Sharif University of Technology
Department of Aeronautics and Astronautics
B.Sc. Project – Reliability Analysis & Risk Assessment (Spring 2025)

Probabilistic Safety Assessment of Aircraft Crew Oxygen Systems

Technical Report

Written by
Hosein Asghari Hosouri
Ali Moradi

Course Instructor
Dr. Khodabakhsh

Submission Date:
9.4.2025

Table of Contents **Page**

Chapter 1: Introduction

The crew oxygen system is one of the most critical life-support subsystems in commercial aircraft. Its primary role is to ensure the availability of breathable oxygen to pilots and crew members in the event of cabin depressurization or other emergency scenarios. The failure of such a system can rapidly escalates into catastrophic consequences, threatening the safety of both crew and passengers.

A notable example of the dangers of inadequate oxygen provision occurred in the **Helios Airways Flight 522 accident (2005)**, where a failure in recognizing and responding to cabin pressure warnings ultimately led to crew incapacitation and the loss of the aircraft. This tragedy highlights the ethical responsibility of aerospace engineers: even seemingly small oversights in design, analysis, or certification can cause irreversible human and financial losses.

The goal of this project is to conduct a **Probabilistic Safety Assessment (PSA)** of a crew oxygen system similar to that installed on the **Boeing 737** platform. The assessment must comply with **FAA Part 25.1309**, which requires that catastrophic failures be "extremely improbable," i.e., less than once in 10^{-9} flight hours. To achieve this, the project integrates system modeling, criticality analysis, and decision-making frameworks to determine whether the system satisfies the regulatory thresholds and to recommend cost-effective improvements.

The project roadmap is structured as follows:

1. **System Modeling & Reliability Prediction** – Using a **Reliability Block Diagram (RBD)** and failure rate data (OREDA, FAA ASRS).
2. **Failure Criticality & Scenario Modeling** – Performing **FMECA** on five critical components and building a **Fault Tree Analysis (FTA)** for the top event of insufficient oxygen delivery.
3. **Risk Mitigation & Decision Analysis** – Evaluating design upgrades using decision tree analysis and sensitivity studies.
4. **Optional Extension** – Application of FORM to a simplified limit state.

This report is organized into eight chapters. Chapter 2 reviews the theoretical foundations of reliability and risk assessment, while Chapters 3–6 present the technical analyses. Chapter 7 discusses the results, and Chapter 8 concludes with recommendations for system improvement and certification.

Chapter 2: Background and Literature Review

2.1 Reliability and Safety in Aerospace Systems

Reliability is the probability that a system or component performs its intended function under stated conditions for a specified duration. In the aerospace domain, reliability analysis is inseparable from safety assessment, since even a low-probability failure can result in catastrophic consequences.

Modern regulations, particularly **FAA AC 25.1309** and **MIL-STD-882E**, establish explicit probabilistic safety objectives. For catastrophic failures, the allowable probability is $\leq 10^{-9}$ per flight hour. These requirements form the backbone of aerospace certification and justify the use of probabilistic tools for system assessment.

2.2 Analytical Methods for Reliability Assessment

Several well-established techniques are used in aerospace reliability engineering and will be applied in this project:

- **Reliability Block Diagram (RBD):** Represents the logical structure of the oxygen supply chain and allows computation of overall system reliability from component-level failure rates.
- **Failure Modes, Effects, and Criticality Analysis (FMECA):** A bottom-up approach that identifies potential failure modes, their effects, and assigns criticality levels using **severity, occurrence, and detection** criteria.
- **Fault Tree Analysis (FTA):** A top-down method that models how combinations of component failures can lead to a top-level undesired event, such as “insufficient oxygen delivery”.
- **Monte Carlo Simulation:** A probabilistic tool used to validate analytical reliability models and quantify uncertainties by generating thousands of random scenarios.
- **Decision Analysis:** A structured approach for selecting cost-effective risk mitigations, using decision trees and sensitivity analysis.

2.3 Data Sources and Standards

This project relies on a combination of **empirical databases** and **regulatory guidelines**:

- **OREDA (Offshore Reliability Data Handbook):** Provides statistical failure rates for valves, generators, and sensors.
- **FAA ASRS (Aviation Safety Reporting System):** Offers incident reports related to oxygen system malfunctions.
- **Regulatory Standards:** FAA AC 25.1309, and MIL-STD-882E establish acceptable risk thresholds and classification schemes.

2.4 Relevance to Crew Oxygen Systems

The crew oxygen system typically consists of **storage & control, distribution & delivery, and User detection & usage**. Failures in any of these elements can compromise oxygen delivery, particularly during decompression events. Due to the system’s critical role in maintaining crew consciousness, probabilistic safety analysis is essential for verifying compliance with certification standards and preventing Helios-like cascades.

Chapter 3: System Modeling & Reliability Prediction

3.1 System description

Based on the conducted research, the new crew oxygen systems in the next-generation Boeing 737 aircraft incorporate high-pressure oxygen gas cylinders instead of chemical generators to enhance reliability. These cylinders are pre-charged and installed beneath the cockpit. The system components have been designed with consideration for various aircraft types, particularly the next-generation Boeing 737.

3.2 Reliability Block Diagram (RBD)

Figure 1 - System RBD

This system can be divided into three subsystems: Storage & Control, Distribution & Delivery, and User Usage & Detection.

Figure 2 - Storage & Control RBD

The Storage & Control subsystem is responsible for storing and maintaining the oxygen supply beneath the pilot's cockpit. Additionally, this subsystem monitors the pressure in the pipes and reservoir, and it reports the oxygen gas reservoir pressure to the flight crew.

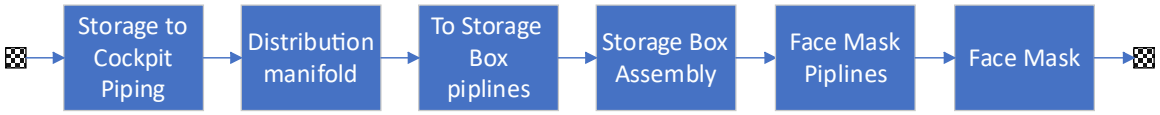


Figure 3 - Distribution & Delivery RBD

The Distribution & Delivery subsystem is responsible for transporting oxygen to the flight crew's masks. This subsystem comprises various valves, hoses, clamps interconnecting the valves, and the pilot's mask itself. Each of these components can be examined in greater detail; however, for the purposes of this project, the current level of analysis is sufficient. In particular, the mask and its associated enclosure could be analyzed in a far more complex manner, which would introduce interdependencies among all components, and a comprehensive analysis of these has not been fully addressed in the available documentation.

Figure 4 - User usage & detection RBD

The final subsystem pertains to User Usage and Detection. In this subsystem, the human factor (i.e., the pilot) exerts a direct influence. This arises from the fact that the accurate identification of gas leakage indicators or reductions in oxygen pressure through sensors, as well as their associated effects, is the responsibility of the flight crew. Moreover, the capability to properly and appropriately utilize the oxygen mask will be incorporated into the analysis, thereby increasing the overall complexity of the evaluation.

3.3 Failure rate assumptions

Component	Failure rate λ (1/hour)	Distribution	Reference
Oxygen Cylinder	0.001 (analog to pressure vessels/coils)	Exponential	MIL-HDBK-217F Sec. 12.2; NASA reports
Pressure Transducer/Gauge	0.0055 (analog to photo-transistors/sensors)	Exponential	MIL-HDBK-217F Sec. 6.11
Manual Isolation Valve	0.0059 (analog to mechanical relays)	Exponential	MIL-HDBK-217F Sec. 13.1
Storage Regulator	0.0022 (analog to thyristors/regulators)	Exponential	MIL-HDBK-217F Sec. 6.10
Supply Lines/Manifold	0.00005 (analog to crimp connections)	Exponential	MIL-HDBK-217F Sec. 17.1
Face Masks	0.10 (analog to fiber optic connectors)	Exponential	MIL-HDBK-217F Sec. 23.1
human errors (using face mask)	0.01	Exponential	
storage box assembly	0.00001	Exponential	
toxic gas sensor	0.000001	Exponential	

According to given Failure rate of the components in the "Failure Rate for RBD.xlsx " we can construct $q_i(t) = P(Basic\ event\ i\ occurs\ at\ time\ t)$

For exponential distribution with respect to $q_i(t) = 1 - e^{-\lambda_i t} \approx \lambda_i t$

For Weibull Distribution with respect to $q_i(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}} \approx -\left(\frac{t}{\eta}\right)^{\beta}$

3.4 Calculation

system reliability over 50,000 flight hours.

