RMD-305 Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション 305 起こり得る故障　解説書

2024 年 3 月

無人航空機の認証に対応した証明手法の事例検討
305 サブ WG 起こり得る故障

目次

図 目次

表 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」と呼ぶ）安全基準「セクション 305 起こり得る故障（以降、「セクション 305」と呼ぶ）」に対する解説書である。

なお、解説対象とする文書は国土交通省航空局から 2022 年（令和 4 年）12 月 2 日発行時点の航空局ガイドラインとする。解説対象に関する詳細は本冊（RMD　Rev.01）1.2 を参照すること。

2　対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領”（以降、「サーキュラーNo.8-001」と呼ぶ）」の「305 起こり得る故障」を以下に引用する。

・305 起こり得る故障

無人航空機は、単一の起こり得る故障によって機体の制御不能又は想定飛行範囲からの逸脱を生じないように設計されなければならない。これは、試験により実証されなければならない。

（a）　起こり得る故障については、少なくとも以下の機器に関係するものを考慮しなければならない。

（1）　推進系統

（2）　C2 リンク

（3）　全球測位衛星システム（GNSS）

（4）　単一障害点がある操縦系統の機器

（5）　コントロールステーション

（6）　申請者によって指定されるその他の関連システム（AE）

（b）　試験に使用する無人航空機は、無人航空機飛行規程に従って運用されること。

（c）　個々の試験は、飛行におけるクリティカルフェーズ及びモードに対し、最も厳しい操縦者と無人航空機数の比率で 実施しなければならない。

3　「航空局ガイドライン」（引用）

「航空局ガイドライン」安全基準「305 起こり得る故障」の「基準の概要」、「適合性証明方法（MoC）」、「その他参考となる情報」を以下に引用する。

・305 起こり得る故障

<u>基準の概要</u>

本基準では、起こり得る故障に対し試験を行うものです。これはセクション 300 の試験に追加で行うもので、セクション 300 とは別の観点で無人航空機を評価する必要性から行うものです。具体的には、単一の起こり得る故障（a probable failure）が発生した場合における無人航空機の機能・性能が低下した状態を評価するものです。

セクション 300 とは Pass/Fail Criteria が異なり、起こり得る故障に起因する機体の制御不能又は想定飛行範囲からの逸脱のみが許容されません。

想定飛行範囲からの逸脱については、無人航空機が飛行する空間と時間の観点から、明らかな飛行経路又は運用エリアからの逸脱を考慮します。本基準では、原則として着陸場所以外でのパラシュートや制御下にある非常着陸は許容され、着陸場所以外での墜落は制御不能とみなされますが、第一種型式認証と第二種型式認証との違い、またCONOPS によってPass/Fail Criteria の調整が必要になるため、検査者とよく話し合う必要があります。

なお、本試験は可能な限り飛行試験で行うことが望ましいものの、その場合、故障模擬を行うための専用ソフトウェア又はハードウェアが必要になるケースが考えられます。一方で、飛行試験が合理的でない場合又は安全への影響が考えられる場合、地上試験、ラボ試験又は解析も許容されます。

また、(a)項(1)～(6)に限らず、無人航空機の設計に応じてその他のフェイラーモードが考えられる場合、それが制御不能又は想定飛行範囲からの逸脱に繋がらないことを実証する必要があります。

この試験はエースパイロットのような熟練の操縦者ではなく、最低限の要件を満たした操縦者によって評価される必要があります。なお、最低限の要件を満たした操縦者とは、型式認証の種類(第一種型式認証又は第二種型式認証)に応じた操縦者資格又は当該資格に相当する能力及び当該機における最低限の操縦要件を満たす者となります。

適合性証明方法(MoC):6

(a),(b),(c): セクション 305 飛行試験方案 (MoC 6)

以下の故障状態を意図的に発生させて、無人航空機が制御不能又は想定飛行範囲からの逸脱を起さないことを評価します。試験ケースとして以下を考慮し、試験方案を作成します:

- *(1) 少なくともひとつの推進システム(例えばモーター)又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。この試験は厳しい飛行フェーズ、モード、最も不利な重量重心位置で行う*
- *(2) C2 リンクの品質低下(可用性の低下、サービス品質の悪化、信号雑音比(Signal-Noise Ratio: S/N)の低下、断続接続及び遅延など)を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(3) C2 リンクが完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(4) GNSS の品質低下を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(5) GNSS が完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(6) フライトコントロール機構における単一障害点(喪失)を実証する。例えば、シングルストリングサーボがある無人航空機では、ハードオーバーを実証すべきである*
- *(7) コントロールステーションの電源、表示ディスプレイ及び/又は運航者の制御用イン*

ターフェースの喪失を実証する

（8） 関連機器に応じた故障状態を実証する

（9） 複数の機体を一人の操縦者で制御する場合、同時に発生し得る最大機数の故障模擬において、その管理能力を実証する

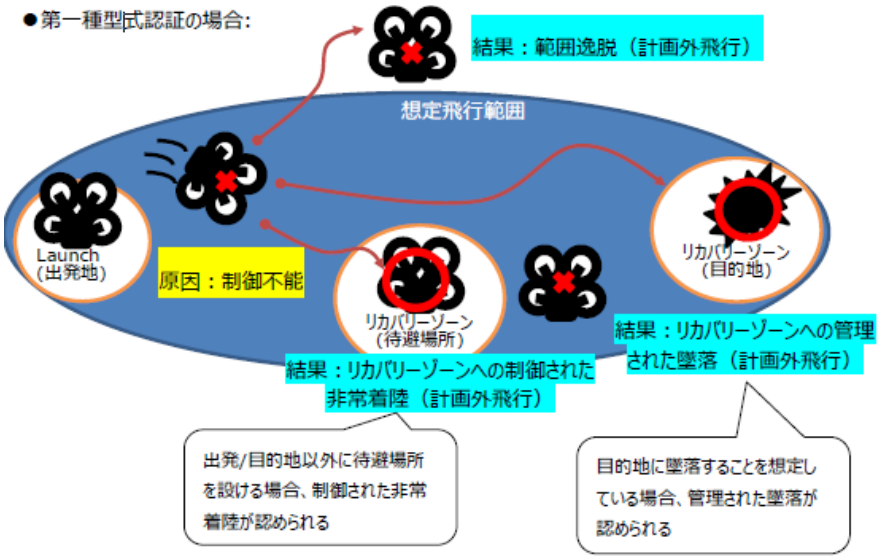
(a),(b),(c): <u>セクション 305 飛行試験報告書</u>（MoC 6）

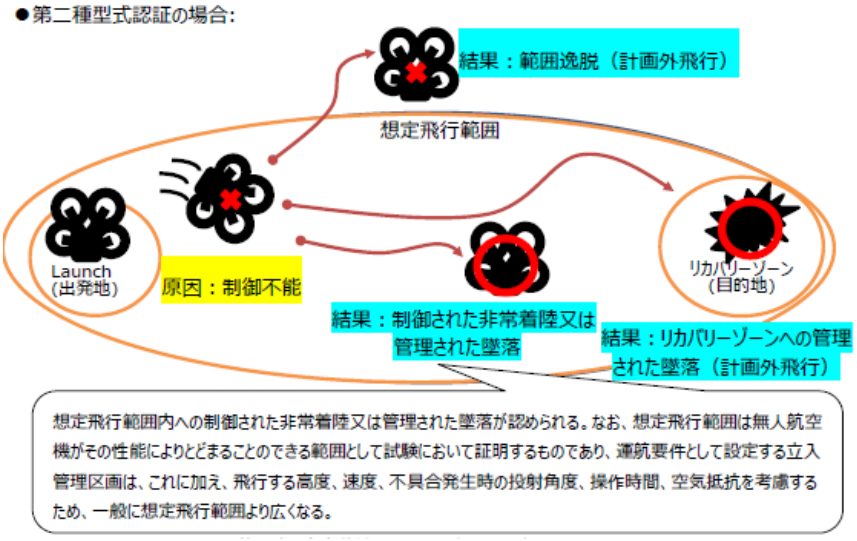
試験結果を報告書としてまとめます。

※「検査のポイント」および「検査者の関与度(LOI)」については引用記載しない

<u>その他参考となる情報</u>

セクション 305 の Pass/Fail Criteria を図示したものが以下となります:





4　解説書

4.1 はじめに

「航空局ガイドライン」では、基準の概要の冒頭にて

> *本基準では、起こり得る故障に対し試験を行う。これは「セクション 300 の試験に追加で行うものであり、「セクション 300」とは別の観点で無人航空機を評価する必要性から行うものである。具体的には、単一の起こり得る故障(a probable failure)が発生した場合における無人航空機の機能・性能が低下した状態を評価し、それに起因する「制御不能又は想定飛行範囲からの逸脱」が発生しないことを原則として試験により検証するものである。*
>
> *[引用:航空局ガイドライン／セクション 305 基準の概要]*

のように記述している。

本基準の第一の趣旨は任意の一故障時に地上の第三者などに被害を与えないことであり、第三者を排除した立入監視区域上空で運用をおこなう第二種認証対象の機体においては、飛行中断などを含め何らかの手段により、任意の一故障時に想定飛行範囲から逸脱しないことが重要である。一方で「サーキュラーNo.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領の安全基準(以降、「安全基準」と呼ぶ)」の要求にはそれと並んで「制御不能」を生じないことが挙げられており、この意義も含めて検査者と申請者の調整により試験方案、Pass/Fail criteria を確立した上で立証を行うことが必要となる。

4.2 適用対象などについて

(1) 基準の適用範囲

「2 対象の基準「サーキュラー」(引用)」で示したサーキュラー基準本文の適用範囲について示す。

同じく「サーキュラーNo.8-001」第Ⅱ部第 1 章の表 1 に示される。以下表 4.2-1 に該当箇所(枠内)を示す。最大離陸重量が 25kg 未満の機体(表中二重枠で表示)で、目視外飛行を実施しないものについては、セクション 305 自体が適用されない。一方同じ 25kg 未満の機体で目視外飛行を実施するものについては、表外の注記※8 が適用され、セクション 305(a)項(2)、(3)、(6)のみ適用される。

(2)C2 リンク

(3)全球測位衛星システム(GNSS)

(6)申請者によって指定されるその他の関連システム(AE)

表 4.2-1 区分に応じて適用される規定

（凡例）✓：適用されるもの、✓✓：該当する特定飛行※1に応じて適用されるもの、N/A：適用されないもの

区分	第二種				第一種
	機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機				機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機
	最大離陸重量4kg未満のもの	最大離陸重量4kg以上25kg未満のもの	最大離陸重量25kg以上のもの		人口密度の低い地域その他の無人航空機の飛行により航空機の航行の安全並びに地上及び水上の人及び物件の安全を損なうおそれが少ないと認められる地域を飛行するもの
			特定飛行を行うもののうち、無人航空機の飛行により航空機の航行の安全並びに地上及び水上の人及び物件の安全を損なうおそれが少ないと認められるもの※2	その他のもの※3	
001 設計概念書(CONOPS)	✓	✓	✓	✓	✓
005 定義	✓	✓	✓	✓	✓
100 無人航空機に係る信号の監視と送信	✓※4	✓	✓	✓	✓
105 無人航空機の安全な運用に必要な関連システム	✓	✓	✓	✓	✓
110 ソフトウェア	✓※5	✓※5	✓※5	✓	✓
115 サイバーセキュリティ	✓	✓	✓	✓	✓
120 緊急時の対応計画	✓✓※6	✓	✓	✓	✓
125 雷	✓	✓	✓	✓	✓
130 悪天候	✓	✓	✓	✓	✓
135 重要な部品（フライトエッセンシャルパーツ）	✓	✓	✓	✓	✓
140 その他必要となる設計及び構成	✓※7	✓※7	✓※7	✓※7	✓※7
200 無人航空機飛行規程	✓	✓	✓	✓	✓
205 ICA	✓	✓	✓	✓	✓
300 耐久性及び信頼性	✓	✓	✓	✓	✓
305 起こり得る故障	✓✓※8	✓✓※8	✓	✓	✓
310 能力及び機能	✓※9	✓	✓	✓	✓
315 疲労試験	N/A	N/A	✓	✓	✓
320 制限の検証	N/A	N/A	✓	✓	✓

