute/Unequal line's length (Item: 3-Drogue)
- 2: *RPN* = 240 – Parachute: No deployment- Packing fault/FB wake effect/material defects (Item: 1 - Drogue)
- 3: *RPN* = 180–Parachutes: Entanglement of parachutes – Wrong packing / rotation (Item: 2 -Main)
- 4: *RPN* = 168 – pre-mature breakage-improper knotting/material flaws (Item: 6-Pilot)
- 5: *RPN* = 144 –Suspension-lines breakage -Rotation in canopy/Uneven line's length (Item: 12 Main)
- 6: *RPN* = 128 – pre-mature breakage of reefing lines- Over-stress/material defects (Item: 3 – Main parachute)
- 7: *RPN* = 120– Uneven line's length/Material flaw/over- load (Item: 10 –Main, 3,4-Drogue)
- 8: *RPN* = 108–Material flaw/poor stitching/rubbing with edge of CM (Item: 6– Main; 7,8 Pilot)
- 9: *RPN* = 100 –Material flaw/poor stitching (Item: 2-Drogue)
- 10: *RPN*=96- Material defect/rotation (Item: 7-Drogue; 10- TCS)
- 11: *RPN* = 90-Fabric defective/ improper angle of deployment (item: 9 TCS)
- 12: *RPN* = 80- Tight packing/rotation in parachute (Item: 3-Drogue; 1-Main)
- 13: *RPN* = 72- Under load (Item: 6-Drogue)
- 14: *RPN* = 60-Material defect/over stress (Item: 5-Drogue parachute)
- 15: *RPN* = 54- Unequal length/ improper deployment (item: 7-Main parachute; 5 Pilot chute)
- 16: *RPN* = 48- Over stress (Item: 11- Main parachute Adapter pin (4:1))
- = 48-Material defect, over load (Item: 4-Main parachute; 3-Pilot chute, 7-TCS chute)

7.5 Limitation of FMEA

Although FMEA provides a succinct methodology for examining the failures and facilitates for corrective actions but it has some drawbacks that limits its usage in the present case. Common problems encountered in the failure mode effects analysis include the following.

- (i) The analysis is time consuming and costly.
- (ii) The analysis results and recommendations are often obtained too late in design to be easily incorporated.
- (iii) Accurate failure data are difficult to obtain.

- (iv) The level of detail necessary for a thorough, economical and effective analysis is difficult to define accurately.
- (v) The process of failure analysis is subject to inaccuracies.
- (vi) Agreement of ratings for severity, delectability and occurrence may be problematic within a group environment.

7.6 Fault Tree Analysis

The fault tree is a graphical model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event (Vesely *et al.*, 1998). In contrast with FMEA, it is therefore a “Top-Down” technique, and so it is an EFFECT to CAUSE model. The fault tree develops the logical fault paths from a single undesired event at the top to all of the possible root causes at the bottom (Waghmode and Rajkumar, 2013). The quantification and numerical evaluation generate following three basic measurements for decision-making relative to risk acceptability and required preventive measures (Hixenbaugh, 1968):

- (i) The probability of occurrence of the undesired event,
- (ii) The probability and significance of fault events (cut sets) causing undesired event,
and
- (iii) The risk significance or importance of the components.

Constructing the fault tree will need several common symbols as depicted in Figure 7.5 (Vesely *et al.*, 1998).








	Intermediate Events	An event that happens between two other events
	Basic Events	Failure. It has no input
	Undeveloped Events	Event with not enough information
	External Events	Event that expected to happen
	AND gate	Output happens if both of the branch happens
	OR gate	Output happens if one of the branches happens
	Conditional event	Event used along with an inhibit gate

Figure 7.5: Common symbols used in FTA

The top event is to be defined and all immediate causes are to be identified. Next, secondary level events are specified until all the root causes down to the basic level, are identified.

A decelerator system consists of the parachutes in a lines arrangement. If any event fails in one parachute, it will affect the next system's performance. FTA analysis of each set of parachutes is investigated and is described in the subsequent sub-sections.