Now we can determine minimal cutsets :

1- Storage & Control
2- Distribution & Delivery
3- User Detection & Usage

According to information above and definition below we can say :

$$Q_0(t) = P(\text{The TOP event occurs at time } t)$$

$$q_i(t) = P(\text{Basic event } i \text{ occurs at time } t)$$

$$\check{Q}_j(t) = P(\text{Minimal cut set } j \text{ fails at time } t)$$

We have 3 approaches to calculate $Q_0(t)$:

1- If it is a series of basic events we multiply them $Q_0(t) = \prod q_i(t)$
2- If it is a parallel of basic events $Q_0(t) = 1 - \prod(1 - q_i(t))$
3- Or we can construct minimal cutsets and calculate their failure probability and then claim that $Q_0(t) \leq 1 - \prod\left(1 - \check{Q}_i(t)\right)$

$$inequality\ ariese \begin{cases} basic\ events\ are\ not\ always\ \ independent \\ some\ basic\ events\ contributes\ to\ more\ than\ one\ cutset \end{cases}$$

And $\check{Q}_i(t) = \prod q_{i,j}(t)$

We use 1th approach because we have already construct minimal cutsets

1- $q_1(t)$:Storage & Control
2- $q_2(t)$: Distribution & Delivery
3- $q_3(t)$:User Detection & Usage

$$\left.\begin{array}{c} q_1(t) = \prod_{j=1}^{5} q_{1,j}(t) \\ q_2(t) = \prod_{j=1}^{6} q_{2,j}(t) \\ q_3(t) = \prod_{j=1}^{5} q_{3,j}(t) \\ q_{1,1}(t): probability\ of\ failure\ of\ Oxygen\ Cylinder \\ q_{1,2}(t): probability\ of\ failure\ of\ Pressure\ Transducer/Gauge \\ q_{1,3}(t): probability\ of\ failure\ of\ Manual\ Isolation\ Valve \\ q_{1,4}(t): probability\ of\ failure\ of\ Storage\ Regulator \\ q_{1,5}(t): probability\ of\ failure\ of\ Discharge\ Equipment \\ q_{2,1}(t): probability\ of\ failure\ of\ Storage\ to\ Cockpit\ Piping \\ q_{2,2}(t): probability\ of\ failure\ of\ Distribution\ manifold \\ q_{2,3}(t): probability\ of\ failure\ of\ Distribution\ manifold \\ q_{2,4}(t): probability\ of\ failure\ of\ Storage\ Box\ Assembly \\ q_{2,5}(t): probability\ of\ failure\ of\ face\ mask\ pipeline \\ q_{2,6}(t): probability\ of\ failure\ of\ face\ mask \\ q_{3,1}(t): probability\ of\ failure\ of\ cockpit\ pressure\ gague \\ q_{3,2}(t): probability\ of\ failure\ of\ detecting\ decompression \\ q_{3,3}(t): probability\ of\ failure\ of\ toxic\ gas\ sensor \\ q_{3,4}(t): probability\ of\ failure\ of\ Detecting\ toxic\ gas/smoke \\ q_{3,5}(t): probability\ of\ failure\ of\ using\ face\ mask \\ q_{2,1} = q_{2,2} = q_{2,3} = q_{2,5} = q_{1,5} \\ q_{1,2} = q_{3,1} \\ q_{3,5} = q_{3,4} = q_{3,2} \end{array}\right\} \Rightarrow$$

$$\left.\begin{array}{c} q_1(t) = 0.001\mathrm{t} \times 0.0055\mathrm{t} \times 0.0059\mathrm{t} \times 0.0022\mathrm{t} \times 0.00005\mathrm{t} = \dfrac{7139 * t^5}{2000000000000000000} \\ q_2(t) = 0.00005\mathrm{t} \times 0.00005\mathrm{t} \times 0.00005\mathrm{t} \times 0.00001\mathrm{t} \times 0.00005\mathrm{t} \times 0.1\mathrm{t} = \dfrac{\mathrm{t}^6}{160000000000000000000000} \\ q_3(t) = 0.0055\mathrm{t} \times 0.01\mathrm{t} \times 0.000001\mathrm{t} \times 0.01\mathrm{t} \times 0.01\mathrm{t} = \dfrac{11 * t^5}{2000000000000000} \end{array}\right\}$$

$$\Rightarrow\ Q_0(t) = q_1 \times q_2 \times q_3$$

But the formulas above are valid when t is small but for our problem where t=50000 we can not use the approximation $1 - e^{-\lambda_i t} \approx \lambda_i t$

So we have :

$$\left.\begin{array}{c} q_1(t) = [1 - \exp(-0.001\mathrm{t})] \times [1 - \exp(-0.0055\mathrm{t})] \times [1 - \exp(-0.0059\mathrm{t})] \times [1 - \exp(-0.0022\mathrm{t})] \times \\ [1 - \exp(-0.00005\mathrm{t})] \\ q_2(t) = [1 - \exp(-0.00005\mathrm{t})] \times [1 - \exp(-0.00005\mathrm{t})] \times [1 - \exp(-0.00005\mathrm{t})] \times [1 - \exp(-0.00001\mathrm{t})] \\ \times [1 - \exp(-0.00005\mathrm{t})] \times [1 - \exp(-0.1\mathrm{t})] \\ q_3(t) = [1 - \exp(-0.0055\mathrm{t})] \times [1 - \exp(-0.01\mathrm{t})] \times [1 - \exp(-0.000001\mathrm{t})] \times [1 - \exp(-0.01\mathrm{t})] \\ \times [1 - \exp(-0.01\mathrm{t})] \end{array}\right\}$$

$$\left.\begin{matrix} q_1(50{,}000) = 0.9179 \\ q_2(50{,}000) = 0.2793 \\ q_3(50{,}000) = 0.0488 \end{matrix}\right\}$$

so our top event will occur according to the formula below :

$$\Rightarrow Q_0(t) = q_1 \times q_2 \times q_3 = 0.0125 = 1.25 \times 10^{-2}$$

3.5 Critical question

Does baseline design meet FAA's "extremely improbable" threshold?

As you can see it does not meet FAA extremely improbable threshold which is

$$Q_0(t) = 1 - e^{-\lambda_s t} \approx \lambda_s t = 10^{-9} \times 5e4 = 5 \times 10^{-5}$$

$$1.25 \times 10^{-2} > 5 \times 10^{-5}$$

Chapter 4: Failure Criticality & Scenario Modeling

4.1 FMECA

To account for FMECA, two approaches will be employed: either the more critical components must be identified through a series of sensitivity analyses and importance ranking calculations, or data from previous incidents and prior safety analyses will be utilized. Furthermore, in accordance with the MIL-STD-882 document, severity levels for incidents are selected on a scale from 1 to 4 (with 1 representing the highest severity), and probability of occurrence is denoted using letters from A to F (with A indicating the highest probability of occurrence).

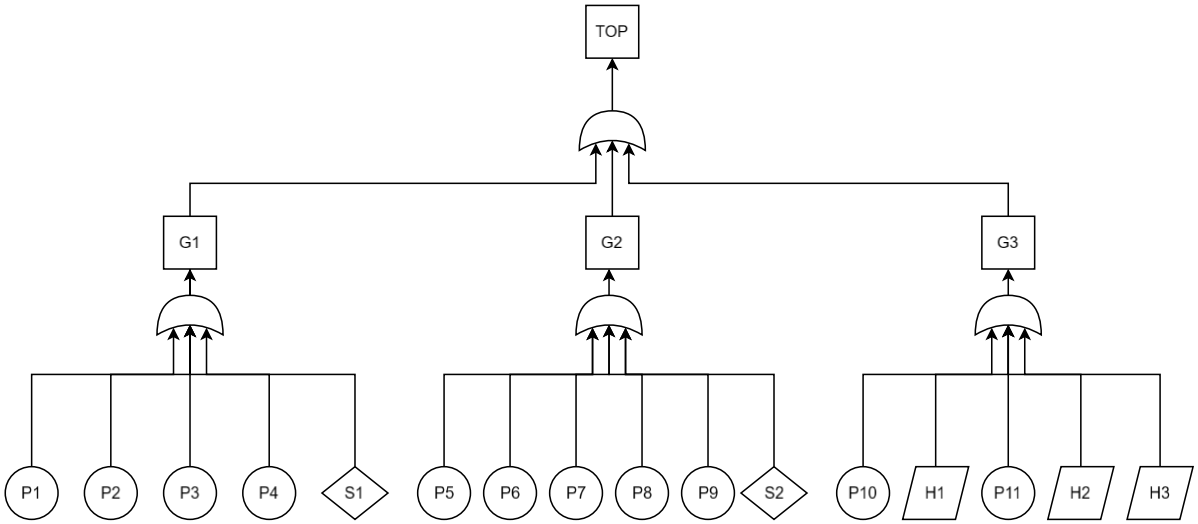
Table 1 - Every component reason for FMECA

COMPONENT	REASON FOR BEING CRITICAL	RELIABLE SOURCE
OXYGEN CYLINDER	The oxygen cylinder stores high-pressure oxygen essential for crew survival during depressurization; failure (e.g., leak or rupture) can cause immediate oxygen loss, hypoxia, or explosion risk due to overpressurization in extreme conditions.	SKYbrary Aviation Safety article on aircraft oxygen systems; B737.org.uk emergency equipment page.
PRESSURE REGULATOR	It controls and reduces oxygen pressure for safe delivery; failures can lead to insufficient flow (causing crew incapacitation) or excessive pressure (damaging masks/system), as seen in FAA-mandated inspections for switch failures that delay warnings.	TechXplore report on US regulator orders for Boeing inspections; Business Insider on Boeing 737 switch issue.
OXYGEN MASKS	Masks provide direct oxygen to crew during emergencies; faults like displacement or blockage prevent effective delivery, potentially leading to rapid hypoxia and loss of aircraft control, prompting FAA airworthiness directives for inspections.	Reuters on FAA orders for 2,600 Boeing 737 inspections; Simple Flying on FAA checks for oxygen mask faults.
PRESSURE TRANSDUCER	This sensor monitors system pressure to detect issues early; failures result in undetected leaks or false readings, delaying crew response and risking oxygen depletion, as highlighted in FAA orders for cabin pressure sensor inspections.	NBC DFW on FAA orders for Boeing 737 cabin pressure sensors; Business Insider on switch failure leading to low oxygen.
TUBING/LINES	These lines distribute oxygen throughout the system; issues like leaks from corrosion or vibration cause pressure loss and contamination, compromising the entire system, as noted in FAA reports on passenger oxygen supply failures.	Reuters on FAA inspections for oxygen mask issues (including supply lines); Aviation Week on FAA order for 737 oxygen system inspections.