※8：目視外飛行の場合は 305(a)項(2)、(3)及び(6)がそれぞれ適用。それ以外の飛行の場合は非適用

出所）サーキュラーNo.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領

セクション 305 はすべての機器を対象としたうえで、セクション 305(a)項指定のものを最低限とする規定であるが、限定の趣旨を考えると、ここでは(2)、(3)、(6)についてのみ立証を行えば良いものと解釈される。その他機体区分（表中点線枠で表示）については、すべて適用となる。

なお、この解説書内では、すべて適用となる場合（最大離陸重量が 25kg 以上の機体）を想定して記載する。

（2）「起こり得る故障」とは

「起こり得る故障：probable failure」を設計検討の際に、極端に故障の発生確率が低い機器に対し過剰な試験を行うことは合理的ではない。設計情報として故障の発生確率を示すことができれば「起こり得る故障」に該当しないと考えられる。ただし、その場合でも最低限実施しなければならない対象を識別したのが、セクション 305(a)項の規定であると考えられる。

では、どの程度の確率を目標とすることが合理的かということになるが、米国連邦航空局（Federal

Aviation Administration：FAA)の基準などから“probable”には、

① 全ライフサイクルにおいて 1 回以上発生するもの

② 一般的に故障状態に対して“Allowable Qualitative Probability”として定性的な要求

という 2 つの解釈がある。②の定性的な要求に対応する定量的な値が Advisory Circular などで示されており、このいくつかの数値例を【参考 1】に紹介する。いずれも飛行時間当たりの発生頻度(probability)として規定されている。機体規模が大きくなると重大度(severity/consequence)が大きくなるので、発生頻度の要求を厳しくしていることが読み取れる。無人航空機の場合は飛行時間当たり 1.0×10^{-3} 程度と考えてよいと思われ、そのような無人航空機の機体寿命が一般に 1,000 時間以下であろうことを勘案すると、制限寿命の中で 1 回以上発生するような故障を想定すればよいと考えられる。また、①に関連して、欧州航空安全機関(European Union Aviation Safety Agency：EASA)では、Special Condition for Light Unmanned Aircraft Systems - Medium Risk においても、注記ではあるが、“probable”は定量的ではなく、定性的に“全ライフサイクルにおいて 1 回以上発生するものと理解する必要がある”と記載している。

※ FAA、EASA における基準などの解釈がそのまま本邦安全基準に適用されるわけではないことに注意は必要であるが、一方で、本邦安全基準が制定にあたって FAA の D&R による証明法を参照していること、EASA は、ASTM-F3478 を適用可能な立証方法(Acceptable Means of Compliance：AMC)として認めており、D&R による証明法についても FAA と協調が進んでいることなどを考えると、上記の考え方により、想定される機体寿命内で発生が想定するような故障を「起こり得る故障」と見做すことは十分に妥当性があると考えられる。

ただし、セクション 305 の対象としないということは、当該故障により想定飛行範囲から逸脱しうる可能性が検証されないということでもある。想定飛行範囲からの逸脱が直ちに第三者の死傷などの破局的なハザードに直結するわけではないため、例えば【参考 2】のような数値がそのまま適用されるわけではないが、対象となるかどうかの基準としてどの数値が妥当かについては、CONOPS も踏まえて十分な検討の上、検査者との合意形成が必要である。

【参考 1】航空関係の基準などにおける probable failure の数値(飛行時間当たりの確率)例：

- FAA AC23.1309[1](軽飛行機向け) 1.0×10^{-3}
- FAA AC25.1309[2] 1.0×10^{-5}
- JARUS AMC RPAS 1309-01[3] 1.0×10^{-3}

【参考 2】機能安全に関する情報：

IEC61508-1(JIS C0508-1) [4]高頻度作動・連続モード時 失敗尺度

SIL4 10^{-9} 以上 10^{-8} 未満

SIL3 10^{-8} 以上 10^{-7} 未満

SIL2 10^{-7} 以上 10^{-6} 未満

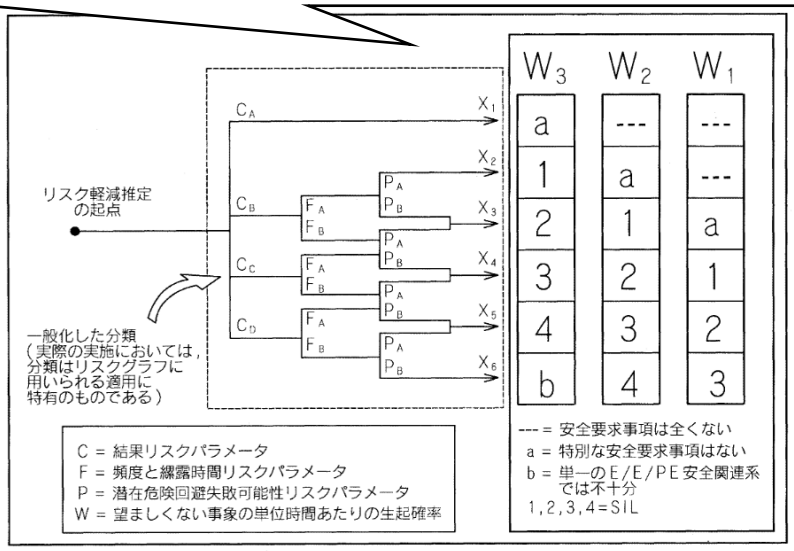
SIL1 10^{-6} 以上 10^{-5} 未満

SIL (Safety Integrity Level) はリスク(被害のひどさ、頻度、回避可能性などの組み合わせ)によって変化する。一般的には確率が低くても複数人の死亡がある場合などは SIL4 といわれる。詳

しくは、IEC61508-5[5] Annex D で紹介されるリスクグラフなど(図 4.2-1)が参考となる。なお、図中のパラメータ(C_A,C_B,C_C,C_D,F_A,F_B,P_A,P_B,W_1,W_2,W_3)の厳密な定義とそれらの重み付けは、それぞれの特別な状況や同種の産業分野ごとに定義される必要がある。

【参考】
「数値を明確に示してほしい」は設計者が持つ当たり前の要求である。故障の発生確率の数値が 10^{-3} か 10^{-7} で異なると、例えばハードウェアは、単一部品か、もしくは、信頼性向上のために冗長設計が求められるなどの違いがあり、設計や製品コンセプトに多大な影響を与える。
当解説書作成のワーキンググループでも、専門家により故障の発生確率についての議論が行われたが、主張する数値に大きな乖離が出て結論には至っていない。これには、以下 2 つの理由が考えられる。
1. 数値を定められるほどの実績が市場に存在していない
2. 既存で用いられる数値の妥当性を社会合意できる情報が存在しない(例えば壊滅的を防ぐために10^{-x}で十分かを説明されることはない。規格策定では実績を元にした技術限界／社会情勢を鑑み、妥協も含む合意形成で決めている)

これら 2 つの理由が示すのは、数値を定めるためには、経験的に得られる実績を元に社会的な合意形成(各種の規格書策定の議論も該当)が必要である。市場に製品を普及させる製造者が、より良い製品づくりのために、規格策定活動に参加する意義が見いだせる事例とも捉えられる。



附属書D図1 リスクグラフ：一般的スキーム

図 4.2-1 安全に関するリスクグラフ

出所)JIS C0508-5:1999[5]附属書 D(参考)「定性的方法による SIL の決定:リスクグラフ)」を引用し、吹き出し部分を加筆

(3) 対象となる機器・フェイラーモードの識別

1) 識別のポイント

「航空局ガイドライン」には、基準の概要にて

> *(a)項(1)～(6)に限らず、無人航空機の設計に応じてその他のフェイラーモードが考えられる場合、それが制御不能又は想定飛行範囲からの逸脱に繋がらないことを実証する必要があります。*
>
> *[引用:航空局ガイドライン／セクション 305 基準の概要]*

と記述されている。そのため基本的にはすべての機器が対象になると考えられる。またフェイラーモー

ドについても、単なる機能喪失にとどまらず、その他にも、暴走、劣化、遅延、固着など、期待した通りに動作しないすべてのフェイラーモードを考慮する必要がある。とはいえ、実行上すべての機器のすべてのフェイラーモードについて立証することは現実的でないため、安全性解析などの手法により、「機体の制御不能又は想定飛行範囲からの逸脱」が起こる可能性のあるものに限定して、試験などによる立証を行うこととなる。安全性解析の結果は、検査者と申請者の間で、部品別のフェイラーモードとその至る結果を共有しやすい文書となる。そのため、すべてをただ網羅的に確認するよりも効率的に試験を行うべき箇所を抽出できるものとなる。ただし、これはすべてのフェイラーモードを網羅的に試験してはいけない、ということではない。部品点数がそれほど多くなく、すべてを試すことが合理的である場合には、1 つの方法として総当たりでの試験も実施可能である。

2） 安全性解析について

安全性解析についてはFTA、FMEA、FHA、STAMP/STPA、リスクアセスメントなどの手法があるが、特に「セクション 135 重要な部品(フライトエッセンシャルパーツ)(以降、「セクション 135」と呼ぶ)」について解説する関連文書[6]において、フライトエッセンシャルパーツ識別の手段として簡易 FMEA によるケースが解説されているため、そちらを参照されたい。ただし、同文書で識別されるフライトエッセンシャルパーツはセクション 305 の対象の識別とはクライテリアが異なるため、フライトエッセンシャルパーツが必ずしもセクション 305 の対象となる、またはその逆となるわけではないことには注意しなければならない。解析の結果から得られる機体システムへの最終的な影響を勘案し、4.3 項で述べるセクション 305 としての Pass/Fail criteria に基づいて対象となる機器、フェイラーモードを識別することが必要になる。

注意点として、「対策」として冗長設計などにより「制御不能又は想定飛行範囲からの逸脱」を防ぐ構造となっている場合についても冗長設計の正しさを証明する観点からセクション 305 の対象になると考えられる。換言すれば「機体の制御不能又は想定飛行範囲からの逸脱」いわば頂上事象として FTA を実施した際に、原因として識別される機器・フェイラーモードがセクション 305 の対象になると考えれば良い。

解析の粒度についても、申請時に提出する書類に含まれる(e)部品表との一致が望ましいが、試験方法や設計活動の結果、部品表よりも要素単位が「統合する」「分割する」は、発生しても直接的な問題はない。必要なことはそれぞれ文書間、設計情報の間に発生するトレーサビリティが取れることとなる。

安全性解析で行う簡易 FMEA ともトレーサビリティが必要となるため、部品表、簡易 FMEA などで設計粒度をあわせ、セクション 305 試験の対象となる機器の切り分けを行うことで、トレーサビリティのための煩雑な作業を避けることができる。

また、“故障”が対象であることから、構造部材などの構造破壊については対象とならないものと考えるが、機器のいわゆる“故障”が内部の物理的・機械的な損傷に起因するようなケースについては考慮が必要と考える。

サンプル事例:(これらがすべてではない点に留意が必要)