7.6.1 TCS/Pilot Chute

The TCS or pilot chutes are the initiating system for operation of deceleration of module. Failure causes must be investigated and proper corrective action should be taken before any event occurs. The investigated fault tree diagram is shown in Figure 7.6.

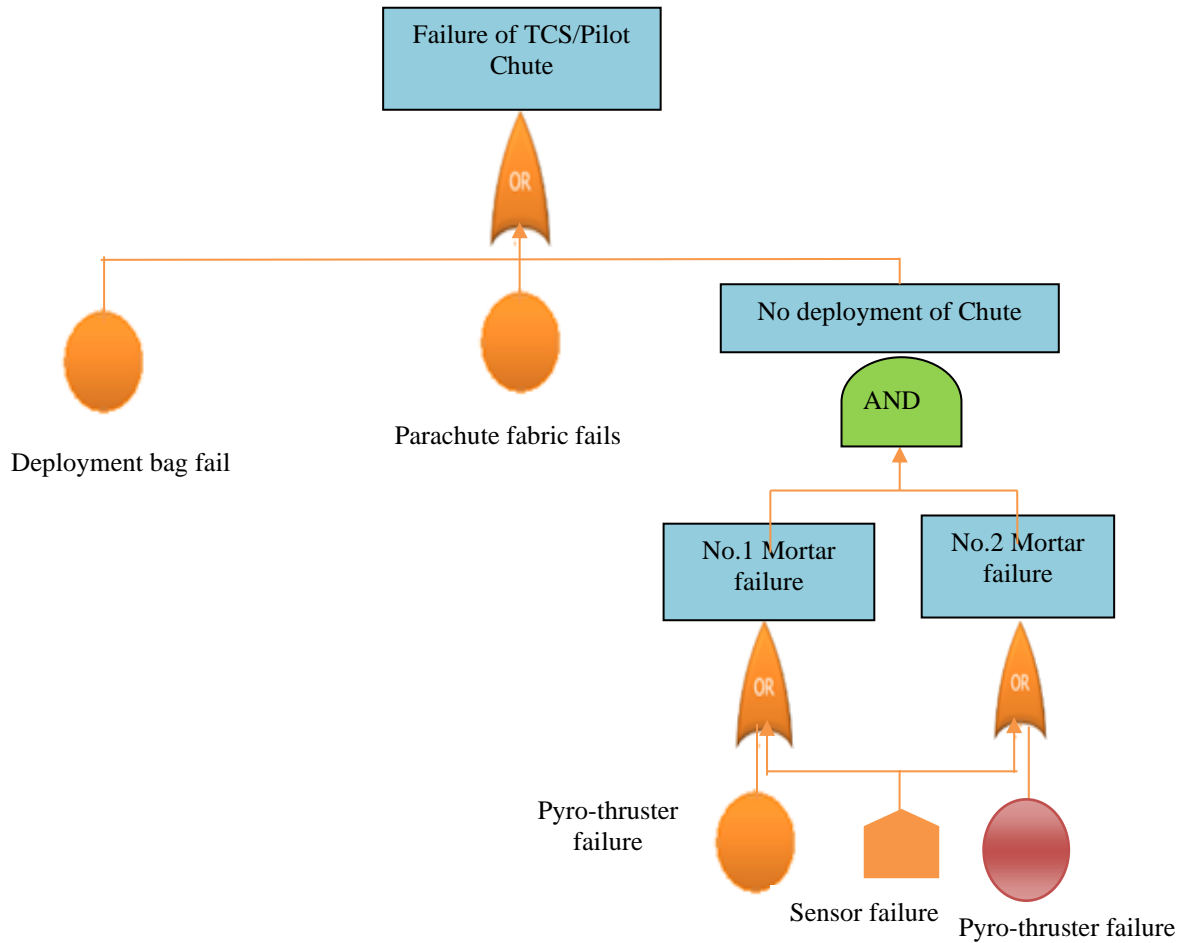


Figure 7.6: FTA of TCS and pilot chutes

7.6.2 FTA of Drogue Parachute

The drogue parachute is the most critical object of the complete deceleration system. Failure of drogue parachute will lead to mission loss. The various possible failure events are as given below.

