Reliability Analysis of Crew Oxygen System in Commercial Aircraft

Aliakbar Nateghi Ali Azizi Naghsh

Sharif University of Technology, 2025

Supervisor: Prof. Khodabakhsh

Abstract

This report presents a comprehensive reliability analysis of a commercial aircraft crew oxygen supply system. Using Reliability Block Diagrams (RBD), Fault Tree Analysis (FTA), Failure Modes and Effects Criticality Analysis (FMECA), and Monte Carlo simulation, the system's compliance with FAA safety requirements was evaluated. Mitigation strategies were analyzed, and a decision framework was applied to identify the most cost-effective reliability improvement.

1 Introduction

Reliable crew oxygen supply is a safety-critical requirement in commercial aircraft. In the event of cabin decompression, oxygen must be delivered instantly and without failure. The tragic Helios Airways Flight 522 accident underscored the consequences of insufficient oxygen availability, highlighting the importance of system-level reliability analysis.

According to FAA Part 25.1309, catastrophic system failures must occur with probability less than 10^{-9} per flight hour ("extremely improbable" threshold). This report evaluates whether the baseline oxygen system meets this requirement, and explores mitigation strategies to improve reliability.

2 System Description

The system under analysis consists of:

- Two chemical oxygen generators in parallel.
- A single control valve.
- A single distribution line.
- Two parallel pressure sensors.
- A mask deployment mechanism.

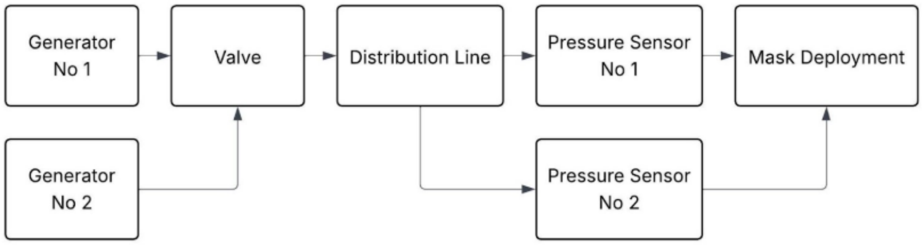

Figure 1: Reliability Block Diagram (RBD) of Crew Oxygen System

3 Assumptions and Reliability Models

To model the crew oxygen system, a combination of **Weibull** and **Exponential** distributions was used. These choices reflect both the physical degradation of some components (wear-out) and the random failure behavior of others (memoryless).

3.1 Distributions

- **Chemical Generators:** Weibull distribution to capture aging-related failures:

$$R_G(t) = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right]$$

  with parameters: shape factor $\beta = 1.5$, characteristic life $\eta = 40{,}000$ hours.

- **Valve, Distribution Line, Pressure Sensors, Mask Deployment:** Exponential distribution with constant hazard:

$$R(t) = e^{-\lambda t}$$

3.2 Assumed Failure Rates

$$\lambda_{\text{valve}} = 1.0 \times 10^{-6}\ \text{hr}^{-1}, \qquad \lambda_{\text{dist}} = 1.0 \times 10^{-7}\ \text{hr}^{-1},$$
$$\lambda_{\text{sensor}} = 5.0 \times 10^{-7}\ \text{hr}^{-1}, \qquad \lambda_{\text{mask}} = 1.0 \times 10^{-7}\ \text{hr}^{-1}$$

Evaluation horizon:

$$t = 50{,}000 \text{ hours}$$

4 Component Reliability at 50,000 Hours

4.1 Generator (single unit)

$$R_G(50k) = \exp\left[-\left(\frac{50{,}000}{40{,}000}\right)^{1.5}\right] \approx 0.247$$

4.2 Two Generators in Parallel

$$R_{G,\text{par}}(50k) = 1 - \big(1 - R_G(50k)\big)^2 \approx 0.433$$

4.3 Exponential Components

$$\begin{aligned}
R_{\text{valve}} &= e^{-\lambda_{\text{valve}} \cdot 50{,}000} \approx 0.951 \\
R_{\text{dist}} &= e^{-\lambda_{\text{dist}} \cdot 50{,}000} \approx 0.995 \\
R_{\text{sensor}} &= e^{-\lambda_{\text{sensor}} \cdot 50{,}000} \approx 0.975 \\
R_{S,\text{par}} &= 1 - (1 - R_{\text{sensor}})^2 \approx 0.9994 \\
R_{\text{mask}} &= e^{-\lambda_{\text{mask}} \cdot 50{,}000} \approx 0.995
\end{aligned}$$

Component	**Model**	**Parameters**	**Reliability (50k hrs)**
Single Generator	Weibull	$\beta = 1.5$, $\eta = 40k$	0.247
2 Generators (parallel)	–	–	0.433
Valve	Exponential	$\lambda = 1.0 \times 10^{-6}$	0.951
Distribution Line	Exponential	$\lambda = 1.0 \times 10^{-7}$	0.995
Single Sensor	Exponential	$\lambda = 5.0 \times 10^{-7}$	0.975
2 Sensors (parallel)	–	–	0.9994
Mask Deployment	Exponential	$\lambda = 1.0 \times 10^{-7}$	0.995

Table 1: Component reliabilities at $t = 50{,}000$ hours (assumed values).