- モーター・ステータ折れ → 一般的には故障と見做される。

- ボルトの破損　→　複数本で止めているようなもの（1 本の破損が「機体の制御不能又は想定飛行範囲からの逸脱」に至らない場合）は、含まれない。

3）　ソフトウェアエラーの扱い

ソフトウェアエラーによる「機体の制御不能又は想定飛行範囲からの逸脱」が発生することが想定される場合には対象として扱う。

ソフトウェアエラーは、一般的にはシステマチック故障として扱われる（バスタブ曲線による発生ではなく、バグとして潜在的にある故障モード）ため、「セクション 110 ソフトウェア（以降、「セクション 110」と呼ぶ）」で規定された、テスト、形態管理、不具合管理など、開発プロセスの品質によって担保することが前提となる。一方で、ハードウェアとの相互作用など、ハードウェアと不可分な要目もあり、「セクション 300 耐久性と信頼性（以降、「セクション 300」と呼ぶ）」による実動作環境での動作確認のための評価時間についても十分にソフトウェア品質に貢献していると考えられる。これら手法により、ソフトウェアエラーを最小化する必要がある。

（4）　ヒューマンファクターの取り扱い

「航空局ガイドライン」では基準の概要において

> *この試験はエースパイロットのような熟練の操縦者ではなく、最低限の要件を満たした操縦者によって評価される必要があります。*
>
> *［引用：航空局ガイドライン／セクション 305　基準の概要］*

のように記述されている。

セクション 305 の対象となる機器の故障にヒューマンエラーは含まなくてよい。ただし、試験時の操縦者の規定については検討を行う必要がある。「エースパイロットのような熟練の操縦者ではなく、最低限の要件を満たした操縦者」は、飛行規程に添った操作を確実に実施できる一方で、それ以上の咄嗟の判断やより適切な操作などまでは実施できない操縦者と解釈できる。

また、操縦者へ与えるワークロードも考える必要があるが、有人航空機で用いられている handling quality 評価の Cooper-Harper Rating（CHR）Scale[7]などが参考になると考えられる。以下は負荷となると考えられる項目を抽出した。

- 継続的に過度な作業負荷が求められる
- 過度な繰り返し作業が求められる
- 誤操作が致命的な影響となる操作が不用意に実施できる
- 操縦者が知るべき機器の状態が明確に伝達されていない
- 情報取得に手間取るユーザインタフェース
- 多様な解釈が可能となる警告表示
- 自律制御から人制御の切り替えが明確でない
- 自律制御から人制御への切り替えと同時に急な制御が求められる

- その他

一部項目については、「セクション 310 能力及び機能（以降、「セクション 310」と呼ぶ）」でも規定されており、相関を取りながら設計検討する必要がある。

4.3 前提となる安全管理手法

（1） 立証のポイント

「安全基準」にある通り、「制御不能又は想定飛行範囲からの逸脱」が発生しないことが最終的な Pass/Fail criteria となる。

第二種認証を申請する無人航空機においては、運用時には飛行領域（落下時の飛散領域も含む）に第三者がいない前提となるため、「想定飛行範囲からの逸脱」を発生させないことで第三者への危害を防止することが重視されると考えられる。ただし、要求に「制御不能」が追加されている趣旨を考慮すると、その場合においても、飛行領域における立入管理措置の実効性や第三者の資産（含むライフラインなどのインフラなど）への重大な危害、運用関係者の死傷なども考慮されている可能性があり、単純に「想定飛行範囲からの逸脱」さえしなければ良いとも言いかねる点に留意する必要がある。

（2） 飛行中断に関する“制御不能”の考え方

第二種認証を想定する機体は概ね立入管理区域の上空を飛行するものと想定され、故障などが生じて制御された飛行を継続することができない場合に、地上からの操作やフライトコントローラの指示により飛行を中断することで想定飛行範囲からの逸脱を防止し、第三者への危害を防止するものが多くある。また、特定の故障（例えばフライトコントローラからの信号喪失、動力の喪失など）に際しては、結果的に速やかに自由落下状態に至り、発生地点付近に落着することで、立入管理区域からの逸脱、ひいては第三者への危害防止を担保するような機体も存在する。このような機体についても飛行範囲や安全措置の条件などを飛行規程に適切に規定し、それにしたがって運用することによりセクション 305 の条件のうち「想定飛行範囲からの逸脱」を防止することができる一方、飛行中断措置実施後、ないし故障発生後の自由落下状態、パラシュート降下状態などでは制御された飛行状態を維持しているわけではないことから、もう 1 つの条件である「制御不能」を防止できておらず、セクション 305 の Pass/Fail criteria をクリアできていないのではないかとの指摘が考えられる。

制御不能については、「安全基準」にて

> *制御不能とは、無人航空機の制御された飛行状態からの意図しない逸脱を意味する。（中略）制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。*
>
> *［引用：サーキュラー No. 8-001／セクション 005］*

のように定義されている。一方で、関連文書[8]では「制御不能」の解釈について

> *制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。 ただし、運用者によって管理されている飛行中断は*

制御不能の範疇に入らない。

運用者によって管理されている飛行中断とは、結果としても死傷者（死者及び又は重傷者）が生じないための管理がされた飛行空域及び地上範囲に運用者によって意図的に飛行を完了させること

［引用：航空局ガイドライン解説書（本冊）］

とする見解を示している。上記の「死傷者が生じないための管理」は必ずしも第三者に限定されるものではないため、「想定飛行範囲からの逸脱」を防止しさえすれば良いというものではないが、それらが担保される限りにおいては制御された飛行状態を維持することまでは必須ではないと考えられる。また実際、「航空局ガイドライン」においても、“その他参考となる情報”に Pass/Fail criteria が図示されており、その吹き出しの中で

想定飛行範囲内への制御された非常着陸又は管理された墜落が認められる

［引用：航空局ガイドライン／セクション 305　その他参考となる情報］

との記述があるため、一時的に制御された飛行状態を維持できなくなることについて、最終的に「管理された墜落」に至ることを条件として、原則としては許容されていると見ることができる。

（3） 管理された墜落の考え方

「管理された墜落」は、「航空局ガイドライン」（共通 3.2 用語／略語）にて

無人航空機そのものに加え、墜落後の部品の飛散範囲を考慮するなど予め設計上で想定された墜落のこと。無人航空機飛行規程で操縦者（運航体制）へ別途具体的な指示を行うことを前提とした墜落が該当。
（例）部品の飛散が立入管理区画を超えないように墜落させること　等

［引用：航空局ガイドライン／共通 3.2 用語/略語］

と規定されているため、飛行中断などについても墜落後の部品の飛散範囲の考慮など、設計時点で想定されたものであれば「管理された墜落」に該当すると考えられる。追記の「飛行規程で操縦者へ別途具体的な指示を行うことを前提とした墜落が該当。」については、落下分散や上記部品の飛散も含めて想定飛行範囲領域から出ないように、そのような飛行計画の立案方法、風速制限、運用条件（高度、速度、重量など）に応じた落下分散や部品の飛散範囲の導出方法とかが飛行規程に明記されているということを言っていると考えられる。

フライトコントローラの機能喪失や電源の喪失などの単一故障により、操縦者のその時の意図・操作に関係なく墜落に至るような機体も考えられるが、このような挙動についても設計上で想定されており、墜落時の飛散範囲などを示すなど、想定飛行範囲からの逸脱を防止し、安全を確保するための手段が飛行規程に明示されていることで「管理された墜落」と見做すことが可能となる。

ただし、一時的にも制御された飛行状態からの逸脱が発生することから、安全についての実効性を示す必要がある。これらも CONOPS との相関がある事象のため、個別のケースに対応して、検査者

と申請者の相談により認証プロセスの早い段階から合意した方針が示せることが望ましい。

4.4 実際の立証方法

本項では、実際の立証法について、各対象に共通する基本的な考え方を記述する。実際の試験方案については Appendix 1.2 にそれぞれのケースに対応してまとめた。

(1) 飛行試験の必要性

セクション 305 の記述では「試験により」となっており、立証のための試験は必ずしも飛行試験である必要はないと考えられるが、一方で「航空局ガイドライン」の MoC では

> *以下の故障状態を意図的に発生させて、無人航空機が制御不能又は想定飛行範囲からの逸脱を起さないことを評価します。*
>
> *［引用：航空局ガイドライン／セクション 305 MoC］*

となっており、単純に故障状態から制御不能又は想定飛行範囲からの逸脱を起こさないことを立証する以上、想定する飛行状況での試験が暗に前提となっているようにも読める。ただ、一方で同じ「航空局ガイドライン」でも

> *なお、本試験は可能な限り飛行試験で行うことが望ましいものの、その場合、故障模擬を行うための専用ソフトウェア又はハードウェアが必要になるケースが考えられます。一方で、飛行試験が合理的でない場合又は安全への影響が考えられる場合、地上試験、ラボ試験又は解析も許容されます。*
>
> *［引用：航空局ガイドライン／セクション 305 基準の概要］*

との記述もあり、やはり飛行試験が必須とまでは要求していないと考えられる。総合すると

- 本来の要求としては、解析ではなく「試験」であることが必要
- 「飛行試験が合理的でない場合 or 安全への影響が考えられる場合」に限定して、地上試験、ラボ試験、さらには解析へと緩和することが許容される

と言える。ただし、「航空局ガイドライン」の MoC に記述されているような飛行状態からの立証によらない場合、単純に試行して「制御不能又は想定飛行範囲からの逸脱」が起きなかったという形では立証できないため、どのような形で Pass/Fail criteria を設定するかが問題になると考えられる。例えば不具合に対して安全機能を起動できることを地上試験などで立証した上で、安全機能が起動できれば「制御不能又は想定飛行範囲からの逸脱」が起きないことを別の試験や解析で立証するような方法、環境条件の影響に関係ない部分を飛行実験で実証した上で、環境条件の影響は解析で補完するような方法、解析で立証した上で、解析の妥当性を飛行実験で実証したりするようなこともあり得ると考える。そのうえで重要なことは、地上試験にせよ解析にせよ、

- 飛行試験では合理性や安全性に問題があること

- その手法で要求される故障許容性が(飛行試験よりも合理的に)立証できること

を申請者が検査者に筋道立てて説明した上で、合意された試験方案および Pass/Fail criteria を得ることであると考える。

(2) 「厳しい飛行フェーズ」とは

例えば「航空局ガイドライン」では、適合性証明方法(MoC)の(1)で

> *この試験は厳しい飛行フェーズ、モード、最も不利な重量重心位置で行う*
> *[引用:航空局ガイドライン／セクション 305 MoC]*

のように記述されている。最も不利な重量重心位置についてはセクション 300 と同様に考えられる。

厳しい飛行フェーズについては故障ケースに依存すると考えられるが、例えば、典型的なパターンとして、機体の暴走に対応して地上からの指令で強制降下するような状況を想定すると

- 想定飛行範囲から導出される飛行可能な空域の外縁に一番近いところで
- 外縁のほうに向かって最大(対地)速度で飛行しており
- 外部風も真後ろから運用可能な最大風速で吹いていて
- 不具合の検出や操縦者の判断に要する時間が最大(といっても判断ミスや不必要な逡巡などはないとして)である

ような状況が考えられる。この場合でも、例えば巡航だけではなく上昇・降下を考えた場合

- 上昇中は、水平速度が低いことから巡航中に比べると落下分散が少なくなる傾向がある一方、出力が大きいので暴走(例えば推力指令値の固着など)のときにより速度が上がりやすく、高度が上がることで落下分散が拡大する傾向がある。
- 降下中も、水平速度は比較的小さいが、出力を絞っていることで制御余裕が少なくなり、安定性が低くなるような傾向もある。