- (i) Drogue parachute fabric failure
- (ii) Failure of apex weak-ties to break, or premature breakage
- (iii) Inflation and deployment problem with the drogue parachute

FTA of drogue parachute system has been investigated and is shown in Figure 7.7.

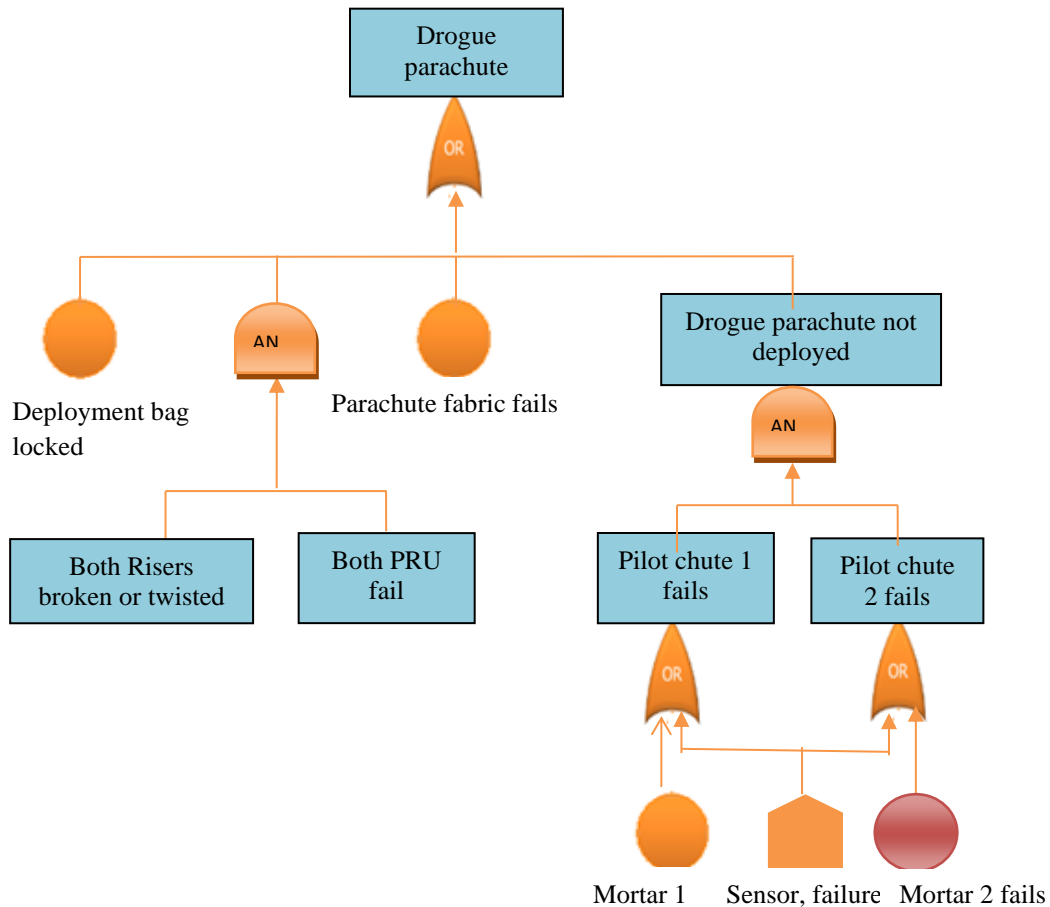


Figure 7.7: FTA of drogue parachute system

7.6.3 Main Parachute

The subsystem and undesired events relate to the main parachute are listed below.

- (i) Main parachute fabric failure
- (ii) Metallic and load bearing component (strap, linkage or adopter) failure
- (iii) Reefing lines-cutter failure resulting in the loss of operation of main parachute
- (iv) Weak-ties or mouth-ties failure leading to non-deployment and thus inflation problem

Investigated FTA diagram for the main parachute is shown in Figure 7.8.