Table 2 - FMECA

Component	Failure Mode	Causes	Effects	Severity	Probability	Risk	Mitigation Measures	Post-Mitigation Risk	Detection	Verification
Oxygen Cylinder	Pressure leak or explosion	Corrosion, mechanical damage, overpressure	Oxygen depletion, crew hypoxia, fire risk	1 (Catastrophic)	C (Occasional)	High	Periodic inspections, use of resistant materials, backup system	Medium	5 (Moderate detection with test tools)	Annual pressure testing (e.g., C35001-37)
Pressure Regulator	Improper pressure regulation (high/low)	Mechanical failure, clogging	Insufficient or excessive oxygen, mask damage	2 (Critical)	B (Probable)	High	Redundant design, input filters, automatic monitoring	Low	3 (Easy detection with indicators)	Simulation testing in AMM 35-12
Oxygen Masks	Failure in oxygen delivery (leak or blockage)	Physical damage, wear	Immediate crew hypoxia, loss of aircraft control	1 (Catastrophic)	C (Occasional)	High	Quick-donning masks, pre-flight testing	Medium	4 (Detection via checklist)	FAA inspections for B737 models
Pressure Transducer	Incorrect pressure reading	Electronic failure, miscalibration	Undetected leak, delayed response	2 (Critical)	D (Remote)	Serious	Redundant sensors, automatic alerts	Low	6 (Difficult detection without tools)	Periodic calibration with pressure gauge
Tubing/Lines	Leak or crack	Corrosion, vibration, weak connections	System pressure loss, contamination	2 (Critical)	B (Probable)	High	Stainless steel usage, flareless fittings, visual inspections	Medium	2 (Easy detection with leak tests)	Pressure testing per FAA AD

4.2 Fault Tree Analysis (FTA)



NO.	ID	DESCRIPTION
1	TOP	Insufficient oxygen delivery during decompression
2	G1	Leaks and pressure problems in the tank
3	G2	Leaks in transmission lines
4	G3	Inability of the crew to recognize and use the oxygen system
5	P1	Gas leak or burst oxygen cylinder
6	P2	Gas leak in the pressure gauge or failure to measure pressure
7	P3	Gas not passing through the manual valve
8	P4	Failure to adjust the gas pressure output from the tank
9	P5	Gas not reaching the cockpit
10	P6	Lack of/improper distribution of gas
11	P7	Gas not reaching from the distribution plate to the storage box
12	P8	Leakage in storage box
13	P9	No gas flow in the mask hose
14	P10	Error in cockpit oxygen pressure report
15	P11	Error in cockpit toxic gas/smoke report
16	S1	Failure to relieve excess pressure from the tank and pipes
17	S2	Oxygen mask failure
18	H1	Pilot's failure to understand oxygen pressure drop
19	H2	Pilot's failure to understand toxic gas/smoking
20	H3	Incorrect use of masks

Minimal cut sets:

$$\{P1\},\{P2\},\{P3\},\{P4\},\{P5\},\{P6\},\{P7\},\{P8\},\{P9\},\{P10\},\{P11\},\{S1\},\{S2\},\{H1\},\{H2\},\{H3\}$$

4.3 Monte Carlo Simulation

- Run ~10,000 trials to validate analytical probabilities.
- Compare with deterministic results.
- Are your assumed failure rates defensible given realworld incidents like Alaska Airlines Flight 261

Because all elements are series so we have 16 minimal cutest in size of 1 for our system which are as follows:

$$q_{1,1}(t): probability\ of\ failure\ of\ Oxygen\ Cylinder$$
$$q_{1,2}(t): probability\ of\ failure\ of\ Pressure\ Transducer/Gauge$$
$$q_{1,3}(t): probability\ of\ failure\ of\ Manual\ Isolation\ Valve$$
$$q_{1,4}(t): probability\ of\ failure\ of\ Storage\ Regulator$$
$$q_{1,5}(t): probability\ of\ failure\ of\ Discharge\ Equipment$$
$$q_{2,1}(t): probability\ of\ failure\ of\ Storage\ to\ Cockpit\ Piping$$
$$q_{2,2}(t): probability\ of\ failure\ of\ Distribution\ manifold$$
$$q_{2,3}(t): probability\ of\ failure\ of\ To\ Storage\ Box\ piplines$$
$$q_{2,4}(t): probability\ of\ failure\ of\ Storage\ Box\ Assembly$$
$$q_{2,5}(t): probability\ of\ failure\ of\ face\ mask\ pipeline$$
$$q_{2,6}(t): probability\ of\ failure\ of\ face\ mask$$
$$q_{3,1}(t): probability\ of\ failure\ of\ cockpit\ pressure\ gague$$
$$q_{3,2}(t): probability\ of\ failure\ of\ detecting\ decompression$$
$$q_{3,3}(t): probability\ of\ failure\ of\ toxic\ gas\ sensor$$
$$q_{3,4}(t): probability\ of\ failure\ of\ Detecting\ toxic\ gas/smoke$$
$$q_{3,5}(t): probability\ of\ failure\ of\ using\ face\ mask$$
$$q_{2,1} = q_{2,2} = q_{2,3} = q_{2,5} = q_{1,5}$$
$$q_{1,2} = q_{3,1}$$
$$q_{3,5} = q_{3,4} = q_{3,2}$$

$all\ q_{i,j} = \check{Q}_{i,j}$

Monte Carlo simulation :

It is a bit vague in this situation for this concept because we do not have limit state function for our project yet and limit state function can be reached via physical model of the problem and distribution of each variables that we do not have .

But I struggle to string somethings together to create a limit state function whole system

According to our code in RBD.m and RBD_Id=1

Our $R_s = \prod_{i=1}^{16} R_i(t) = \prod_{i=1}^{16} \exp(-\lambda_i t) = \frac{\prod_{i=1}^{16} exponential(\lambda_i)}{\prod_{i=1}^{16} \lambda_i}$ $and\ we\ then\ say\ if\ it\ become$

$less\ than\ zero\ then\ we\ fail\ so \quad g(t) = \frac{\prod_{i=1}^{16} exponential(\lambda_i)}{\prod_{i=1}^{16} \lambda_i} = \frac{\prod_{i=1}^{16} X_i}{\prod_{i=1}^{16} \lambda_i} \quad where\ \ X_i \sim \exp(x, \lambda_i)$

Due to our denominator is nonzero then our equivalent limit state function will be :

$$g_s(t) = \prod_{i=1}^{16} X_i \quad where\ \ X_i \sim \exp(x, \lambda_i)$$

You can see our answer in detail in “Q_2_MC.docx” but I bring only some details here and its matlab code is available in “Q2.mlx”:

Oxygen System

INITIALIZE UQLAB

Clear all variables from the workspace, set the random number generator for reproducible results, and initialize the UQLab framework:

```
clc; clear all; close all;
rng(100,'twister');
uqlab;
```

COMPUTATIONAL MODEL

```
ModelOpts.mString =
'X(:,1).*X(:,2).*X(:,3).*X(:,4).*X(:,5).*X(:,6).*X(:,7).*X(:,8).*X(:,9).*X(:,
10).*X(:,11).*X(:,12).*X(:,13).*X(:,14).*X(:,15).*X(:,16)';
ModelOpts.isVectorized = true;

myModel = uq_createModel(ModelOpts);
```

PROBABILISTIC INPUT MODEL

The probabilistic input model consists of eight independent lognormal random variables.