など、どのフェーズが最も厳しいか単純には決められない場合もある。上記のような状況を総合的に検討して「厳しい飛行フェーズ」を選定する、場合によっては複数フェーズを「厳しい飛行フェーズ」として識別したりするといった可能性もある。

ただし、落下分散については、実際に飛行領域の外縁で試験を実施しなくても、安全なところで故障を模擬して発生地点から最終的な落下地点までの距離を計測し、飛行規程で要求されているクリアランスの範囲内であることを確認するような方法もあると考えられる。また外部風の影響についても、解析で加算するような方法も考えられる。外部風の落下分散への影響を解析的に評価する方法については、JIS W 0711[8]の解説書が参考になる。

(3) 試験回数について

セクション 300 には使用する機数についての要求があるが、セクション 305 については「航空局ガイドライン」他には試験の回数に対する具体的な要求はなく、クリティカルな状況を押さえられれば 1 回

の試験で良いと考えられる。一方で、確率事象や気象条件、ヒューマンファクターなんかの影響のために 1 回でクリティカルな状況を押さえられるか分からない場合は、複数回試験を実施するケースも出てくると考える。一方で、品質のばらつきやソフトウェアエラーはセクション 300 やセクション 110 で押さえていると考えられ、その再現のために複数回の試験を実施する必要はないと考えられる。最終的には所定の回数の試験でクリティカルな状況を押さえられることを検査者に説明し、合意された試験方案および Pass/Fail criteria を得られれば良いと考える。

（4） 故障模擬の方法

故障模擬の方法については、故障を想定する機器や想定するフェイラーモードに依存するが、飛行中に実際に故障を発生させるために、ハードなりソフトなりの改修は許容されると考えられる。

例えば、喪失の模擬としては、実際に配線を抜く、伝送経路に継電器などを挿入して実際に伝送経路を切断するなどの方法が考えられるが、これを飛行中に実施するのは困難であったり危険であったりするため、ソフトウェア的に模擬することも許容されると考えられる。ただし、喪失の結果が「不定」になる場合など、ソフトウェアでの模擬が妥当か、検討が必要な場合もあると思われる。

結局のところ、想定する故障の結果としてどのような効果が生じて、実際に模擬する手段でそれが包含できているということを、検査者に説明して、合意された試験方案および Pass/Fail criteria を得る必要がある。故障の結果がどのようになるかについては、安全性解析の分析結果も利用することができる。

模擬のための改修は機体コンフィギュレーションの変更になるが、それなしで故障を模擬することが困難である以上、許容されると考えられる。これについても変更の内容、それが立証したい機能の部分に影響がないことの説明などを通じて、検査者と合意する必要がある。また、コンフィギュレーションを変えたために、試験そのものが危険にならないように注意する必要がある。例えば一故障の発生に対して想定飛行範囲からの逸脱などが発生しないようになっている機体でも、最初から一故障が発生した状態相当だと、次の一故障で危険な状況が発生しうることに注意し、安全が確保できない場合は、地上試験や屋内試験などにより、安全を確保することも考える必要がある。

（5） 複数同時喪失の考え方

「航空局ガイドライン」では MOC(1)の中で、推進系の故障について

> *又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。*
>
> *［引用：航空局ガイドライン／セクション 305 MoC］*

のように記述されていることから、セクション 305 においては、「単一の起こり得る故障」を対象とするが、「複数同時喪失」が存在する場合を想定することが望まれていると考えられる。

例えば、2 つの推進システムを 1 つのモーターコントローラ(ESC)で制御している場合において、ESC が故障(すなわち単一の起こり得る故障)した場合の対策を求める記述である。この場合の試験においては、2 つの推進システムが同時に停止した場合に、想定した対策が取れることを証明する必

要がある。

また、機器の故障ではないが、外的な単一の要因、例えば雷撃、氷結、砂塵、鳥衝突などの影響により、複数機器が同時に故障することも考えられないわけではない。セクション 305 はあくまで機器の起こり得る単一故障への対応を求めるものであり、このような事態への対応は原則として同セクションにおける安全基準要求の埒外と考えられる。また、特に外部の気象条件に起因するものについては「セクション 120 雷」、「セクション 125 悪天候」などにしたがって対応することが原則となる。ただし、CONOPS に規定される運用方法において、このような事態が相応の頻度で想定されうると判断された場合には、セクション 305 の手法を準用して試験による実証をおこなうこともあり得るとは思われる。

5　今後の課題(未議論項目)

5.1　非常対応における飛行試験と、セクション 300 との関係

セクション 300 では耐久性と信頼性の評価をおこなうために、すべての飛行エンベロープの評価を含む飛行試験による立証が求められている。一方で、MoC としては複数の代表的な運用の仕方(ミッション)および飛行ルートによる飛行試験が求められており、危険などを回避するための行動や非常運用など通常の運用以外の局面における検証は(結果的に飛行試験の中で実施する羽目になってしまう可能性はあるにしても)明確には要求されていない。

一方で、セクション 305 では耐久性の評価が求められていないことから、セクション 300 で規定されているように、クリティカルな環境条件などを網羅的に実証することについては明示的な要求がない(厳しい飛行フェーズ、モード、最も不利な重量重心位置についての要求はあるが、これが環境条件まで包含する要求とは、陽には読み取り難い)。

このため、

- セクション 300 の評価において、例えば最大荷重が生じるような機動が、避航や非常運用など通常の運用以外の局面でのみ用いられるような場合における耐久性などの評価。
- セクション 305 の評価において、制御不能や環境条件、制御不能又は想定飛行範囲からの逸脱が発生しないことの判定について、環境条件がクリティカルになり得るようなケースにおける評価。

などが担保されないことが懸念される。最終的にはそのような局面をどのように包含するか検討し、検査者と調整し、合意の取れた試験計画を得る必要があると思われるが、そのための手法について補足できれば望ましい。

Appendix 1　証明手順例など

Appendix 1.1　飛行中断に関する考え方の補足

4.3(2)で述べたように、第二種認証を想定する機体においては、故障などにより飛行の継続に支障が生じた場合に、飛行中断により最終的な影響を立入管理区画内に限定し、特に第三者への危害を防止することで安全を確保するような機体が存在する。このような機体について、飛行中断措置実施後、ないし故障発生後の自由落下状態、パラシュート降下状態などでは制御された飛行状態を維持しているわけではない ことから、想定飛行範囲からの逸脱は防止できていても、もう 1 つの条件である「制御不能」を防止できていないのではないかとの考え方があり得ることも 4.3(2)で述べた通りである。

4.3(2)で述べたように、関連文書[6]では本基準における「制御不能」の解釈として、「運用者によって管理されている飛行中断は制御不能の範疇に入らない」としている。また、4.3(3)で述べたように「航空局ガイドライン」の Pass/Fail criteria でも「管理された墜落」に至ることで許容されることが明示されており、「管理された墜落」の要件は「予め設計上で想定された墜落」であり、ここでは設計者の意図に言及している。

この関係を整理するため、複雑なリスク構造を図解説明できる SafeML(SysML を拡張した安全設計用の言語[1])にて解説を試みた。例えばパラシュート降下をおこなうケースについては、以下の 2 つの視点が必要であると言える。

1. (制御可能)操縦者が意図的、もしくは設計者が意図した条件下で自動的に開く場合には、「意図」された環境と考える
2. (制御不能)パラシュートで吊られた状態(風によって流される可能性がある)については、制御された飛行状態と言えない

1 と 2 の関係は、1 によって対策された後に 2 の追加リスクが発生した状態であり、安全措置に対する責任も複数のステークホルダが有する。リスク構造を図解すると図 A1.1-1 のようになる。

[1] RRI, WG3/SafeML メタモデル仕様書 Ver.2.1　公開, https://www.jmfrri.gr.jp/document/library/4662.html

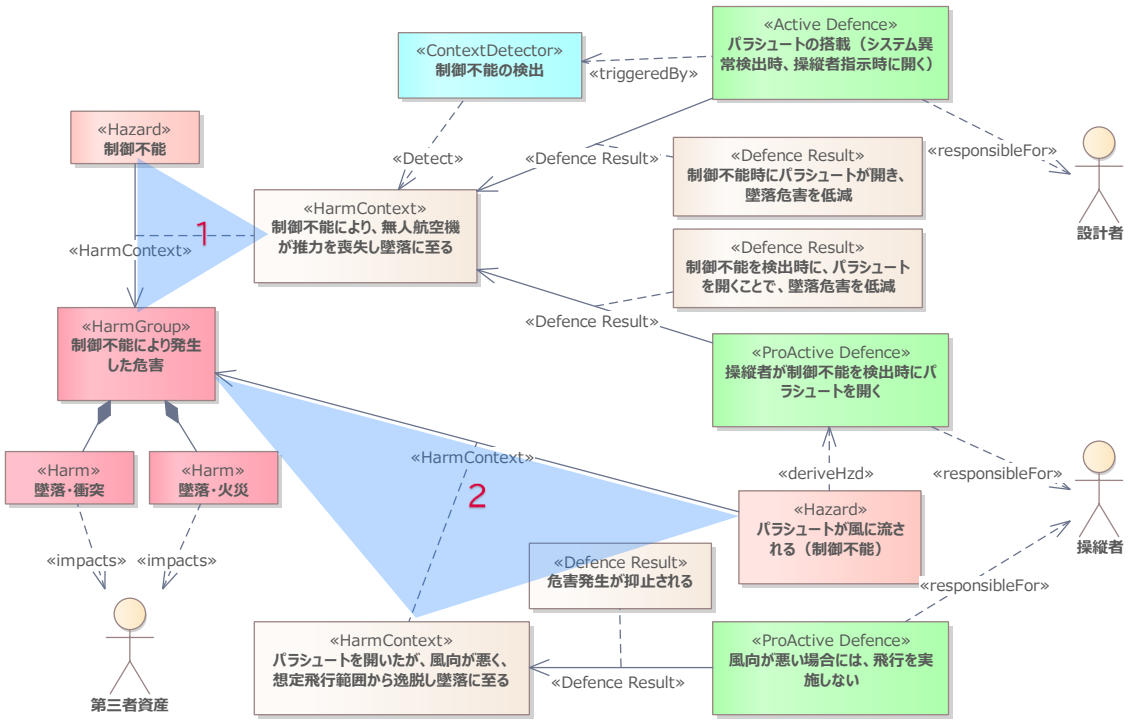


図 A1.1-1　SafeML を用いた飛行中断時のリスク構造分析

＜図 A1.1-1 説明＞

図中青枠 1、2 が前述した本文中の 1、2 と対応する。各要素には≪ステレオタイプ≫が定義されているが、意味は以下の通りである。

Hazard:	危険源
Harm:	危害
HarmContext:	リスクに至るシナリオ
～Defence:	リスクに対する方策（対策）を示す。Active/ProActive の違いは、ユーザーズガイド[2]を参照のこと。

各対策における責任分解を示すが、2 における対策「飛行を実施しない」責任は操縦者が担う。このような操縦者の対策にてカバーする項目については、製造者が正しく運用限界などの必要事項を伝達する必要があり、伝達すべき情報および実効性を十分に検討する必要がある。

以上から、セクション 305 に対応する観点から、飛行中断により安全を確保する無人航空機の認証にあたっては、申請者は

1. 無人航空機が任意の単一故障時を含む必要な状況下で確実に飛行中断ができること、または機体が飛行中断に陥ること
2. 操縦者が必要な準備、判断、操作をおこなうために必要な情報を提供すること