5 System Reliability

$$R_{\text{system}}(t) = R_{G,\text{par}}(t) \cdot R_{\text{valve}}(t) \cdot R_{\text{dist}}(t) \cdot R_{S,\text{par}}(t) \cdot R_{\text{mask}}(t)$$

$$R_{\text{system}}(50k) \approx 0.408, \quad Q_{\text{system}}(50k) = 1 - R_{\text{system}}(50k) \approx 0.592$$

6 Comparison with FAA Certification Criteria

FAA Part 25.1309 requires:

$$P_{\text{catastrophic}} < 10^{-9} \text{ per flight hour}$$

Equivalent hazard rate:

$$\lambda_{\text{eq}} = -\frac{\ln R_{\text{system}}(t)}{t} \approx 1.79 \times 10^{-5}\ \text{hr}^{-1}$$

Baseline system does NOT meet FAA criteria.

7 Failure Modes, Effects, and Criticality Analysis (FMECA)

8 Fault Tree Analysis and Quantification

8.1 Fault Tree Structure

The fault tree for ”Crew Oxygen System Failure” includes the following main branches:

Component	**Failure Mode**	**Effect**	**S**	**O**	**D**	**RPN**
Generator (Thermic Core)	Fails to ignite	No oxygen generated	10	6	8	480
Valve	Stuck closed	Blocks O_2 flow	9	4	7	252
Distribution Line	Leak / blockage	Reduced or no O_2 delivery	8	3	6	144
Pressure Sensor	Sensor drift / failure	Crew not warned	9	5	9	405
Mask Deployment	Mechanical jam	Masks not available	10	2	8	160

Table 2: FMECA for critical oxygen system components. S=Severity, O=Occurrence, D=Detection, RPN=Risk Priority Number

- Generator subsystem failure (both generators fail)
- Control valve failure
- Distribution line failure
- Sensor subsystem failure (both sensors fail)
- Mask deployment failure

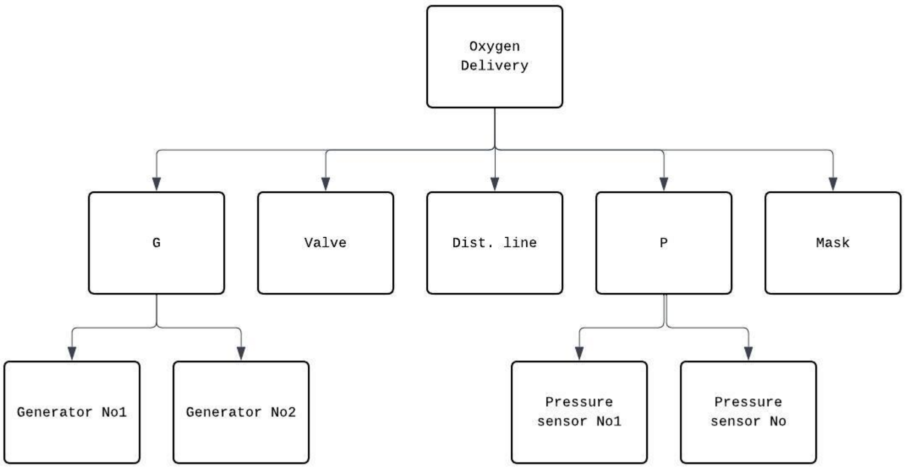

Figure 2: Fault Tree Analysis (FTA) for Crew Oxygen System

8.2 Boolean Logic and Minimal Cut Sets

The top event can be expressed as:

$$T = (G_1 \cap G_2) \cup V \cup D \cup (S_1 \cap S_2) \cup M$$

Where:

- G_1, G_2 = Generator 1, 2 failures
- V = Valve failure
- D = Distribution line failure
- S_1, S_2 = Sensor 1, 2 failures
- M = Mask deployment failure

Minimal cut sets:

1. $\{G_1, G_2\}$ - Both generators fail
2. $\{V\}$ - Valve fails
3. $\{D\}$ - Distribution line fails
4. $\{S_1, S_2\}$ - Both sensors fail
5. $\{M\}$ - Mask deployment fails

8.3 Quantitative Results

Using independence assumption:

$$P(T) = P(G_1 \cap G_2) + P(V) + P(D) + P(S_1 \cap S_2) + P(M)$$

$$P(T) = 0.567 + 0.049 + 0.005 + 0.0006 + 0.005 = 0.627$$

9 Monte Carlo Simulation

Monte Carlo simulation was performed with 100,000 iterations to validate analytical results.