Define an INPUT object using the following marginals:

```
InputOpts.Marginals(1).Name = 'X1';  %failure of Oxygen Cylinder
InputOpts.Marginals(1).Type = 'Exponential';
InputOpts.Marginals(1).Moments = 1/0.001.*ones(1,2);

InputOpts.Marginals(2).Name = 'X2';  %failure of Pressure Transducer/Gauge
InputOpts.Marginals(2).Type = 'Exponential';
InputOpts.Marginals(2).Moments = 1/0.0055.*ones(1,2);

InputOpts.Marginals(3).Name = 'X3';  %failure of Manual Isolation Valve
InputOpts.Marginals(3).Type = 'Exponential';
InputOpts.Marginals(3).Moments = 1/0.0059.*ones(1,2);

InputOpts.Marginals(4).Name = 'X4';  %  failure of Storage Regulator
InputOpts.Marginals(4).Type = 'Exponential';
```

```
 InputOpts.Marginals(4).Moments = 1/0.0022.*ones(1,2);

 InputOpts.Marginals(5).Name = 'X5';  % failure of Discharge Equipment
 InputOpts.Marginals(5).Type = 'Exponential';
 InputOpts.Marginals(5).Moments = 1/0.00005.*ones(1,2);

 InputOpts.Marginals(6).Name = 'X6';  % failure of Storage to Cockpit Piping
 InputOpts.Marginals(6).Type = 'Exponential';
 InputOpts.Marginals(6).Moments = 1/0.00005.*ones(1,2);

 InputOpts.Marginals(7).Name = 'X7';  % failure of Distribution manifold
 InputOpts.Marginals(7).Type = 'Exponential';
 InputOpts.Marginals(7).Moments = 1/0.00005.*ones(1,2);

 InputOpts.Marginals(8).Name = 'X8';  % failure of Distribution manifold
 InputOpts.Marginals(8).Type = 'Exponential';
 InputOpts.Marginals(8).Moments = 1/0.00005.*ones(1,2);

 InputOpts.Marginals(9).Name = 'X9';  % failure of Storage Box Assembly
 InputOpts.Marginals(9).Type = 'Exponential';
 InputOpts.Marginals(9).Moments = 1/0.00001.*ones(1,2);

 InputOpts.Marginals(10).Name = 'X10';  % failure of face mask pipeline
 InputOpts.Marginals(10).Type = 'Exponential';
 InputOpts.Marginals(10).Moments = 1/0.00005.*ones(1,2);

 InputOpts.Marginals(11).Name = 'X11';  % failure of face mask
 InputOpts.Marginals(11).Type = 'Exponential';
 InputOpts.Marginals(11).Moments = 10.*ones(1,2);

 InputOpts.Marginals(12).Name = 'X12';  % failure of cockpit pressure gague
 InputOpts.Marginals(12).Type = 'Exponential';
 InputOpts.Marginals(12).Moments = 1/0.0055.*ones(1,2);

 InputOpts.Marginals(13).Name = 'X13';  % failure of detecting decompression
 InputOpts.Marginals(13).Type = 'Exponential';
 InputOpts.Marginals(13).Moments = 100.*ones(1,2);

 InputOpts.Marginals(14).Name = 'X14';  %p failure of toxic gas sensor
 InputOpts.Marginals(14).Type = 'Exponential';
 InputOpts.Marginals(14).Moments = 1/0.000001.*ones(1,2);

 InputOpts.Marginals(15).Name = 'X15';  % failure of Detecting toxic
gas/smoke
 InputOpts.Marginals(15).Type = 'Exponential';
 InputOpts.Marginals(15).Moments = 100.*ones(1,2);

 InputOpts.Marginals(16).Name = 'X16';  % failure of using face mask
```

```
InputOpts.Marginals(16).Type = 'Exponential';
InputOpts.Marginals(16).Moments = 100.*ones(1,2);
```

Create an INPUT object based on the defined marginals:

```
myInput = uq_createInput(InputOpts);
```

RELIABILITY ANALYSIS

Failure event is defined as $g(\mathbf{x}) \leq 0$. The failure probability is then defined as $P_f = P[g(\mathbf{x}) \leq 0]$.

Monte Carlo simulation (MCS)

Select the Reliability module and the Monte Carlo simulation (MCS) method:

```
MCSOpts.Type = 'Reliability';
MCSOpts.Method = 'MCS';
```

Specify the sample size and the target coefficient of variation (CoV):

```
MCSOpts.Simulation.BatchSize = 5e3;
MCSOpts.Simulation.MaxSampleSize = 1e4;
MCSOpts.Simulation.TargetCoV = 5e-2;
```

Run the Monte Carlo simulation:

```
MCSAnalysis = uq_createAnalysis(MCSOpts);
```

Print out a report of the results:

```
uq_print(MCSAnalysis)
```

```
--------------------------------------------------

Monte Carlo simulation

--------------------------------------------------

Pf               0000

Beta             Inf

CoV              NaN

ModelEvaluations 10000

PfCI             [0.0000e+00 0.0000e+00]

BetaCI           [Inf        Inf       ]

--------------------------------------------------
```

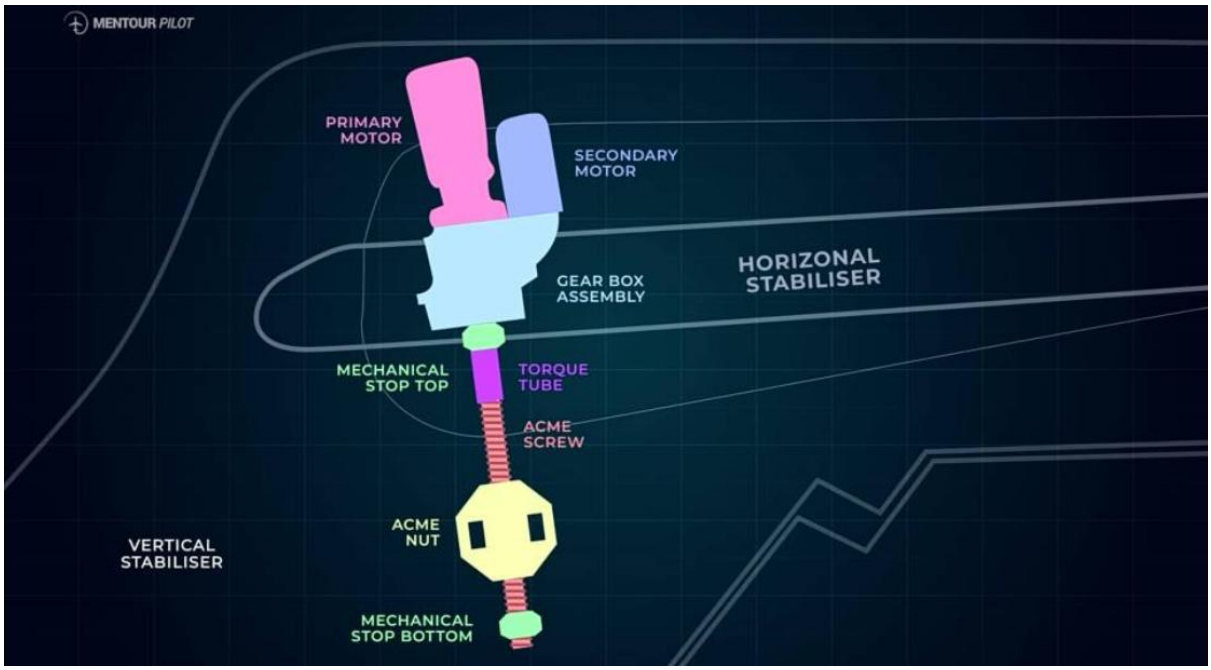
Create a graphical representation of the results:

```
uq_display(MCSAnalysis)
```

so it does not evaluates it as 1.25e-2

Are your assumed failure rates defensible given realworld incidents like Alaska Airlines Flight 261?

This airplane incidence is fully scrutinized in file “Alaska Airlines Flight 261.docx” and I pay to this in brief here .
this airplane had problem in autopilot system in horizontal stabilizer and more accurate in its maintenance of greasing the actuator of its jackscrew system . and after this incidence 24 certification obliged to airline companies for this problem and lubrication scheduled was immediately changed to be completed every 650 hours but it does not have nothing to do with our project because the main cause of failure of our aircraft was oxygen system to horizontal stabilizer but as we mentioned we can prevent this happening by decreasing test interval for this system.



Chapter 5: Risk Mitigation & Decision Analysis

- **Proposed design upgrades:**
  - Example: add redundant sensors.
  - Example: shorten inspection intervals.
- **Cost estimation:** installation, maintenance, penalties avoided.
- **Decision tree:** calculate utility function
- **Sensitivity analysis:** vary cost parameters; test robustness of decision.
- **Discussion:** which option provides best cost–safety trade-off?