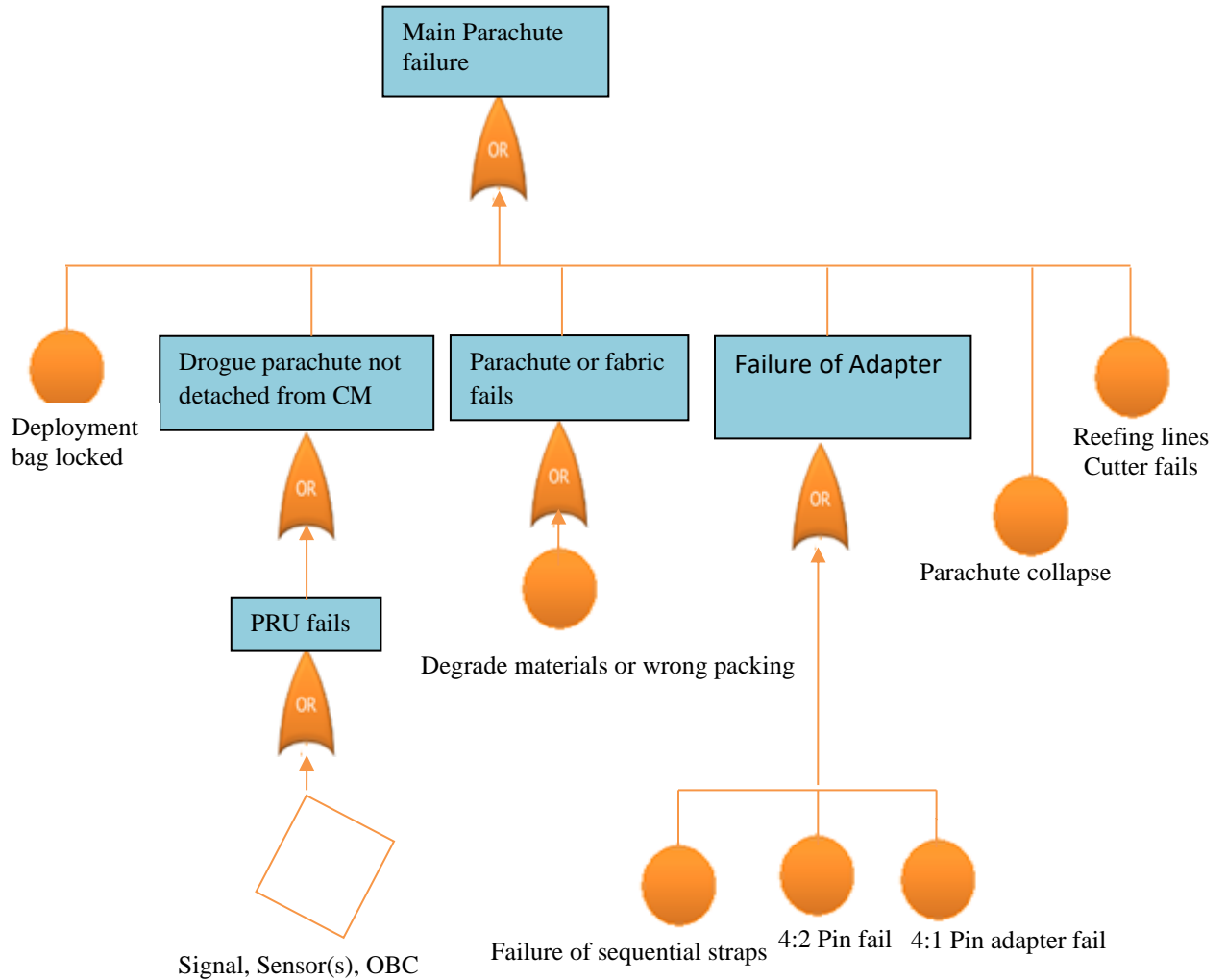


Figure 7.8: FTA of main parachute

7.7 Proposed Integrated FTA-FMEA Model

Traditional FMEA prioritizes the risk of components based on the severity of the class but ignores the functional weightage or importance of the component. Therefore, this proposed model is chosen for identifying critical components, sub-components, system and reliability value of highly complex systems under the present research work.