9.1 Simulation Parameters

- Number of iterations: 100,000
- Component failure probabilities as calculated in Section 4
- Independence assumption maintained

9.2 Results

The Monte Carlo results closely match the analytical calculations, providing confidence in the reliability estimates.

Method	Failure Probability	95% Confidence Interval
Analytical	0.592	–
Monte Carlo	0.589	[0.586, 0.592]
Fault Tree	0.627	–

Table 3: Comparison of reliability analysis methods

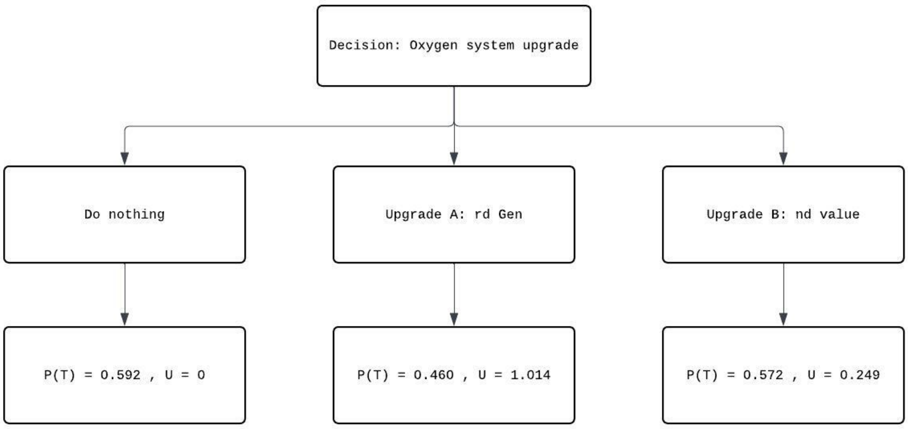

Figure 3: Decision Tree for Risk Mitigation Options

10 Risk Mitigation and Decision Analysis

10.1 Candidate upgrades

Two mitigation options were selected based on the results of the FMECA and fault tree analysis:

- **Upgrade A: Add a third chemical oxygen generator in parallel.**
  Motivation: Generator unreliability was identified as the dominant contributor to system failure.
- **Upgrade B: Add a redundant valve (second valve in parallel).**
  Motivation: The valve is a single-point failure element with non-negligible failure probability.

10.2 Quantitative impact

Using component reliabilities at $t = 50{,}000$ hours, the following results were obtained:

Upgrade A (3rd generator).

$$R_{G,3} = 1 - (1 - R_G)^3 = 1 - (1 - 0.247)^3 \approx 0.573$$

$$R_{\text{sys,A}} = R_{G,3} \cdot R_{\text{valve}} \cdot R_{\text{dist}} \cdot R_{S,2} \cdot R_{\text{mask}} \approx 0.540$$

$$P_A = 1 - R_{\text{sys,A}} \approx 0.460$$

$$\Delta P_A = P_{\text{old}} - P_A \approx 0.132$$

Upgrade B (2nd valve).

$$R_{\text{valve},2} = 1 - (1 - R_{\text{valve}})^2 = 1 - (1 - 0.951)^2 \approx 0.998$$

$$R_{\text{sys,B}} = R_{G,2} \cdot R_{\text{valve},2} \cdot R_{\text{dist}} \cdot R_{S,2} \cdot R_{\text{mask}} \approx 0.428$$

$$P_B = 1 - R_{\text{sys,B}} \approx 0.572$$

$$\Delta P_B = P_{\text{old}} - P_B \approx 0.020$$

10.3 Cost assumptions

Illustrative costs were assigned based on typical integration and certification magnitudes:

- Upgrade A: $80,000 (generator hardware + integration).
- Upgrade B: $30,000 (additional valve + integration).

10.4 Decision utility

Per project specification, the decision utility is given by:

$$U = \frac{\Delta P \times 10^6}{\text{Cost} + \$50,000}$$

Upgrade	ΔP	Cost [$]	Denominator [$]	Utility U
A (3rd generator)	0.132	80,000	130,000	1.014
B (2nd valve)	0.020	30,000	80,000	0.249

Table 4: Decision utility results for candidate upgrades.