の 2 つについて責任を有する。

前者は、試験対象の識別に関連して、簡易 FMEA などにより検証されることが想定される。申請者は

[2] “信頼性システム モデリング言語「SafeML」ユーザーズガイド Version 2.0.” https://www.jmfrri.gr.jp/followup/3154tml

故障などの発生から飛行中断に至る時系列に留意し、例えば操縦者が飛行中断を指令するようなケースについては、判定に必要な情報伝達、操作者による判断、操作などに要する時間なども考慮して確実に動作するようシステムを構成する必要がある。

後者は、

- ICA に記載される、点検・整備のための情報
- 飛行規程に記載される限界事項、想定飛行範囲の設定方法
- 飛行規程に記載される非常時の操作方法
- 飛行中に適切に判断を行うための、地上局などに表示される情報

などが包含される。図 A1.1-2 に、実際の運用フェーズにて必要な情報の例を示す。

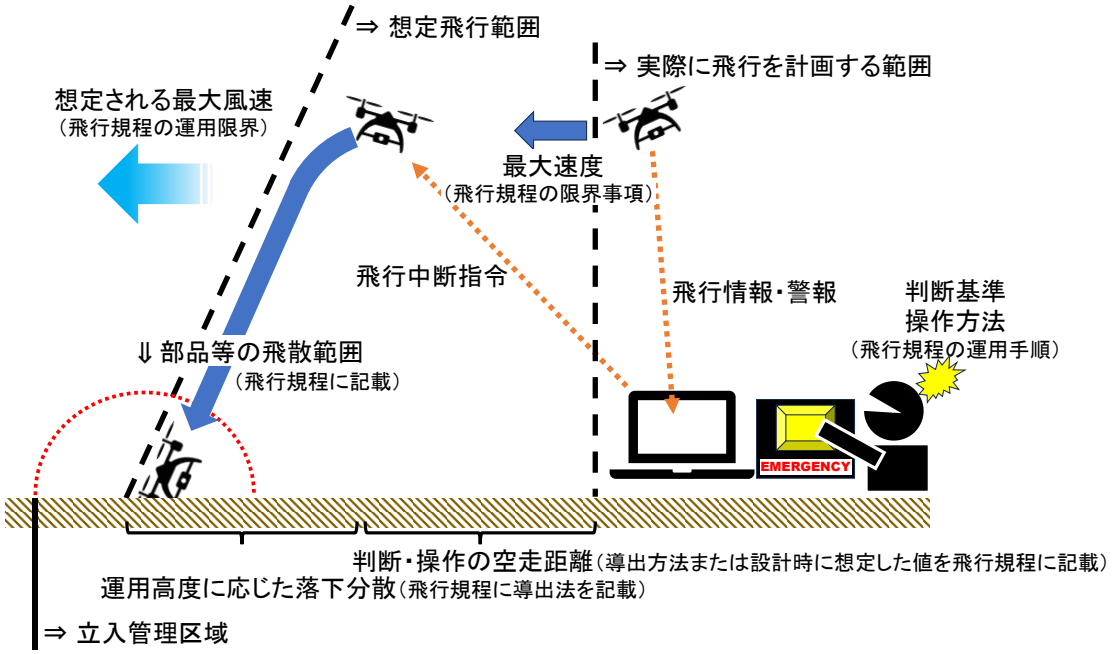


図 A1.1-2 飛行中断による安全の確保に必要な情報の例

尚、「想定飛行範囲」については「航空局ガイドライン」では定義、用語解説などには含まれていないが、

> *なお、想定飛行範囲は無人航空機がその性能によりとどまることのできる範囲として試験において証明するものであり、運航要件として設定する立入管理区画は、これに加え、飛行する高度、速度、不具合発生時の投射角度、操作時間、空気抵抗を考慮するため、一般に想定飛行範囲より広くなる。又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。*
>
> *［引用：航空局ガイドライン／セクション 305 その他参考となる情報］*

と説明されており、文字通りに読めば空走距離、落下分散などを考慮したマージンは「想定飛行範囲」には含まれないように読める。が、このように考えると飛行中断時に「想定飛行範囲からの逸脱」が発生してしまうことになり、Pass/Fail criteria と整合しないことから、空走距離、落下分散などについても「その性能」の範疇と解釈し、図 A1.1-2 のように図示した。飛行規程への記載も含め、当該用語をどのように用いるかは最終的に検査者と相談し、合意する必要がある。

Appendix 1.2 実際の立証のための試験計画例

本付録においては、4.4 項で述べた実際の立証方法について、特に「航空局ガイドライン」の MoC の項で特記された個別の対象について、マルチロータ無人航空機を例にして実際の試験方法事例を示すものである。

> *(1) 少なくともひとつの推進システム(例えばモーター)又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。この試験は厳しい飛行フェーズ、モード、最も不利な重量重心位置で行う。*
>
> *[引用:航空局ガイドライン／セクション 305 MoC]*

＜機体条件＞

第二種認証をおこなう機体で、最大離陸重量 25kg 以上を想定する(25kg 未満は立証の必要なし)。

飛行規程で示される故障発生後の対処について、以下の 2 ケースを想定する。

a) 自動制御による飛行を継続し、地上からの指令により制御された非常着陸を実施する場合(1 推進器を喪失した状態で飛行を継続できる機体でも、劣化した飛行性能でそのままミッションを継続することは考えにくいことから、本ケースを想定した。)

b) 地上からの指令により飛行中断をおこない、落着させる場合

＜実証方法＞

ケース a)

飛行中に推進器の一故障を発生させ、制御可能な飛行が継続できることを実証する。墜落を伴わないため、飛行試験により実施する。劣化した飛行性能でミッションを継続することはリスクがある(という機体を想定する)ことから、故障の検知と非常着陸指示、実際の着陸までのシークエンスを実証する。機体が極端な異常姿勢を取ることは考えにくいため、故障検知は各モーターへの指令値の変動や ESC からのステイタス情報により行われることを想定する。

試験が必要なクリティカルフェーズ(危険な状態)は 4.4(2)項を参照のこと。原則としては以下の 4 フェーズに包含されると考えられる。申請者はこの全ケースを実施する必要はないが、実施しないフェーズについては、実施するいずれかのフェーズと比較して危険度がより低いことを説明し、検査者と合意する必要がある。

① ホバリング時
② 最大上昇率での上昇時
③ 最大降下率での降下時
④ 最大速度前進時

具体的な工程は以下の通り

	目 的	方 法
1	推進器停止機能の装着	飛行中に 1 つの推進システムを停止できるシステムを追加。実証方法の具体的な案を以下に挙げる。 ● フライトコントローラからの回転指令信号線を継電器などにより遮断 ● モーターに供給される電源を遮断 ● フライトコントローラのソフトウェアにより、1 つの推進器への信号を 0(またはその他停止を意図する値)に設定する ● その他 いずれのケースについても推進器停止機能は地上からの指令により動作するもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。
2	推進器停止機能の動作確認	プロペラを外したモーターのみでアイドリングさせ、推進器停止機能が正常にコントロールできることを地上試験で確認する。
3	正常状態確認 (1 分間の離着陸・ホバリング)	推進器停止機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認する。安全な試験のためにも正常に飛行できることを実証することは重要。
4	故障模擬	機体離陸後、クリティカルフェーズで、推進器停止機能を発動させて 1 つの推進器を停止させ、機体が制御された飛行状態を維持できること、故障が検知され、地上局の表示などにより操縦者に認識されることを確認する。停止させる推進器の選定に当たり、推進器によって停止の影響が異なる可能性を考慮する必要がある。
5	着陸指示	地上局からの指令により、機体が非常着陸に移行できること、操縦者が着陸点などを指定する仕様の場合、地上局より正常に指定できることなどを確認する。フライトコントローラにより自動的に非常着陸に移行する仕様の場合は、前項にて検知に伴って発動することを確認する。
6	着陸	機体が自動制御により、想定飛行範囲内に着陸することを確認する。
7	推進器停止機能の取り外し	1 項で装着した推進器停止機能を取り外し、必要に応じて動作確認などを実施する。

ケース b)

飛行試験で実証しようとすると墜落による機体の喪失や、試験要員の危険を伴うことから、地上試験により、故障が検知できること、強制停止やパラシュート動作の発動が実施できることなどを実証する。故障の検知方法については、機体の傾き角や、各モーターの異常な指令値のばらつきなど、各機体の設計に依存するため、それらの故障検知方法が合理的であることの説明が必要である。また、操縦者が飛行中断を発動させる場合には、故障状態の伝達方法についても実証が必要である。一方、それらの検知方法が通常運用で誤動作しないことはセクション 300 で立証されるため、ここでは実証の必要はない。

試験が必要なクリティカルフェーズ(危険な状態)は 4.4(2)項を参照のこと。ただし、地上試験の為実測により落下分散を実証するわけではないこと、制御された飛行状態を維持できなくても良いことなどから限定された状況でのみ試験をおこなえば良い可能性がある。

具体的な工程は以下の通り

	目 的	方 法
1	推進器停止機能の装着	必要に応じ、飛行中に 1 つの推進システムを停止できるシステムを追加する。実証方法の具体的な例はケース a)と同様であるが、地上試験が前提となるため、直接スイッチ操作などにより動作するものも考慮される。
2	故障検知の実証	設定した故障検知方法により故障検知できるかを実証する。地上からの指示により飛行中断措置をおこなう場合は、地上局の表示により操縦者が故障を認識できることも併せて実証する。 例 1:機体の傾きにより検知する場合 地上で機体の傾きを再現し、所定の閾値で故障が検知されることを確認する。また、推進器の一故障に対して生じるケースを閾値の設定が包含していること、ないし閾値を超えない範囲では危険な状況が起こり得ないことを説明し、必要に応じてシミュレーションなどで立証する。 例 2:モーター回転数の変動により検知する場合 地上で実施する場合は、機体が姿勢制御を自律でき、ホバリング状態を継続できる装置上で、1 つの推進システムを停止させ、モーター回転数がアンバランスな状態を作り出し、故障検知動作を確認する。 モーター回転数のアンバランス状態はソフトウェア的に作り出すことも可能であるが、実際の飛行状態と同等であることを説明する必要がある。 例 3:ESC からのステイタス情報などにより検知する場合 地上で飛行を模擬して推進器を運転し、推進器停止機能を用いて 1 つの推進器を停止させて、故障が検知されることを確認する。
3	飛行中断措置の実証	地上からの指示により飛行中断措置をおこなう場合は、地上局の指示により操縦者が飛行中断措置を実施できたこと(全推進器の停止、パラシュートの放出など)を実証する。 フライトコントローラが自動的に飛行中断措置をおこなう場合は、前項の検知の実証と同時に同様の実証をおこなう。
4	墜落範囲の検証	故障検知後、飛行中断措置を実施した場合の落下分散、部品などの飛散範囲を解析により算出し、飛行規程に記載されたマージンなどを設定することで想定飛行範囲からの逸脱が発生しないことを確認する。
5	推進器停止機能の取り外し	1 項で装着した場合には、推進器停止機能を取り外し、必要に応じて動作確認などを実施する。

＜結果判定＞

Pass/Fail criteria については 4.3 項で解説した通りであるが、原則としてはいずれのケースにおいても「制御された非常着陸又は管理された墜落」に至ると考えられることから最終的に想定飛行範囲内に着陸／落着することを示せば良いと考えられる。ただし、ケース b)のように実際に落下させて落下分散を実証するわけではない場合は、別途実験、または解析により落下分散、部品などの飛散範囲を示し、飛行規程に記載されたマージンなどを設定することで想定飛行範囲からの逸脱が発生しないことを示す必要がある。落下分散の解析に当たっては一般的な高度と初速度から計算すればよいが、空気抵抗の影響は考慮する必要がある。機体の抵抗係数などを正確に導出することが困難である場合は、無視ないし概算値を取ることも想定されるが、結果が安全側(基本的には落下分散が拡大する側)となるように仮定を置くよう注意すること。