7.7.1 FTA-FMEA Framework

Parachute system is considered complex, it comprises several interacting components whose series/parallel breakdown is difficult. Some components are deemed critical, relative to others. For this purpose, several advance techniques such as FTA, FMEA, RBD, RCM etc. have been developed. To integrate both FTA and FMEA technique for the purpose of identifying, evaluating and prioritizing the components failure modes, a methodology is proposed based on the minimal cut sets theory and Bimbaum's measure of importance. An integrated FTA-FMEA technique can provide a thorough evaluation of system safety concerns.

In the backward integration framework, as shown in Figure 7.11, the components of a complex system under consideration are de-coupled by means of the FTA technique. The undesired top event is identified based on the reliability requirements of the complex system and the initial itemization of components emanates from the fault trees. Results provide information for adjusting the FMEA criteria subsequently. With root nodes in the fault tree forming the base for system function in the failure mode table, probability, severity and detectability measures are modified based on the set reliability goal.

The top event is defined and all immediate causes are identified. The FT diagram is built and different fault combinations leading to top event are presented.

The FTA-FMEA combined procedure is elaborated through example in the subsequent paragraphs. The steps of the proposed methodology are explained in Figure 7.9.

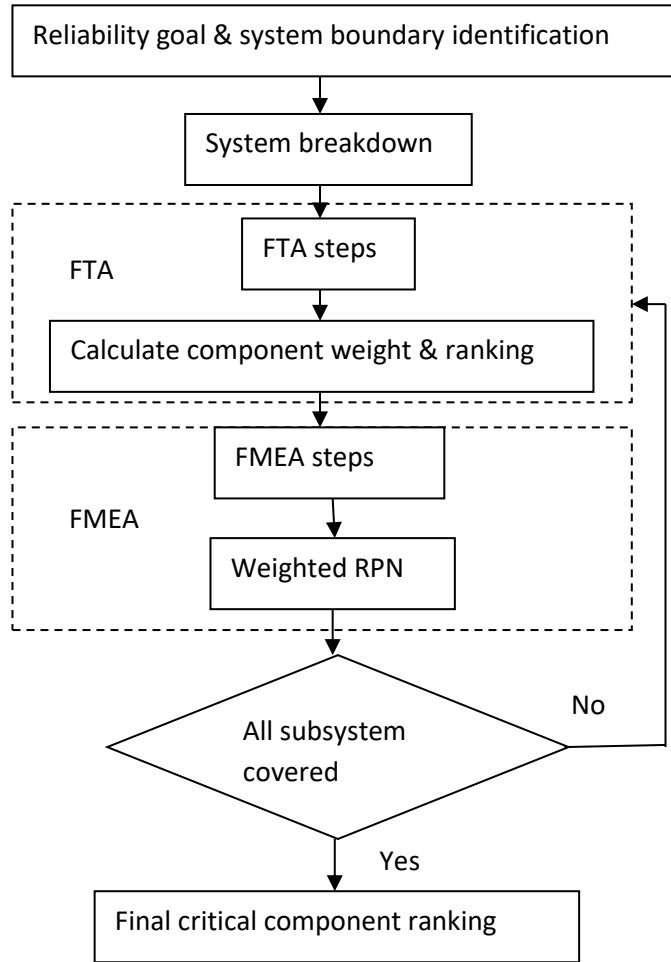


Figure 7.9: FTA-FMEA integrated approach framework

7.7.2 FTA-TMEA Working Steps

In order to tap the maximum benefits from FTA-FMEA integration, minimal cut set theory will be used in this study. A cut set is an event such that when it occurs, the system falls in the indicated failure mode. The FTA methodology is selected for this purpose, as it readily provides and ranks minimal cut sets in terms of importance to system performance. Subsequent breakdown of minimal cut sets allows all components to be analyzed in FMEA worksheets. A minimal set is a set such that the elimination of any element renders it no longer a cut set as shown in Figure 7.10.