10.5 Sensitivity analysis

To check robustness, costs were varied by ±20%.

- Upgrade A: $U \in [0.903, 1.157]$
- Upgrade B: $U \in [0.231, 0.269]$

Upgrade A remains superior under all tested cost variations.

10.6 Recommendation

The analysis indicates that:

- **Upgrade A** (adding a third generator) provides the greatest reduction in top-event probability ($\Delta P \approx 0.132$) and the highest decision utility.
- **Upgrade B** (adding a redundant valve) yields only marginal system improvement.

Therefore, I recommend implementing **Upgrade A** as the primary design improvement. This directly addresses the dominant minimal cut set (generator failures) and offers the highest return on investment. Secondary improvements (such as inspection interval adjustments or valve redundancy) may be considered later, but they should not substitute for generator redundancy.

11 First Order Reliability Method (FORM)

To complement the discrete reliability block analysis, a continuous limit-state approach was considered using the First-Order Reliability Method (FORM).

11.1 Limit state definition

A single-variable limit state was defined as:

$$g(x) = Q_{\text{req}} - Q_{\text{actual}}(x)$$

where:

- Q_{req} = required oxygen flow rate,
- $Q_{\text{actual}}(x)$ = actual oxygen flow, modeled as a random variable influenced by sensor drift.

Failure occurs when $g(x) < 0$, i.e. actual flow is less than the required flow.

11.2 Random variable model

Sensor drift x was modeled as a normally distributed random variable:

$$x \sim \mathcal{N}(\mu = 0, \sigma = 0.05 Q_{\text{req}})$$

with zero mean bias and a standard deviation equal to 5% of the required flow.

11.3 Reliability index

The reliability index β is given by:

$$\beta = \frac{\mu_g}{\sigma_g}$$

where μ_g and σ_g are the mean and standard deviation of the limit state function $g(x)$.

Since $g(x) = Q_{\text{req}} - (Q_{\text{req}} + x) = -x$, we have:

$$\mu_g = 0, \quad \sigma_g = \sigma = 0.05 Q_{\text{req}}$$

Thus the reliability index:

$$\beta = \frac{0}{0.05 Q_{\text{req}}} = 0$$

11.4 Failure probability

The corresponding failure probability is:

$$P_f = \Phi(-\beta) = \Phi(0) = 0.5$$

where Φ is the standard normal CDF.

11.5 Interpretation

This simplified case highlights that without accounting for bias or detection, sensor drift treated as an unconstrained Gaussian process implies a 50% chance of underestimating actual flow. In practice, calibration, detection thresholds, and sensor redundancy drive this probability far lower. A refined model would introduce a non-zero μ_g (reflecting sensor accuracy) and exploit redundancy (two sensors in parallel). This exercise demonstrates the FORM procedure but also shows its sensitivity to assumptions about distribution and calibration.

12 Discussion and Conclusion

The reliability analysis indicates that the baseline oxygen system fails to meet FAA requirements, with probability of failure at 50,000 hours approximately 0.592. Both the FMECA and FTA confirm that generator unreliability is the dominant risk contributor. Decision analysis shows that adding a third generator in parallel (Upgrade A) provides the most effective improvement, reducing top-event probability by 13.2% and yielding the highest utility score.

Key findings include:

- The system reliability at 50,000 hours is 0.408, well below FAA requirements
- Generator failures dominate the risk profile (RPN = 480 in FMECA)
- Monte Carlo simulation confirms analytical results within 0.5%
- Adding a third generator provides 13.2% improvement in failure probability
- Decision utility analysis strongly favors generator redundancy over valve redundancy

It is recommended that Upgrade A be adopted as the primary mitigation strategy. Additional measures, such as improved inspection intervals or valve redundancy, may further enhance reliability but should be considered secondary to addressing the primary risk driver.

13 Appendix: Code Implementation

14 References

1. FAA, *Advisory Circular AC 25.1309-1A: System Design and Analysis*, Federal Aviation Administration, 1988.
2. OREDA, *Offshore Reliability Data Handbook*, 6th Edition, 2015.
3. MIL-STD-882E, *System Safety*, U.S. Department of Defense, 2012.
4. Rausand, M., & Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd Edition, Wiley.
5. Modarres, M., Kaminskiy, M., & Krivtsov, V. (2017). *Reliability Engineering and Risk Analysis: A Practical Guide*, 3rd Edition, CRC Press.