ケース a)のように飛行状態での実証を行う場合も、飛行エリア外縁でちょうど故障を起こすことが難しいこと、気象条件についても最も厳しい条件を再現することが困難であることなどを考えると、実

際に飛行エリア外縁で故障を模擬して想定飛行範囲から逸脱しないことを示すという形ではなく、故障発生個所から着陸点までの偏差を実測し、外部風の影響などを解析的に補足することで、最大の偏差を推定し、飛行規程に記載されたマージンなどを設定することで想定飛行範囲からの逸脱が発生しないことを示すことが現実的であると考えられる。

セクション 305 の Pass/Fail criteria にあっては・ 4.3 項で述べたように操縦者の意図や、設計上考慮されていることなどが重要であるため、CONOPS や飛行規程で説明されている通りに安全性が確保されている必要があり、例えば自動着陸により安全を確保する筈がそのまま墜落してしまい、しかし結果的に想定飛行範囲からは逸脱しなかったという結果が出た場合に、それが「安全基準」を満たしていると見做されることは難しい。申請者は事前に検査者とよく協議し、CONOPS や飛行規程との整合も含めて合意された Pass/Fail criteria を確立しておく必要がある。

＜注意すべき事項＞

- 推進器停止機能の実装にあたって、フライトコントローラのソフトウェアにより、1 つの推進器への信号を 0(またはその他停止を意図する値)に設定する場合、原則としてはソフトウェアの出力端で値を変更することにより、値が 0 であることがソフトウェア内で認識・利用されないように、また値がソフトウェア内のリミッタなどにより変更されたり、フィルタなどにより変更過程が平滑化されたりしないよう注意するとともに、検査者から求められた場合はそれを立証する必要がある。
- また、フライトコントローラから ESC への信号線を遮断する場合も、ESC で前値保持などの設定により回転数が 0 にならない可能性があり、必要に応じて設定変更するなどの対応が必要になることに注意すべきである。
- 飛行試験で実施する場合の飛行高度についてはクリティカルな状況を包含できるように注意する必要がある。例えば単純な落下分散であれば高度が高くなるほど広くなるが、制御された着陸をおこなう場合、故障発生時に一度水平面の位置が変動した後で降下しながら修正するような動きをする場合もあり、発生高度が低いほうがクリティカルになるようなケースもありえる。
- マルチロータ無人航空機は一般に軸対象に推進器を配置しているが、巡航中などは推進器によって出力が異なるため停止した場合の影響も異なる。また、外部風の風向、重心位置(最も不利な重心位置を設定する場合、推力中心から水平面内で推力中心から偏差した場所に重心が設定される可能性は高い)などによっても、推進器によって停止した場合の影響は異なると考えられる。特に飛行中に 1 推進器を停止させる場合、これらの要素を総合的に勘案し、最も悪影響の大きい推進器を停止させる必要がある。
- 固定翼型(ないし VTOL 型の固定翼モード)においては、滑空する能力を有することから推進システムが故障しても直ちに墜落しない可能性が高く、結果的に想定範囲外に容易に逸脱することが想定される。そのため、マルチロータ無人航空機以上に、機体の故障状態の伝達、飛行中断の確実性などについて、十分な検討が必要である。

(2)　C2 リンクの品質低下(可用性の低下、サービス品質の悪化、信号雑音比(Signal-Noise Ratio: S/N)の低下、断続接続及び遅延など)を実証する。この試験は厳しい飛行フェーズ、モードで行う。

[引用:航空局ガイドライン／セクション 305 MoC]

＜機体条件＞

第二種認証をおこなう機体で、最大離陸重量 25kg 以上または目視外飛行を実施する機体を想定する(25kg 未満かつ目視外飛行を実施しない機体は立証の必要なし)。

C2 リンクについては操縦方式により影響が大きく異なるため、以下の 2 ケースを想定する。

a) 手動操縦による飛行を行う場合

b) 自動制御による飛行を行う場合

飛行フェーズに応じて操縦方式が異なる機体の場合は、それぞれのフェーズについて必要なケースの実証を実施する。また、手動操縦用、自動操縦のために異なる C2 リンクを有する無人航空機システムの場合は、それぞれの C2 リンクについて対応するケースの実証が必要となる。

＜実証方法＞

ケース a)

飛行中に C2 リンクの可用性の低下、サービス品質の悪化、信号雑音比(Signal-Noise Ratio: S/N)の低下、断続接続および遅延などの、強度ならびに品質の低下を発生させ、

- 飛行を通じて通信信号の強度ならびに品質が計測・表示・記録されること
- 強度または品質が、手動操縦が可能であると規定された閾値を下回らない範囲にて、手動操縦による操縦が問題なく実施でき、必要な飛行位置の制御が確保できること
- 強度または品質が規定された閾値を下回った際に、必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと

などを実証する。操縦性などの評価を含むため飛行試験により実施する必要がある。強度または品質が、手動操縦が可能であると規定された閾値を下回る際には、墜落による機体の喪失や、試験要員の危険を伴うことから、そのような局面については別途地上試験で立証することも考えられるが、例えば自動的に自動制御飛行に移行するような場合は、飛行状態を維持して遷移できることの確認などのため、飛行試験により実施することが望ましい。

試験が必要なクリティカルフェーズ(危険な状態)は 4.4(2)項を参照のこと。C2 リンクによるデータが直接飛行誘導制御に影響を与えるケースは少ないため、クリティカルフェーズを規定する必要がないケースもありえる。一方で、強度または品質が規定された閾値を下回った際に飛行モードが自動で変化するような場合は、そのような遷移が危険な飛行状態に至らずに実施できることを確認する観点から、クリティカルフェーズを考慮する必要が生じる場合もある。原則としては以下の 3 フェーズに包含されると考えられ、申請者はこの全ケースを実施する必要はないが、実施しないフェーズについては、実施するいずれかのフェーズと比較して危険度がより低いことを説明し、検査者と合意する必要があ

る。

① 最大上昇率での上昇時

② 最大降下率での降下時

③ 最大速度前進時

具体的な工程は以下の通り

	目 的	方 法
1	C2 品質低減機能の装着	C2 システムの品質・強度を低下させるシステムを追加する。実証方法の具体的な案を以下に挙げる。 ● C2 の伝送経路にアッテネータ機構を挿入するもの ● フライトコントローラなどのソフトウェアにより、C2 の品質低下を模擬するもの ● その他 アッテネータ機構については、地上からの指令により(または地上で)変化させるもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。また、定常的に一定量低下させた上で、機体と地上局の離隔により閾値を下回るような品質・強度の低下を実現することも考えられる。
2	正常状態確認 (1 分間の離着陸・ホバリング)	C2 品質低減機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認するとともに、信号の強度ならびに品質が計測・表示されることを確認する。
3	C2 品質低下模擬	機体離陸後、クリティカルフェーズで、C2 品質低減機能を発動させ、ないし機体を地上局から離隔することで C2 の品質・強度を低下させ ● 強度または品質が、手動操縦が可能であると規定された閾値を下回らない範囲にて、手動操縦による操縦が問題なく実施でき、必要な飛行位置の制御が確保できること ● 強度または品質が規定された閾値を下回った際に、必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと などを確認する。
4	自動帰還、着陸	自動帰還、着陸などが自動で起動する機体の場合は、それらの過程が適切に実施されることを確認する。
5	着陸	機体を回収し、試験を終了する。
6	C2 品質低減機能の取り外し	1 項で装着した場合は、C2 品質低減機能を取り外し、必要に応じて動作確認などを実施する。

ケース b)

飛行中に C2 リンクの可用性の低下、サービス品質の悪化、信号雑音比(Signal-Noise Ratio: S/N)の低下、断続接続および遅延などの、強度ならびに品質の低下を発生させ、

- 飛行を通じて通信信号の強度ならびに品質が計測・表示・記録されること
- 強度または品質が規定された閾値を下回った際に、必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと

などを実証する。

必ずしも墜落による機体の喪失や、試験要員の危険などの安全上の問題があるわけではないが、C2 低下状況でも自動制御の機能に大きな違いがないこと、飛行モードなどの遷移過程においても手動操縦からの移行ほどには制御系へのインパクトがないと思われることなどから、地上試験でも立証

できる可能性がある。ただし、一定以上の品質・強度の低下により自動帰還などに移行する過程を立証する場合は、飛行試験による実証が推奨される。

具体的な工程は以下の通り

	目 的	方 法
1	C2 品質低減機能の装着	C2 システムの品質・強度を低下させるシステムを追加する。実証方法の具体的な案を以下に挙げる。 ● C2 の伝送経路にアッテネータ機構を挿入するもの ● フライトコントローラなどのソフトウェアにより、C2 の品質低下を模擬するもの ● その他 アッテネータ機構については、地上からの指令により(または地上で)変化させるもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。また、定常的に一定量低下させた上で、機体と地上局の離隔により閾値を下回るような品質・強度の低下を実現すること、地上試験においては無線通信の減衰を可能とするシールドテントやカバーなどを利用することなども考えられる。
2	正常状態確認 (1 分間の離着陸・ホバリング)	飛行を行う場合は、C2 品質低減機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認するとともに、信号の強度ならびに品質が計測・表示されることを確認する。
3	C2 品質低下模擬	機体離陸後、クリティカルフェーズで、(または地上にて)C2 品質低減機能を発動させ、ないし機体を地上局から離隔することで C2 の品質・強度を低下させ ● 強度または品質が規定された閾値を下回った際に、必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと などを確認する。
4	自動帰還、着陸	自動帰還、着陸などが自動で起動する機体の場合は、それらの過程が適切に実施されることを確認する。
5	着陸	機体を回収し、試験を終了する。
6	C2 品質低減機能の取り外し	1 項で装着した場合は、C2 品質低減機能を取り外し、必要に応じて動作確認などを実施する。

＜結果判定＞

Pass/Fail criteria については 4.3 項で解説した通りであり、原則としてはいずれのケースにおいても、最終的に飛行を継続して帰還回収できること、または想定飛行範囲内に着陸／落着することで「制御された非常着陸又は管理された墜落」に至ることを示せば良いと考えられる。

セクション 305 の Pass/Fail criteria にあっては 4.3 項で述べたように操縦者の意図や、設計上考慮されていることなどが重要であるため、CONOPS や飛行規程で説明されている通りに安全性が確保されている必要があり、結果的に想定飛行範囲からは逸脱しなかったかどうかだけではなく、想定された通りにシステムが動作したかを検証することが重要となると考えられる。例えば、飛行を通じて通信信号の強度ならびに品質が計測・表示・記録されること、強度または品質が規定された閾値を下回った際に、必要な警報などが表示されることについても評価の対象となりうると考えられる。(本来はセクション 100、セクション 105 に係る事項であるが、セクション 305 の試験においても正常に機能している必要はあるという考えである。)