First upgrade (consider redundancy) :

According to sensitivity analysis and criticality analysis both conclude same result as follows:

By running “Pr_1_2.m” we have :

{[11]}

{[13 16 15]}

{[3]}

{[2]}

{[4]}

{[12 1 5]}

{[6 10 7 8]}

{[9]}

{[14]}

And their sensitivity values are as follows :

11	3.2512501208286002134303734722992 e-1017
13	1.537736123719366231266713670798 9 e-2971
16	1.537736123719366231266713670798 9 e-2971
15	1.537736123719366231266713670798 9 e-2971
3	1.433880724270560737059148485478 4 e-3060
2	2.955448448975089187158780097895 9 e-3069

4	6.486850282199618084686030654862 8e-3141
12	5.680217431208191594512646469858 e-3167
1	5.680217431208191594512646469858 e-3167
5	5.680217431208191594512646469858 e-3167
6	1.334679745448039926149366005737 5e-3187
10	1.334679745448039926149366005737 5e-3187
7	1.334679745448039926149366005737 5e-3187
8	1.334679745448039926149366005737 5e-3187
9	1.806292613803806125875822946392 6e-3188
14	1.151743020627782483670686742637 2e-3188

Which are sorted in descending order so the most critical element is 11th which is equivalent to $q_{2,6}(t)$: $probability\ of\ failure\ of\ face\ mask$

And after that 13,15,16

$q_{3,2} = q_{3,4} = q_{3,5}$

So if we consider a parallel element for each of elements below :

{[11]}

{[13 16 15]}

We can increase our reliability so we do that and according to the slide below

Example: Consider a parallel structure of two independent components with constant failure rates λ_1 and λ_2, respectively. The reliability or the survivor function of the system is:

$$R_S(t) = \exp(-\lambda_1 t) + \exp(-\lambda_2 t) - \exp(-(\lambda_1 + \lambda_2)t)$$

The Mean Time To Failure (MTTF) is

$$\text{MTTF} = \int_0^\infty R_S(\tau)d\tau = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

The system failure rate function $z_S(t)$ is:

$$z_S(t) = -\frac{\dot{R}_S(t)}{R_S(t)} = \frac{\lambda_1 \cdot \exp(-\lambda_1 t) + \lambda_2 \cdot \exp(-\lambda_2 t) - (\lambda_1 + \lambda_2) \cdot \exp(-(\lambda_1 + \lambda_2)t)}{\exp(-\lambda_1 t) + \exp(-\lambda_2 t) - \exp(-(\lambda_1 + \lambda_2)t)}$$

Even when the components have exactly the same failure rates, i.e., $\lambda_1 = \lambda_2 = \lambda$

$$z_S(t) = \frac{2\lambda \cdot (\exp(-\lambda t) - \exp(-2\lambda t))}{2\exp(-\lambda t) - \exp(-2\lambda t)} = \frac{2\lambda \cdot (1 - \exp(-\lambda t))}{2 - \exp(-\lambda t)} \Rightarrow \lim_{t\to\infty}(z_S(t)) = \lambda$$

Supposing that we use identical element for all of those mentioned above then $\lambda_1 = \lambda_2$

So we implemented that as follows in RBD.m in RBD_Id==2

But as you can see the reliability and failure rate did not change and it is obvious because as t approaches infinity it again have same failure rate with single element. It was hot redundancy called active redundancy and it does not meet our needs so it is obvious that if we use another type of redundancy called passive redundancy such as warm or cold it will get worse not better so merely add redundancy to our systems has just cost and to considerable risk reduction

Second upgrade (consider test interval) :

If the test interval were τ_i $\Rightarrow$ $q_i(t) = \frac{\lambda_i \times \tau_i}{2}$ $or\ equivalently\ q_i(t) = 1 - e^{-\frac{\lambda_i \times \tau_i}{2}}$

We implement this technique for those all elements with $\tau_i = 500\ hours$:

Then failure probability will become

0.000000030326331456987187243107630833772 e-9 << 5 e-5

And it passes our constraint of FAA extremely improbable threshold

And we set $\tau_i = 5000\ hours$ for less cost of maintenance

Then failure probability will become (in RBD.m as RBD_Id==3)

9.052018230551364659004314010364 6 e-9 << 5 e-5 = 5e4 * 1 e-9

And It also passes our constraint of FAA extremely improbable threshold.

But it is obvious that it is not appliable for all elements for example how can we test our crew !!!

So we do it for elements below in RBD.m as RBD_Id==4 :

$$q_{1,1}(t): probability\ of\ failure\ of\ Oxygen\ Cylinder$$
$$q_{1,2}(t): probability\ of\ failure\ of\ Pressure\ Transducer/Gauge$$
$$q_{1,3}(t): probability\ of\ failure\ of\ Manual\ Isolation\ Valve$$
$$q_{1,4}(t): probability\ of\ failure\ of\ Storage\ Regulator$$
$$q_{1,5}(t): probability\ of\ failure\ of\ Discharge\ Equipment$$
$$q_{2,1}(t): probability\ of\ failure\ of\ Storage\ to\ Cockpit\ Piping$$
$$q_{2,2}(t): probability\ of\ failure\ of\ Distribution\ manifold$$
$$q_{2,3}(t): probability\ of\ failure\ of\ To\ Storage\ Box\ piplines$$
$$q_{2,4}(t): probability\ of\ failure\ of\ Storage\ Box\ Assembly$$
$$q_{2,5}(t): probability\ of\ failure\ of\ face\ mask\ pipeline$$
$$q_{2,6}(t): probability\ of\ failure\ of\ face\ mask$$
$$q_{3,1}(t): probability\ of\ failure\ of\ cockpit\ pressure\ gague$$
$$q_{3,3}(t): probability\ of\ failure\ of\ toxic\ gas\ sensor$$

Then failure probability will become

9.052018230928506422166374340087 5 e-9 << 5 e-5 = 5e4 * 1 e-9

And It also passes our constraint of FAA extremely improbable threshold.

So it is our second upgrade.

Constructing Decision tree :

According to our codes we can define multiple RBD in RBD.m according to our decision tree.

We combine two upgrades for each element and due to we have 16 elements it will get so enormous decision tree so for just conveying that we have understood we consider that we focus only on inspection intervals for (as whole part)

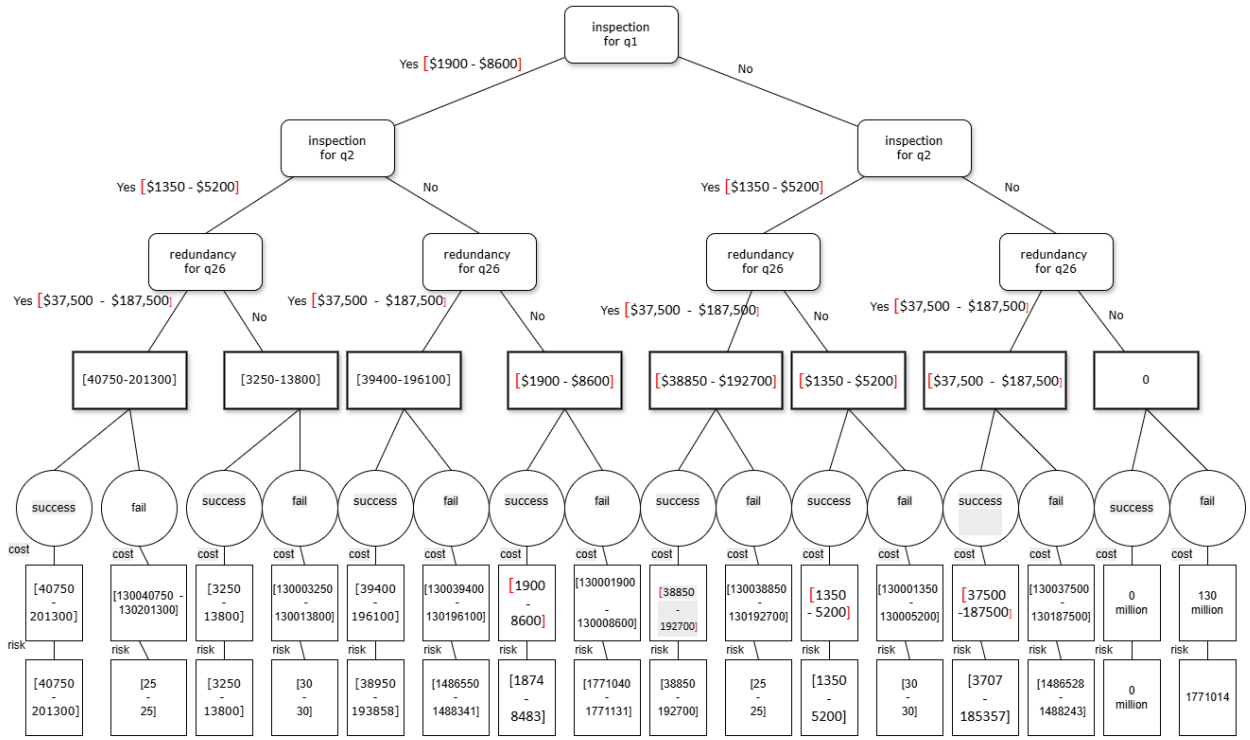
1- $q_1(t)$:Storage & Control according to inspection cost.docx [$1900 - $8600]
2- $q_2(t)$: Distribution & Delivery according for inspection cost.docx [$1350 - $5200]