If A, B, C, D, E = 0.1 then TE = 0.14

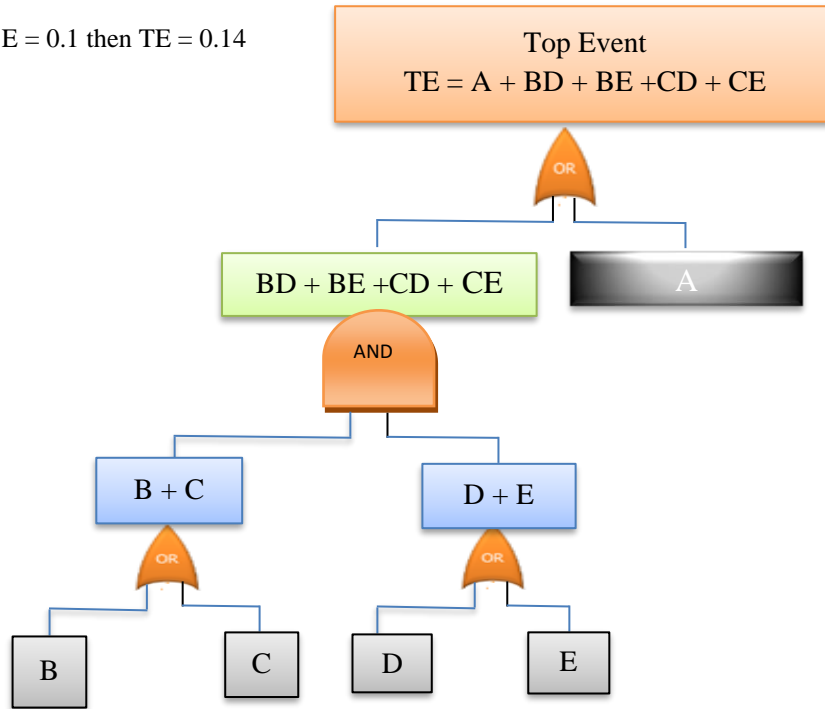


Figure 7.10: Simplified cut set example

After the minimal cut sets are obtained, their importance weights are evaluated. Let w be an independent weight representing the importance of i^{th} minimal cut set in the fault tree structure. The weight w is associated with RPN values obtained from FMEA technique to incorporate the importance of the component in the system. The weighted RPN value is calculated using equation (7.2) given below.

$$wRPN = w \times S \times O \times D \quad 7.2)$$

The criticality of components is then calculated, not based on RPN but on the weighted $wRPN$. Based on the assessment catalogue proposed by Pickard *et al.* (2005), Table 7.8 is reproduced objectively assign value to w based on the number of failed items are one million due to a failure mode.

Table 7.8: Value of w according to number of failures per million

No. of failure per million (n)	w
$n \leq 1$	1
$1 < n \leq 10$	2
$10 < n \leq 100$	3
$100 < n \leq 1000$	4
$1000 < n \leq 5000$	5
$5000 < n \leq 10000$	6
$10,000 < n \leq 50000$	7
$50,000 < n \leq 100000$	8
$100,000 < n \leq 500000$	9
$500,000 < n \leq 1000000$	10

It must be noted that minimal cut sets may include one or more components and each should be assigned relative importance. Aside from typical FMEA steps that are detailed and explained by Shafiee (2014), the additional tasks that should be implemented at this stage include revising traditional RPN values and ranking components based on the weighted RPNs. In the traditional FMEA process, generally the experts brainstorm and report their results. In this case, the minimal cut sets that were obtained from the fault trees aid the failure mode identification process. The weights are multiplied with RPNs obtained from the traditional FMEA procedure. Components with highest RPNs may not necessarily possess highest w RPN in this methodology.