申請者は事前に検査者とよく協議し、CONOPS や飛行規程との整合も含めて合意された

Pass/Fail criteria を確立しておく必要がある。

＜注意すべき事項＞

- C2 機能を意図的に低下させた機体を飛行させること、特に長距離進出させることは運用上のリスクを伴う。申請者は当該試験に特化したリスクについて十分検討し、安全を確保する必要がある。例えば C2 リンクの品質低下機能をなるべく地上局側に置く、複数の地上局または操縦装置を持つ無人航空機の場合は、C2 リンクの品質低下を模擬する地上局のほうを移動するなどの工夫が考えられる。
- 品質低下に伴って手動操縦から自動操縦に移行する場合、自動操縦でもモードが切り替わる場合などにおいて、C2 リンクの品質・強度が閾値付近で上下した場合、機体の挙動と連成した場合などに短時間で頻繁に切り替えが起きる、所謂チャタリングが起きる場合がある。特に機体の挙動と連成したチャタリングは地上試験では模擬できない場合がある。申請者は試験においては意図的にチャタリングが発生しやすい状況を形成する、またはチャタリングを防止する機能などについて検査者に説明し、合意を得るなどして、クリティカルな状況が検証されないリスクを回避する必要がある。
- 複数の C2 リンクを切り替えて連接を維持する機体においても、一方の品質低下に伴って自動的に C2 リンクを切り替える際に問題が発生するケース（例えばあるリンクからより遅延の大きいリンクに切り替えた際に地上からのコマンドを 2 重に受信するようなケースなど）がある。このような無人航空機システムについても、申請者は C2 機器の構成、切り替えやコマンド受信のアルゴリズムなどについて検査者に説明し、合意を得るなどして、クリティカルな状況が検証されないリスクを回避する必要がある。
- 品質・強度が一定の閾値を下回った場合に自動帰還、または回復のための機動（上昇など）を行う機体の場合、そのために自動生成する飛行経路が想定飛行範囲からの逸脱などのリスクを生じる場合がある。これらは特定の飛行試験で偶々機能したというだけではその安全性を立証することは難しいため、申請者はそのような機能の実装について検査者に説明し、その特定の状況に依らない安全性について了解を得る必要がある。
- 特に手動操縦により飛行する固定翼型（ないし VTOL 型の固定翼モード）無人航空機においては、滑空する能力を有することから C2 リンクが故障しても直ちに墜落しない可能性が高く、結果的に想定範囲外に容易に逸脱するリスクがある。そのため、マルチロータ無人航空機以上に、機体の故障状態の伝達、飛行中断の確実性などについて、十分な検討が必要である。

（3） C2 リンクが完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う。

［引用：航空局ガイドライン／セクション 305 MoC］

＜機体条件＞

第二種認証をおこなう機体で、最大離陸重量 25kg 以上または目視外飛行を実施する機体を想定する（25kg 未満かつ目視外飛行を実施しない機体は立証の必要なし）。

＜実証方法＞

飛行中に C2 リンクの喪失を発生させ、

- 喪失時に、必要な警報などが表示されること
- 安全上必要な措置が適切に起動し、飛行に悪影響を与えないこと

などを実証する。

必ずしも墜落による機体の喪失や、試験要員の危険などの安全上の問題があるわけではないが、C2 喪失時でも自動制御の機能に大きな違いがない場合、自動制御での飛行など、飛行モードなどの遷移過程において制御系へのインパクトがないと思われること場合などは、地上試験でも立証できる可能性がある。ただし、喪失により自動帰還などに移行する過程を立証する場合は、飛行試験による実証が推奨される。

試験が必要なクリティカルフェーズ(危険な状態)は・ 4.4(2)項を参照のこと。C2 リンクによるデータが直接飛行誘導制御に影響を与えるケースは少ないため、クリティカルフェーズを規定する必要がないケースもありえる。一方で、強度または品質が規定された閾値を下回った際に飛行モードが自動で変化するような場合は、そのような遷移が危険な飛行状態に至らずに実施できることを確認する観点から、クリティカルフェーズを考慮する必要が生じる場合もある。原則としては以下の 3 フェーズに包含されると考えられ、申請者はこの全ケースを実施する必要はないが、実施しないフェーズについては、実施するいずれかのフェーズと比較して危険度がより低いことを説明し、検査者と合意する必要がある。

① 最大上昇率での上昇時
② 最大降下率での降下時
③ 最大速度前進時

具体的な工程は以下の通り

	目 的	方 法
1	C2 遮断機能の装着	C2 リンクを喪失させるシステムを追加する。実証方法の具体的な案を以下に挙げる。 ● C2 の伝送経路にアッテネータ機構、遮断機構を挿入するもの ● フライトコントローラなどのソフトウェアにより、C2 の遮断を模擬するもの ● その他 遮断機構については、地上からの指令により変化させるもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。また、定常的に一定量低下させた上で、機体と地上局の離隔により閾値を下回るような品質・強度の低下を実現することも考えられる。 とは言え、単純な遮断の模擬であれば、地上でアンテナを遮蔽ないし抜線するような方式も可能である。
2	正常状態確認 (1 分間の離着陸・ホバリング)	C2 遮断機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認するとともに、信号の強度ならびに品質が計測・表示されることを確認する。
3	C2 遮断模擬	機体離陸後、クリティカルフェーズで、C2 遮断機能を発動させ、 ● 必要な警報などが表示されること、安全上必要な措置が適切に

	目 的	方 法
		起動し、飛行に悪影響を与えないこと などを確認する。
4	自動帰還、着陸	自動帰還、着陸などが自動で起動する機体の場合は、それらの過程が適切に実施されることを確認する。
5	着陸	機体を回収し、試験を終了する。
6	C2 遮断機能の取り外し	1 項で装着した場合は、C2 遮断機能を取り外し、必要に応じて動作確認などを実施する。

＜結果判定＞

Pass/Fail criteria については 4.3 項で解説した通りであり、原則としては最終的に飛行を継続して帰還回収できること、または想定飛行範囲内に着陸／落着することを示せば良いと考えられる。

セクション 305 の Pass/Fail criteria にあっては・ 4.3 項で述べたように操縦者の意図や、設計上考慮されていることなどが重要であるため、CONOPS や飛行規程で説明されている通りに安全性が確保されている必要があり、結果的に想定飛行範囲からは逸脱しなかったかどうかだけではなく、想定された通りにシステムが動作したかを検証することが重要となると考えられる。申請者は事前に検査者とよく協議し、CONOPS や飛行規程との整合も含めて合意された Pass/Fail criteria を確立しておく必要がある。

＜注意すべき事項＞

- C2 機能を遮断した状態で機体を飛行させること、特に長距離を自動帰還させることは運用上のリスクを伴う。申請者は当該試験に特化したリスクについて十分検討し、安全を確保する必要がある。
- 複数の C2 リンクを切り替えて連接を維持する機体においては、一方の喪失に伴って自動的に C2 リンクを切り替える際に問題が発生するケース（例えばあるリンクからより遅延の大きいリンクに切り替えた際に地上からのコマンドを 2 重に受信するようなケースなど）がある。このような無人航空機システムについても、申請者は C2 機器の構成、切り替えやコマンド受信のアルゴリズムなどについて検査者に説明し、合意を得るなどして、クリティカルな状況が検証されないリスクを回避する必要がある。
- C2 リンク喪失時に自動帰還、またはリンク回復のための機動（上昇など）を行う機体の場合、そのために自動生成する飛行経路が想定飛行範囲からの逸脱などのリスクを生じる場合がある。これらは特定の飛行試験で偶々機能したというだけではその安全性を立証することは難しいため、申請者はそのような機能の実装について検査者に説明し、その特定の状況に依らない安全性について了解を得る必要がある。勿論、実際の飛行試験においても想定飛行範囲からの逸脱などのリスクを生じないように計画することが必要である。

（4） GNSS の品質低下を実証する。この試験は厳しい飛行フェーズ、モードで行う。

［引用：航空局ガイドライン／セクション 305 MoC］

＜機体条件＞

第二種認証をおこなう機体で、最大離陸重量 25kg 以上または目視外飛行を実施する機体を想定する（25kg 未満かつ目視外飛行を実施しない機体は立証の必要なし）。

＜実証方法＞

飛行中に GNSS 信号の可用性の低下、サービス品質の悪化、信号雑音比（Signal-Noise Ratio: S/N）の低下、断続接続および遅延などの、強度ならびに品質の低下を発生させ、

- 飛行を通じて GNSS 信号の強度ならびに品質が計測・表示・記録されること
- 強度または品質が、その時点での飛行方式による飛行の継続がが可能であると規定された閾値を下回らない範囲にて、飛行が問題なく継続でき、必要な飛行位置の制御が確保できること
- 強度または品質が規定された閾値を下回った際に、必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと

などを実証する。飛行性、操縦性などの評価を含むため飛行試験により実施する必要がある。強度または品質が、飛行の継続が可能であると規定された閾値を下回る際には、墜落による機体の喪失や、試験要員の危険を伴うことから、そのような局面については別途地上試験で立証することも考えられるが、例えば自動的に制御モードや自動制御に用いる情報源を変更するような場合は、飛行状態を維持して遷移できることの確認などのため、飛行試験により実施することが望ましい。

試験が必要なクリティカルフェーズ（危険な状態）は 4.4（2）項を参照のこと。原則としては以下の 4 フェーズに包含されると考えられる。申請者はこの全ケースを実施する必要はないが、実施しないフェーズについては、実施するいずれかのフェーズと比較して危険度がより低いことを説明し、検査者と合意する必要がある。

④ ホバリング時
⑤ 最大上昇率での上昇時
⑥ 最大降下率での降下時
⑦ 最大速度前進時

具体的な工程は以下の通り

	目 的	方 法
1	GNSS 品質低減機能の装着	GNSS システムの品質・強度を低下させるシステムを追加する。実証方法の具体的な案を以下に挙げる。 ● GNSS アンテナ下流の伝送経路にアッテネータ機構を挿入するもの ● フライトコントローラなどのソフトウェアにより、GNSS の品質低下を模擬するもの ● その他 アッテネータ機構については、地上からの指令により（または地上で）変化させるもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。
2	正常状態確認 （1 分間の離着陸・ホバリ	GNSS 品質低減機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認すると

	目 的	方 法
	ング）	ともに、信号の強度ならびに品質が計測・表示されることを確認する。
3	GNSS 品質低下模擬	機体離陸後、クリティカルフェーズで、GNSS 品質低減機能を発動させ、 ● 強度または品質が、その時点での飛行方式が可能であると規定された閾値を下回らない範囲にて、飛行が問題なく継続でき、必要な飛行位置の制御が確保できること ● 強度または品質が規定された閾値を下回った際に、必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと などを確認する。
4	自動帰還、着陸	自動着陸などが自動で起動する機体の場合は、それらの過程が適切に実施されることを確認する。
5	着陸	機体を回収し、試験を終了する。
6	GNSS 品質低減機能の取り外し	1 項で装着した場合は、GNSS 品質低下機能を取り外し、必要に応じて動作確認などを実施する。

＜結果判定＞

Pass/Fail criteria については 4.3 項で解説した通りであり、原則としてはいずれのケースにおいても、最終的に飛行を継続して帰還回収できること、または想定飛行範囲内に着陸／落着することで「制御された非常着陸又は管理された墜落」に至ることを示せば良いと考えられる。

セクション 305 の Pass/Fail criteria にあっては・ 4.3 項で述べたように操縦者の意図や、設計上考慮されていることなどが重要であるため、CONOPS や飛行規程で説明されている通りに安全性が確保されている必要があり、結果的に想定飛行範囲からは逸脱しなかったかどうかだけではなく、想定された通りにシステムが動作したかを検証することが重要となると考えられる。例えば、飛行を通じて GNSS 信号の強度ならびに品質が計測・表示・記録されること、強度または品質が規定された閾値を下回った際に、必要な警報などが表示されることについても評価の対象となりうると考えられる。申請者は事前に検査者とよく協議し、CONOPS や飛行規程との整合も含めて合意された Pass/Fail criteria を確立しておく必要がある。