And not $q_3(t)$:User Detection & Usage

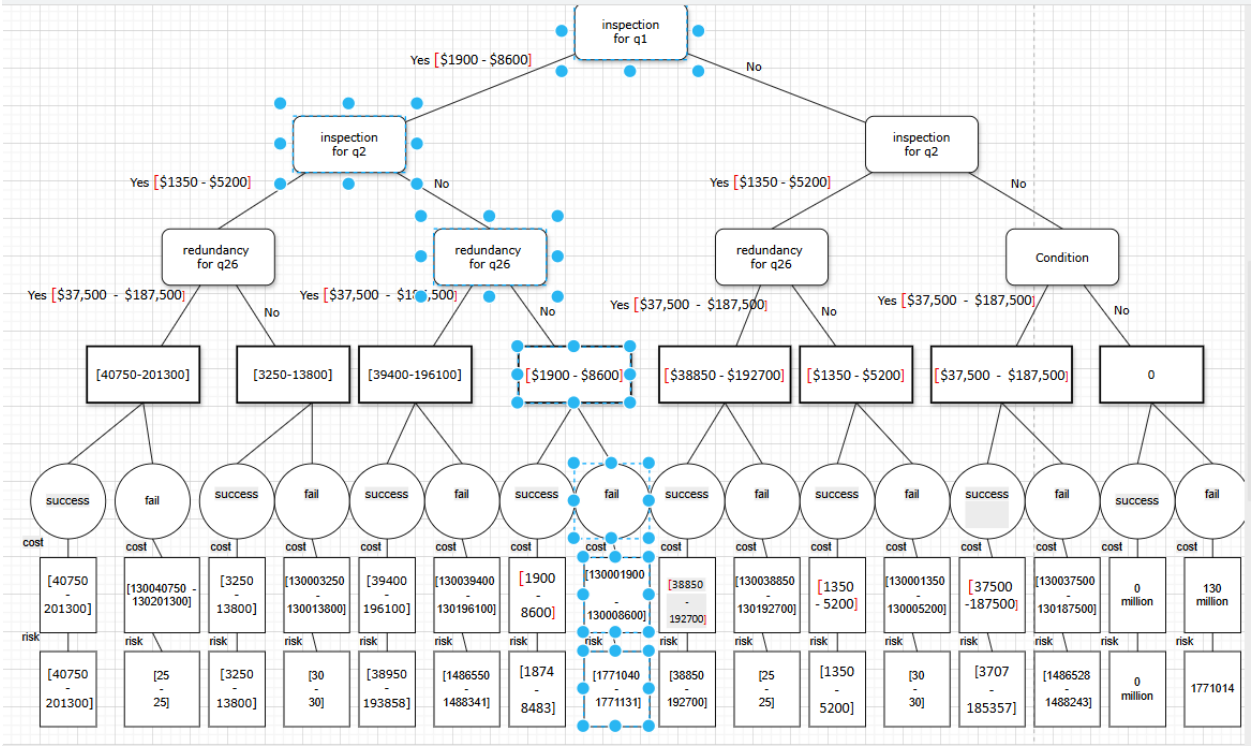
And redundancy only for the most critical element is 11th which is equivalent to $q_{2,6}(t): probability\ of\ failure\ of\ face\ mask$ according to face mask redundancy.docx [**$37,500 (if only the purchase of additional masks) - $187,500**]

And if boing 737 fails then the cost itself is **$130 million=$130,000,000 .**

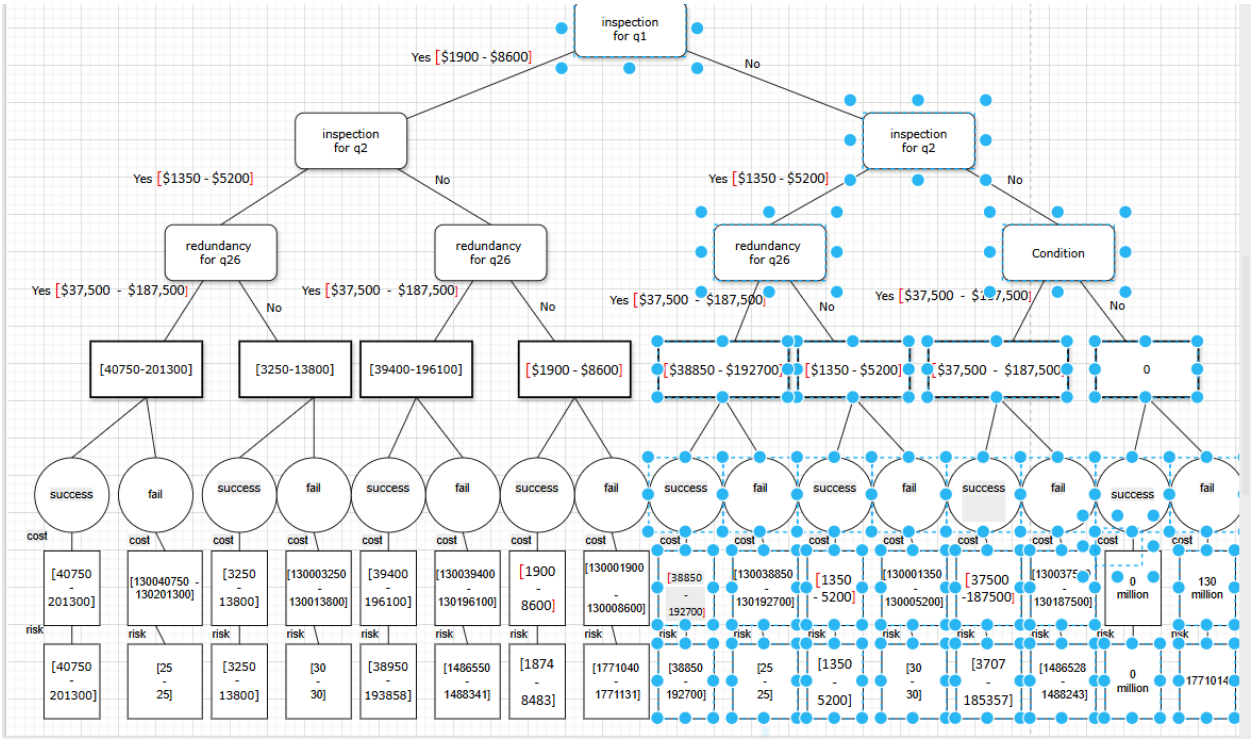
So we decision tree (and we have this picture in folder decision tree) as follows :



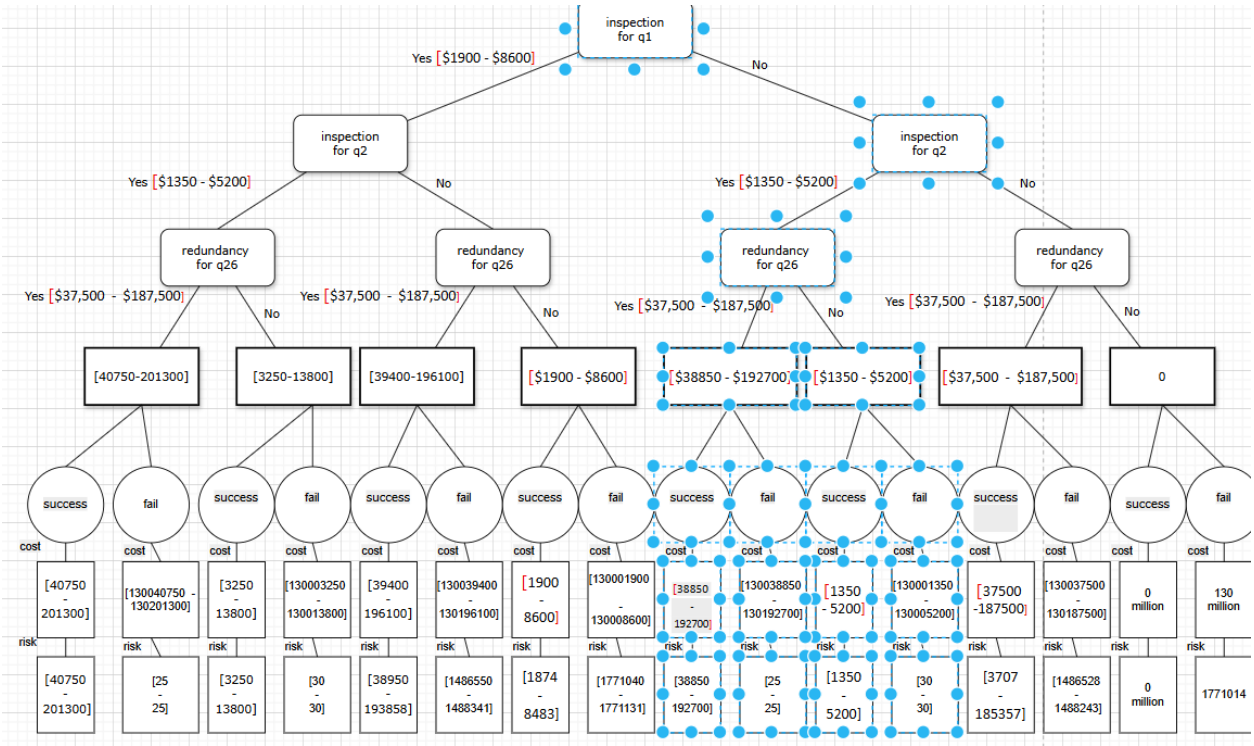
As you can see the branch below has the highest risk (by running pr_3.m):