Certain assumptions that are further considered in implementation of FTA-FMEA are as follow:

- (i) Failure modes in FMEA are a direct result of the faults identified in the FTA process and the failure causes are assumed to be mutually independent.

- (ii) In the FMEA method, only the most critical failure modes are considered. Double or multiple failure modes inclusion, as a major improvement to traditional FMEA, would be important only when the assessment's aim is beyond the scope of this work such as risk identification and further quantitative analysis.
- (iii) The complex system under consideration should be coherent and modular, with each module relevant to system functioning and FTA possessing only AND and OR gates.

7.7.3 Integrated FTA-FMEA Approach for Failure Analysis of PDS

Detailed FMEA study is conducted on critical components of parachute system using the severity, occurrence and detectability ratings already reported in Table 7.4 to Table 7.7. The methodology used ten-point scales for severity rating, occurrence rating, and detectability rating to represent the risk priorities of the parachute probable failures. To get the required data for such missions are very costly and time consuming. For this reason, the data from the work of Pickard *et al.* (2005) was taken and accordingly the weights were assigned. The same is shown in Table 5.9 for the six most critical components as listed in Figure 7.6.

Table 7.9: Weights of critical components

Failure Mode	Weight (w)
Rotation in drogue parachute	10
Drogue parachute not deployed	8
Entanglement of parachutes	8
Wrong knotting	2
Suspension-lines breakage	2
Over-stress/Material defects	8

For all the above critical failure modes, RPN values were determined using the data from Tables 7.4 to 7.7. These RPN values obtained from the traditional FMEA technique along with those obtained by the proposed method is shown in Table 7.10.

Table 7.10: RPN from traditional FMEA and weighted RPN from integrated FTA-FMEA model for critical failure models

Failure Modes	Traditional FMEA		FTA-FMEA Approach	
	RPN	Ranking	wRPN	Ranking
Rotation in drogue parachute	250	1	2500	1
Drogue parachute not deployed	240	2	1920	2
Entanglement of parachutes	180	3	1440	3
Wrong knotting	168	4	336	5
Suspension-lines breakage	144	5	288	6
Over-stress/Material defects	128	6	1024	4

Table 7.10 clearly shows that the ranking of the critical failure mode obtained from FMEA are changed for three of the failure modes. The above analysis clearly shows that FTA-FMEA, as compared to FMEA, gives more weightage to frequency of occurrence of failure, ultimately changing its scale from 1 to 10 to 1 to 100.

In addition to the traditional FTA and FMEA, the integrated FTA-FMEA methodology provide a modified, systematic and structured approach for identifying, evaluating and prioritizing the risks associated with different components in a complex system. By using

the proposed technique, it is possible to gain insights about any complex system which otherwise might be overlooked.

7.8 Summary

Space mission is a very capital-intensive program and any failure is likely to cause death of astronauts and loss of crew module. From this perspective, this chapter presents FMEA and FTA of the four parachute that make the parachute deceleration system. The analyses identified possible failure modes and causes of failures. Safety aspects and remedial measures have also been examined. Based on previous work and testing, failure modes with $RPN \geq 48$ (a low value) is considered as the ones with 'corrective action definitely required'. Failure modes with RPN in the range of 25 to 47 are classed as the ones with 'scope for corrective action'.

The results of the study proved the benefits of the combined FTA-FMEA methodology. This combined methodology assessed the internal risks that may occur during the design, manufacturing and strategic operation. FTA-FMEA, as compared to FMEA, gives more weightage to frequency of occurrence of failure, ultimately changing its scale from 1 to 10 to 1 to 100. In comparison to the FTA and FMEA analysis to be carried out in a traditional manner, the integrated FTA-FMEA technique provided a systematic and structured approach for identifying, evaluating and prioritizing the risks associated with various components. By using the proposed technique, it is possible to gain insights about any complex system which otherwise might be overlooked in the traditional FMEA. A minute change in ranking order may have huge implications, particularly for a safety-critical system, such as material defect in over-stressed suspension lines.