＜注意すべき事項＞

- 特に GNSS 機能を意図的に低下させた機体を飛行させること、特に長距離進出させることは運用上のリスクを伴う。申請者は当該試験に特化したリスクについて十分検討し、安全を確保する必要がある。
- 品質低下に伴って手動操縦から自動操縦に移行する場合、自動操縦でもモードが切り替わる場合などにおいて、GNSS 信号の品質・強度が閾値付近で上下した場合、機体の挙動と連成した場合などに短時間で頻繁に切り替えが起きる、所謂チャタリングが起きる場合がある。特に機体の挙動と連成したチャタリングは地上試験では模擬できない場合がある。申請者は試験においては意図的にチャタリングが発生しやすい状況を形成する、またはチャタリングを防止する機能などについて検査者に説明し、合意を得るなどして、クリティカルな状況が検証されないリスクを回避する必要がある。
- 品質・強度が一定の閾値を下回った場合に自動着陸、または回復のための機動（上昇など）を

行う機体の場合、そのために自動生成する飛行経路が想定飛行範囲からの逸脱などのリスクを生じる場合がある。これらは特定の飛行試験で偶々機能したというだけではその安全性を立証することは難しいため、申請者はそのような機能の実装について検査者に説明し、その特定の状況に依らない安全性について了解を得る必要がある。

- 品質低減機能の実装にあたって、フライトコントローラのソフトウェアにより、GNSS による位置情報を異常値に設定する場合、原則としてはセンサからの情報入力端で値を変更することにより、異常値の影響がソフトウェア全体に及ぶよう注意するとともに、検査者から求められた場合はそれを立証する必要がある。また(市販、自作を問わず)複合航法装置を使用する場合は、GNSS の測位結果が複合航法演算を通じて、位置情報だけでなく、一般には IMU の出力と見做されるデータ(姿勢角、角速度、加速度など)に影響する場合があるため、どの項目にどのような異常値を設定すれば良いかにも注意し、試験に先立って検査者と合意する必要がある。
- 品質低下中の GNSS による位置情報はいわば審査対象であるため立証手段として使用することはできないが、一方で飛行中の無人航空機の位置を地上から高精度で検出することは困難である。申請者は、品質低下中の GNSS による位置情報の妥当性を検証する手段として
  - 本来搭載する GNSS と別系統の、品質低減機能の影響を受けない GNSS システムの搭載
  - GNSS の品質低下の影響を受けない IMU のデータなどを使用した総合的な評価

  などを検討し、試験に先立って検査者と合意する必要がある。
- 本項では主に GNSS 信号の強度低下を想定して記述しているが、場合によっては GNSS 信号の汚染(例えば狭隘空間におけるマルチパスの受信、地上付近で、周辺で使用されていた GPS リピータによる汚染などの事例がある)を考慮する必要もある。申請者は CONOPS に基づいてどのような品質低下を模擬すべきか検討し、試験に先立って検査者と合意する必要がある。また、GNSS 信号の強度低下や汚染だけでなく、航法装置そのものの故障[3]を想定する場合、例えば複合航法装置全体の故障による IMU データも含めた異常、機器間の通信不良による影響など GNSS 信号によるものとは別の影響が発生する可能性があることに注意が必要である。

(5)　GNSS が完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う。 *[引用:航空局ガイドライン／セクション 305　MoC]*

＜機体条件＞

第二種認証をおこなう機体で、最大離陸重量 25kg 以上または目視外飛行を実施する機体を想定する(25kg 未満かつ目視外飛行を実施しない機体は立証の必要なし)。

[3] これがセクション 305(a)項(3)全球測位衛星システム(GNSS)の単一故障に該当するかどうかは議論の余地があると思われるが、いずれにせよ装置自体に単一故障点があれば考慮しなければならない事象ではあると考えられる。

＜実証方法＞

飛行中に GNSS 信号または GNSS による測位機能の喪失を発生させ、

- 必要な警報などが表示されること、安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと

などを実証する。墜落による機体の喪失や、試験要員の危険を伴うことから、地上試験で立証することも考えられるが、例えば自動的に制御モードや自動制御に用いる情報源を変更するなどして自動着陸などの自動飛行の継続を実施するような場合は、飛行状態を維持して遷移し、非常措置が完遂できることの確認などのため、飛行試験により実施することが望ましい。

試験が必要なクリティカルフェーズ(危険な状態)は 4.4(2)項を参照のこと。原則としては以下の 4 フェーズに包含されると考えられる。申請者はこの全ケースを実施する必要はないが、実施しないフェーズについては、実施するいずれかのフェーズと比較して危険度がより低いことを説明し、検査者と合意する必要がある。

① ホバリング時
② 最大上昇率での上昇時
③ 最大降下率での降下時
④ 最大速度前進時

具体的な工程は以下の通り

	目 的	方 法
1	GNSS 遮断機能の装着	GNSS システムを遮断するシステムを追加する。実証方法の具体的な案を以下に挙げる。 ● GNSS アンテナ下流の伝送経路に信号遮断機構を挿入するもの ● フライトコントローラなどのソフトウェアにより、GNSS の喪失を模擬するもの ● その他 遮断機構については、地上からの指令により(または地上で)変化させるもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。
2	正常状態確認 (1 分間の離着陸・ホバリング)	GNSS 遮断機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認するとともに、信号の強度ならびに品質が計測・表示されることを確認する。
3	GNSS 品質低下模擬	機体離陸後、クリティカルフェーズで、GNSS 遮断機能を発動させ、 ● 必要な警報などが表示されること、 ● 安全上必要な措置が自動的に実施される場合は、適切に起動し、飛行に悪影響を与えないこと などを確認する。
4	自動帰還、着陸	自動着陸などが自動で起動する機体の場合は、それらの過程が適切に実施されることを確認する。
5	着陸	機体を回収し、試験を終了する。
6	GNSS 遮断機能の取り外し	1 項で装着した場合は、GNSS 遮断機能を取り外し、必要に応じて動作確認などを実施する。

＜結果判定＞

Pass/Fail criteria については 4.3 項で解説した通りであり、原則としては、最終的に飛行を継続して帰還回収できること、または想定飛行範囲内に着陸／落着することで「制御された非常着陸又は管理された墜落」に至ることを示せば良いと考えられる。

セクション 305 の Pass/Fail criteria にあっては 4.3 項で述べたように操縦者の意図や、設計上考慮されていることなどが重要であるため、CONOPS や飛行規程で説明されている通りに安全性が確保されている必要があり、結果的に想定飛行範囲からは逸脱しなかったかどうかだけではなく、想定された通りにシステムが動作したかを検証することが重要となると考えられる。例えば GNSS データを参照しない自動着陸により安全を確保する筈がそのまま墜落してしまい、しかし結果的に想定飛行範囲からは逸脱しなかったという結果が出た場合に、それが「安全基準」を満たしていると見做されることは難しい。また、飛行を通じて GNSS 機能を喪失した際に必要な警報などが表示されることなどについても評価の対象となりうると考えられる。申請者は事前に検査者とよく協議し、CONOPS や飛行規程との整合も含めて合意された Pass/Fail criteria を確立しておく必要がある。

＜注意すべき事項＞

- GNSS 機能を遮断することは運用上のリスクを伴う。申請者は当該試験に特化したリスクについて十分検討し、安全を確保する必要がある。
- 遮断機能の実装にあたって、フライトコントローラのソフトウェアにより、GNSS による位置情報を 0 値（または相当する異常値）に設定する場合、原則としてはセンサからの情報入力端で値を変更することにより、異常値の影響がソフトウェア全体に及ぶよう注意するとともに、検査者から求められた場合はそれを立証する必要がある。また（市販、自作を問わず）複合航法装置を使用する場合は、GNSS の測位結果が複合航法演算を通じて、位置情報だけでなく、一般には IMU の出力と見做されるデータ（姿勢角、角速度、加速度など）に影響する場合があるため、どの項目にどのような異常値を設定すれば良いかにも注意し、検査者と合意する必要がある。
- 本項では主に GNSS 信号の強度低下などによる喪失を想定して記述しているが、場合によっては航法装置やそこからの伝送経路の故障が想定される場合もある、そのような場合、例えば複合航法装置全体の故障による IMU データも含めた異常、機器間の通信不良による影響など GNSS 信号によるものとは別の影響が発生する可能性があることに注意が必要である。

Appendix 2 各セクション特有の用語集

#	用 語	意 味	備 考
1	EASA	欧州航空安全機関（European Union Aviation Safety Agency）	
2	ESC	Electric Speed Controller	
3	FAA	米国連邦航空局（Federal Aviation Administration）	
4	GNSS	全地球航法衛星システム（Global Navigation Satellite System）	
5	制御された飛行状態	ここでは、操縦者の意図通りに飛行させられる状態の意味で用いる。	「航空局ガイドライン」の定義では“制御不能”は「無人航空機の制御された飛行状態からの意図しない逸脱」とされるため、“制御された飛行状態”は必ずしも“制御不能”の補集合ではないことに注意が必要である。
6	非常着陸	安全の確保のために実施する、通常以外の着陸	
7	フェイラーモード	ここでは、故障の結果の様相の意で用いる。	類似の用語として「故障モード」があるが、此方は「航空局ガイドライン」にて「故障がどのような状態で発生するかをまとめたもの。例えば、部品やコンポーネントの断線、短絡、折損、摩耗、特性の劣化などの構造の破壊など」と解説しており、推定故障原因的なものと考えられるため、故障状態（現象）としては此方の用語を用いた。
8	フライトコントローラ	無人航空機の機体全体の制御統括および飛行制御を担う装置。また、フライトログの保存および地上局とのデータのやりとりも行い、ジャイロおよび加速度の IMU も定義上、フライトコントローラに含む場合がある。	出典：JIS W 0141:2019

Appendix 3 関連文書

(1) FAA Advisory Circular No.23 .1309-lE: SYSTEM SAFETY ANALYSIS AND ASSESSMENT FOR PART 23 AIRPLANES
https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_23_1309-1E.pdf

(2) FAA Advisory Circular No.25 .1309-lA: SYSTEM DESIGN AND ANALYSIS
https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1309-1A.pdf

(3) JARUS AMC RPAS 1309-01
http://jarus-rpas.org/wp-content/uploads/2023/07/jar_04_doc_amc_rpas_1309_issue_2_2.pdf

(4) IEC61508-1:2010(JIS C0508-1:2012) - Functional safety of electrical / electronic / programmable electronic safety-related systems : Part 1 General requirements

(5) IEC61508-5:2010(JIS C0508-5:2019) - Functional safety of electrical / electronic / programmable electronic safety-related systems : Part 5 Examples of methods for the determination of safety integrity levels

(6) 無人航空機の型式認証等の取得のためのガイドライン安全基準セクション 135 重要な部品(フライトエッセンシャルパーツ)解説書(RMD-135、Rev.01)

(7) G. Cooper and R. Harper. The use of pilot rating in the evaluation of aircraft handling qualities. Technical Report TN D-5153, NASA (1969)

(8) 無人航空機の型式認証等の取得のためのガイドライン解説書(RMD Rev.01)2.2.1 安全基準の各セクションにおける「安全」等の用語の解釈

(9) JIS W 0711:2021 無人航空機システム設計管理基準

Appendix 4　サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 305 起こり得る故障の構成員名簿（サブ WG 主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD Rev.01）Appendix4 を参照すること。

役割	氏名	所属
主査	河野 敬	国立研究開発法人宇宙航空研究開発機構
ライター	下地 広泰	大分県産業科学技術センター
ライター	三輪 昌史	国立大学法人徳島大学
ライター	三好 崇生	サイバネット MBSE 株式会社
ライター	幸 嘉平太	大分県産業科学技術センター

無人航空機の型式認証等の取得のためのガイドライン解説書

2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。