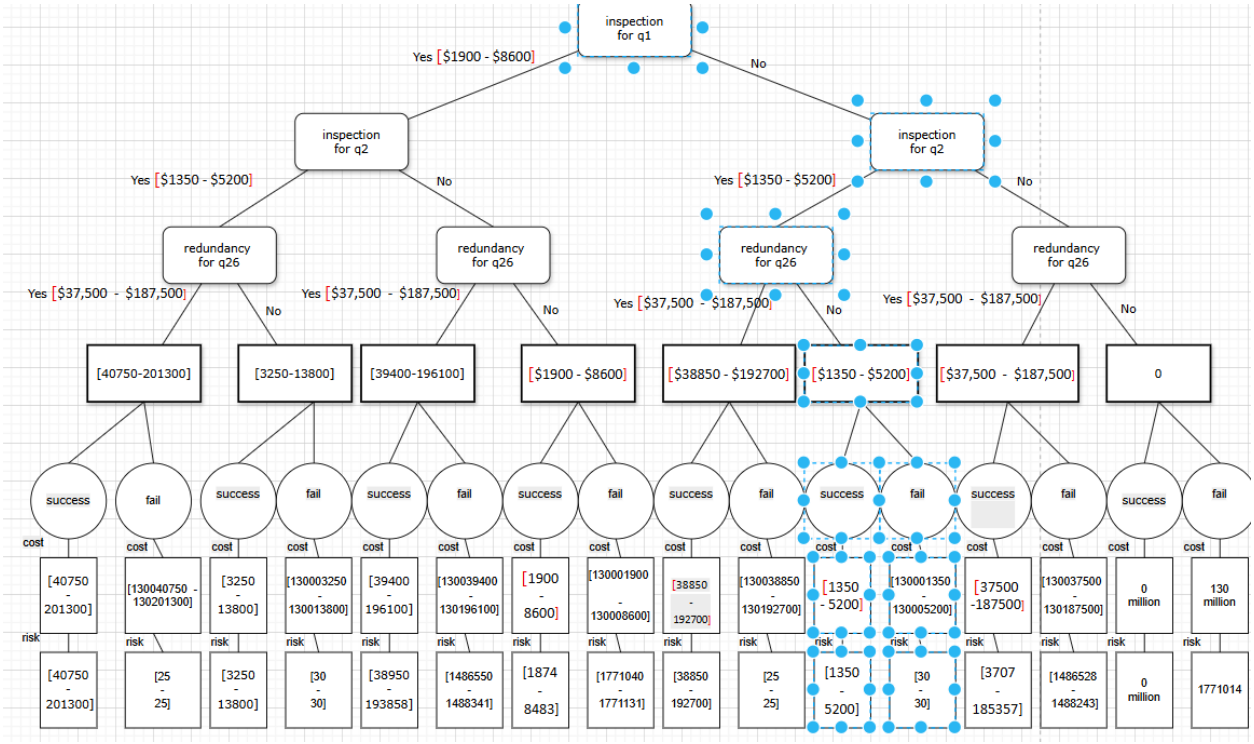
Then by running pr_3.m we conclude the picture below where right hand side is safer:



Then by running pr_3.m we conclude the picture below where left hand side is safer:



Then by running pr_3.m we conclude the picture below where right hand side is safer:



So if we define utility function as $Utility = Risk = p_f \times cost$

Then it is more **economical** only choose $q_2(t)$: Distribution & Delivery according for inspection.

But in the question free we are going to set $Utility = \frac{Risk\ Reduction \times 10^6}{(Cost + \$50K)}$

Where Risk reduction is calculated according to RPN=severity*occurrence *detection and with those facilities mentioned as upgrades we are only able to reduce occurrence so for comparison in practical view we can reduce our utility function as follows:

$$Utility = \frac{\text{occurrence } Reduction}{(Cost\ +\ \$50K)} = \frac{\mathrm{p_f}(initial) - p_f(new)}{(Cost\ +\ \$50K)}$$

Then by running pr_3.m we and maximizing utility we conclude that:

we should have q_2 (t): Distribution & Delivery has inspection

as you can see the same result achieved but we can not say exactly this utility function is risk neutral rather due to 50K$ in denominator it means that somehow we want an risk seeking attitude

Would your solution prevent a Helios-like cascade?

If we calculate p_f for $q_2(t)$: Distribution & Delivery according for inspection

Which is equivalent to RBD_Id==6 in RBD.m then by running pr_1_2.m for RBD_Id==6 :

$$p_f = 0.011431532345604757045890711174997 > 5e-5$$

And it does not meet FAA extremely improbable threshold

But if we decrease test interval from 5000 hours to 500 hours :

$$p_f = 0.000162491467472803537111638178831 27 > 5e - 5$$

And it does not meet FAA extremely improbable threshold

But if we decrease test interval from 500 hours to 240 hours :

$$p_f = 0.990812064629431384317325317612 87 > 5e - 5$$

And it meets FAA extremely improbable threshold so we choose test interval=240 hours

Chapter 6: FORM Analysis

Define a simple **limit state function**

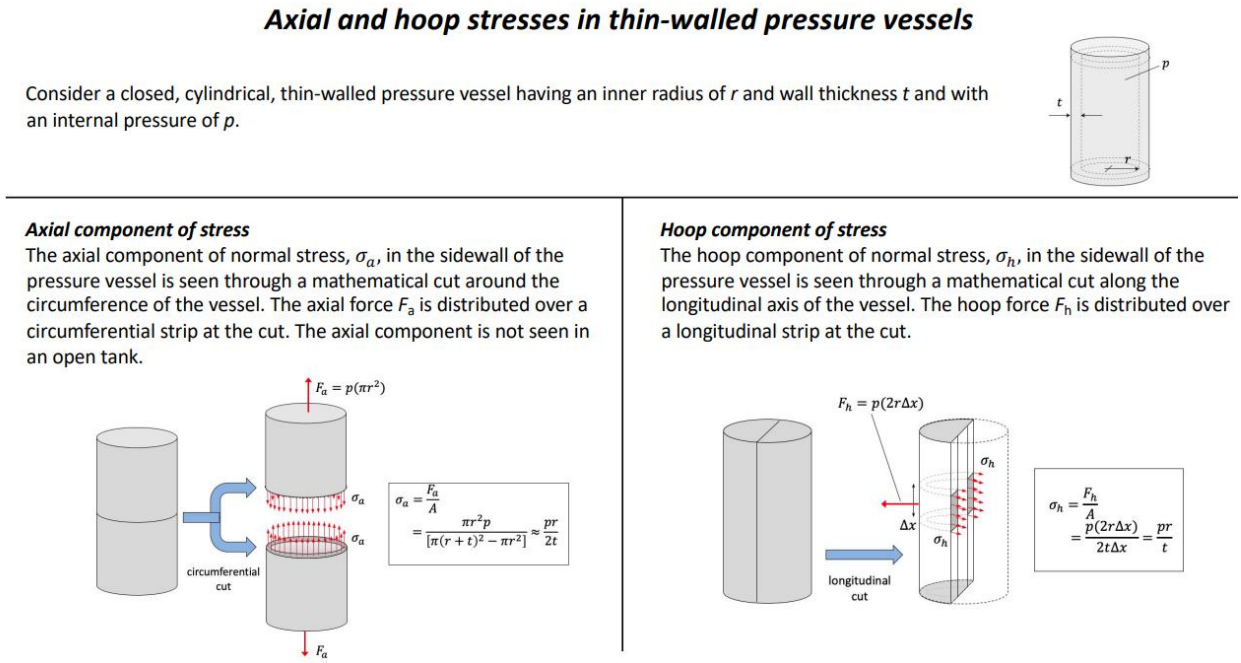
Assume one uncertain variable (e.g., sensor drift).

Apply FORM approximation.

Show how probability of failure compares to Monte Carlo.

As far as I perceived from intention of question I just need to investigate one and only one component and then apply form to this component .

So I choose Oxygen Cylinder and I consider it as a thin-walled pressure vessels. therefor in this case we have two types of tension which are knows as axial and radial(hoop) tension which are as follows :



Because this component is inside the airplane so if it enters plastic region of buckles is not that much important and we can neglect deformation so we consider ultimate strength instead of yield strength ('Ultimate strength', 'ultimate tensile strength' and 'tensile strength' mean the same thing)

According to “Aircraft Oxygen Cylinders.docx” in references folder we choose 6061-T6 Aluminum

(UTS = 310 MPa)

Operating Pressure (P): 30 MPa (Approx 2900 PSI) we consider it as $P \sim N(\mu = 30\ ,\ S = 2)$

Assume a Safety Factor (SF) = 2 (This is for illustration only. A higher SF is recommended for aircraft)
Allowable Stress: $\sigma_{allowable} = 310\ MPa\ /\ 2 = 155\ MPa$

Dimensions:

Radius = 0.1 m (10 cm)

Length = 0.637 m (63.7 cm)

Thickness = 0.02 m (2 cm)

With respect formula hoop stress is twice larger than axial stress so hoop stress is more dangerous and we consider it for reliability analysis :

$$\sigma_h = \frac{Pr}{t} = 5P$$

So the limit state function is $g(P) = 5P - 155$;

You can see our answer in detail in “Q_4_oxygen_vessel.docx” but I bring only some details here and its matlab code is available in “Q4.mlx”:

Oxygen Cylinder

INITIALIZE UQLAB

```
clc; clear all; close all;
uqlab;
```

COMPUTATIONAL MODEL

The **P** function is defined as:

$$g(\mathbf{P}) = 5P - 155$$

Create a limit state function model using a string, written below in a vectorized operation:

```
ModelOpts.mString = 'X(:,1) -155'; % mSting stands for model string, g(x) =
R - S
ModelOpts.isVectorized = true;

myModel = uq_createModel(ModelOpts);
```

PROBABILISTIC INPUT MODEL

The probabilistic input model consists of two independent Gaussian random variables:

$$p \sim \mathcal{N}(30, 2)$$

Specify the probabilistic input model for the p:

```
InputOpts.Marginals(1).Name = 'P';  % resistance variable
```

```
InputOpts.Marginals(1).Type = 'Gaussian';
InputOpts.Marginals(1).Moments = [30 2]; % mean and std dev
```

Create an INPUT object based on the specified marginals:

```
myInput = uq_createInput(InputOpts);
```

FORM

Select FORM as the reliability analysis method:

```
FORMOpts.Type = 'Reliability';
FORMOpts.Method = 'FORM';
```

Run the FORM analysis:

```
FORMAnalysis = uq_createAnalysis(FORMOpts);
```

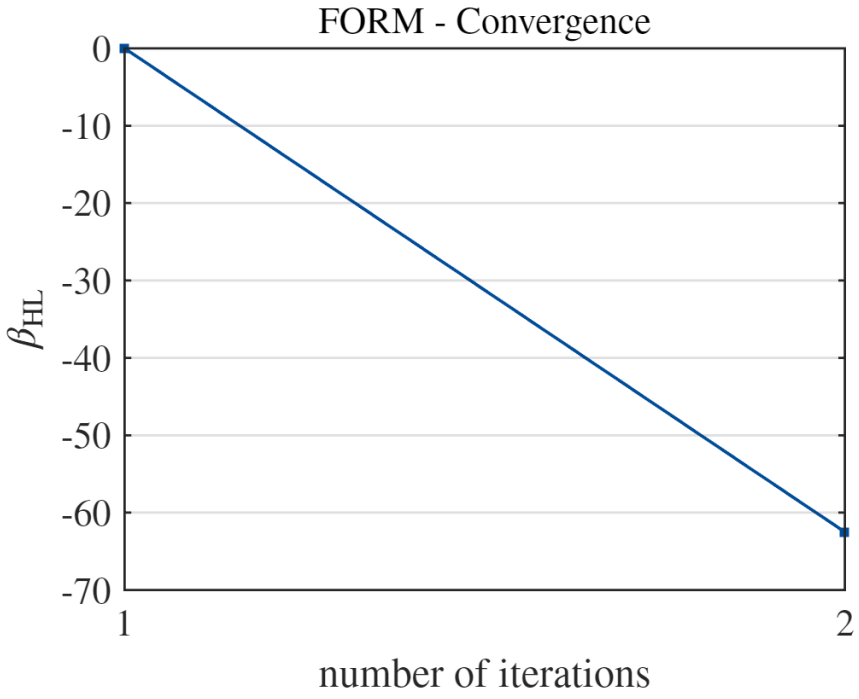
Print out a report of the results:

```
uq_print(FORMAnalysis)
```

```
-------------------------------------------------
FORM
-------------------------------------------------
Pf               0001
BetaHL           -62.5000
ModelEvaluations 6
-------------------------------------------------
Variables        P
  Ustar          62.500000
  Xstar          155
  Importance     1.000000
-------------------------------------------------
```

Create a graphical representation of the results:

```
uq_display(FORMAnalysis)
```



Monte Carlo simulation (MCS)

Select the Reliability module and the Monte Carlo simulation (MCS) method:

```
MCSOpts.Type = 'Reliability';
MCSOpts.Method = 'MCS';
```

Specify the maximum sample size:

```
MCSOpts.Simulation.MaxSampleSize = 1e6;
```

Run reliability analysis with MCS:

```
MCSAnalysis = uq_createAnalysis(MCSOpts);
```

Print out a report of the results:

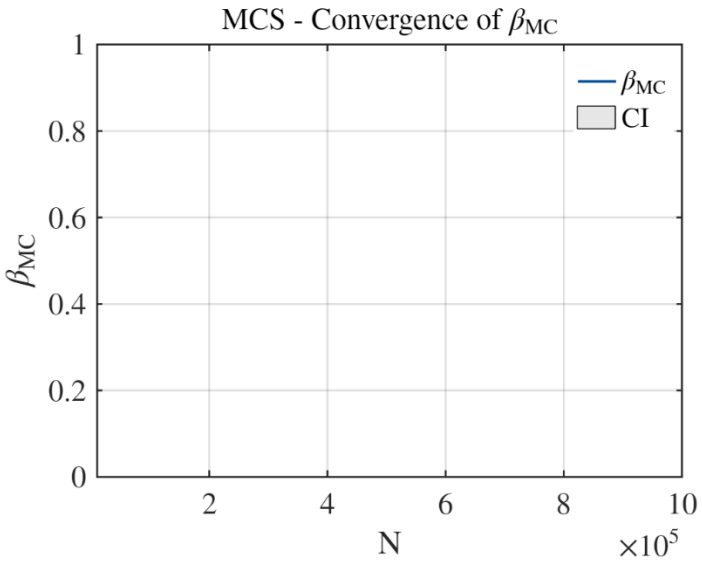
```
uq_print(MCSAnalysis)
```

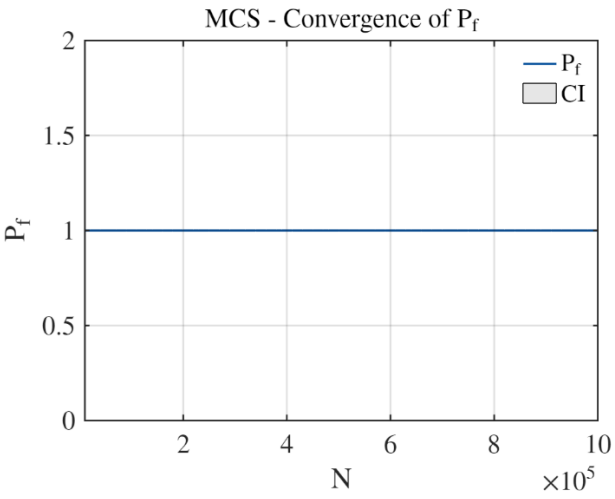
```
-------------------------------------------------
Monte Carlo simulation
-------------------------------------------------
Pf              0001
Beta            -Inf
CoV             0
```

```
ModelEvaluations 1000000
PfCI             [1.0000e+00 1.0000e+00]
BetaCI           [-Inf       -Inf      ]
--------------------------------------------------
```

Create a graphical representation of the results:

```
uq_display(MCSAnalysis)
```





Chapter 7: Conclusion & Recommendations

Final statement: does the system meet FAA safety objectives?

Yes eventually it does . by Reducing test interval. And we see that according to decision tree it is economical for us to just set 240 hours for test inspection of delivery and distribution subsystem and in this situation we have the highest utility (of course our utility function was a bit risk seeking).

Key improvements required.

Reducing test interval and educating maintenance and crew if I want to say it briefly .

Recommendations for future work (e.g., more accurate data, testing).

Reducing test interval and educating maintenance and crew if I want to say it briefly .

Link back to engineering responsibility and preventing Helios-like accidents.

According to National Geography documentation of this incident . somethings that links back to engineering responsibility for preventing helios like accidents are as follows:

1- In this accident the pilot was German and engineers were Greek and they could barely understand each other English accent and it made relationship hard . so we need better communicational abilities for both sides .
2- We should put the green light button which was in charge with indicating manual decompression system in the place which can be easily visible . as it was explained In the documentation it was barely visible in the morning sunlight .
3- After somewhile our heat sensors alarmed and it was not because the motor had problem (of course late on they experienced one engine inoperative situation) rather it was based on calibration of heat sensors that they malfunctioned in the low pressure so they have heavy dependency on pressure.

Appendix

Component	Failure rate λ (1/hour)	Distribution	Reference
Oxygen Cylinder	0.001 (analog to pressure vessels/coils)	Exponential	MIL-HDBK-217F Sec. 12.2; NASA reports
Pressure Transducer/Gauge	0.0055 (analog to photo-transistors/sensors)	Exponential	MIL-HDBK-217F Sec. 6.11
Manual Isolation Valve	0.0059 (analog to mechanical relays)	Exponential	MIL-HDBK-217F Sec. 13.1
Storage Regulator	0.0022 (analog to thyristors/regulators)	Exponential	MIL-HDBK-217F Sec. 6.10
Supply Lines/Manifold	0.00005 (analog to crimp connections)	Exponential	MIL-HDBK-217F Sec. 17.1
Face Masks	0.10 (analog to fiber optic connectors)	Exponential	MIL-HDBK-217F Sec. 23.1
human errors (using face mask)	0.01	Exponential	
storage box assembly	0.00001	Exponential	
toxic gas sensor	0.000001	Exponential	

References

1- Folder “references”
2- Folder “Matlab”
3- Folder “julia”
4- Folder “RESOURCES”
5- Folder ” decision tree”
6- AI
7- alaska flight 261.pdf