<技術情報検討会資料>
技術情報検討会は、新知見のふるい分けや作業担当課の特定を目的とした事務的な会議体であり、その資料及び議事録は原子力規制委員会の判断を示すものではありません。

資料56-2-3-2

「ボーイング 737 墜落：NRC のデジタル計装制御評価プロセスに向けた教訓」のサマリー（案）

令和 4 年 11 月 24 日
技術基盤課

第 43 回技術情報検討会（令和 2 年 10 月 29 日）において、RIS2016-05[1]に記載された原子力施設におけるデジタル計装制御（デジタル I&C）に対する米国 NRC の規制基盤近代化活動を継続注視することとなった。当該近代化活動では、2018 年と 2019 年のボーイング 737 MAX 8 の墜落事故に係る当局の調査報告書を体系的に評価している[2]。以下は、2022 年 9 月 22 日に NRC から発行された「ボーイング 737 墜落：NRC のデジタル計装制御評価プロセスに向けた教訓」[3]のサマリーである。

着目点

2017 年、米国連邦航空局（FAA）は、ボーイング 737 の設計変更（MAX 8 と呼ぶ）を認証した。これには、飛行機の空気力学設計に関連する潜在的な失速状態を阻止するための新しい自動操縦特性向上システム（MCAS）が含まれていた。2018 年 10 月と 2019 年 3 月、MCAS の繰り返し作動のため、2 機の MAX 8 航空機が墜落した。複数の当局による調査報告により、墜落につながった MCAS の開発、審査、実装、訓練及び監視に関連する一連の不良が特定された。

NRC は、原子力発電所（NPP）にデジタル I&C 技術を安全に導入することに責任がある。MCAS の設計プロセスと FAA 認証プロセスに関する調査報告書には、NRC のデジタル I&C 規制プロセスに適用可能な教訓が含まれている可能性がある。デジタル I&C 規制プロセスに適用する目的で、NRC の人間工学（HFE）及びリスク分析スタッフと連携した I&C スタッフ（以降、チームと呼ぶ）は、前記調査報告書の結果と推奨事項を体系的に評価した。なお、この評価では、航空と原子力業界の間の違い、例えば、業界の規模、設計と安全目標、規制の枠組みを考慮した。

チームが焦点を当てたのは、①デジタル I&C の許認可と検査における潜在的な規制上のギャップ（プロセスや文化を含む）の特定と、②NPP におけるデジタル I&C の安全使用をサポートするために維持または改善すべき NRC の規制監督及び組織能力の要素の特定である。レビュー目的は、①NPP のアーキテクチャに新しいデジタル I&C 技術を導入するために使用されるプロセスと、②新型炉用に高度に統合された I&C システムの開発を評価することである。

---

1 安全関連システムに組込まれたデジタル装置〈Embedded Digital Devices in Safety-Related Systems〉, 2016, ML15118A015

2 例：第 54 回技術情報検討会（令和 4 年 7 月 28 日）、【資料 54-2-3-2】NRC 報告「ボーイング 737 MAX 8 事故から得た DIC 規制課題に関する予備的考察」（案）、添付

3 BOEING 737 CRASHES: LESSONS LEARNED FOR NRC DIGITAL INSTRUMENTATION AND CONTROLS EVALUATION PROCESS, 2022-09-22, ML22241A039。付録参照。

わかったこと

墜落は、MCAS 導入おいて重大な欠陥をもたらしたいくつかのエンジニアリング、プログラム及び安全文化の不良の結果であった。しかし、NPP のデジタル制御・保護システムと航空電子工学システムの間で、安全機能、故障影響、深層防護及びリスクを掘り下げて技術比較することは困難であった。

さらに、デジタル I&C の許認可と検査に関する NRC の規制基盤に有意なギャップが存在しないことも判明した。しかし、調査結果に基づいて、NPP において発展し続けるデジタル I&C 技術の安全使用を維持または改善すべきデジタル I&C 規制プログラムと組織能力を特定した。

推奨事項

以下は、チームが推奨するデジタル I&C の許認可と規制監督を継続改善するために焦点を当てるべき分野である。

- NRC は、新規もしくは構想から設置までで大きく異なるアプリケーションに対する、デジタル I&C 技術レビュー、HFE レビュー及びそれに続く検査監督の三者間での統合〈integration〉と情報共有〈communication〉を改善し続ける必要がある。
- NRC は、事前承認を必要としない 10CFR50.59「変更、検査及び試験」[4]を利用したデジタル I&C 改造に対する監督プログラムを改善し続ける必要がある。
- NRC は、デジタル I&C 設計と人的要素ライフサイクル評価のためのシステム工学的アプローチの評価ガイダンスを開発する必要がある。システム工学的アプローチは、承認されたデジタル I&C 設計が安全機能を維持するよう適切に統合されていることを確認するために重要である。
- NRC は、許認可及び監督プロセスにおけるデジタル I&C システムの定量的評価に向けて、デジタル I&C の運転経験の収集と共有を増やす手段を模索する必要がある。

以下は、チームが推奨する維持、強調すべき規制プログラムと組織能力である。

- 堅牢で効果的な安全文化：NPP におけるデジタル I&C の安全使用をサポートするため、中核規制及び監督に関する NRC の使命を効果的に果たすことが可能になる。
- 深層防護的規制アプローチ（リスク洞察と多様性の適切使用）：安全機能に悪影響を与える可能性のある予期せぬデジタル I&C 不良を軽減する。
- 知識管理とデジタル I&C プログラムの有効性継続評価
- リスク上重要な非安全関連システム及び高度に統合された非安全関連制御システム。安全に焦点を当てたレビューアプローチの使用を継続する必要がある。
- パフォーマンスベースのアプローチを可能にするガイダンスの適用。規制ガイドに規定の

[4] Changes, tests and experiments, https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0059.html

アプローチではなく、技術的に中立なもの。

- 安全上重要なデジタル I&C 近代化の許認可変更要求〈license amendment requests〉に対する統合レビューの重要視化
- 安全を最重要視する産業の国内外規制当局が参加するデジタル技術規制アプローチ定期共同セミナーの継続実施

付録

ボーイング 737 墜落：NRC のデジタル計装制御評価プロセスに向けた教訓[1] 抜粋

序論

ボーイング 737 の MCAS 開発及び認証における考慮事項

ボーイング社は、その飛行経済性を高めるため、737 シリーズの新型（737 MAX）に大型で燃費の良いエンジンを搭載した。自動操縦特性向上システム（MCAS）は、737 MAX 8（以降 MAX 8 と呼ぶ）に施されたいくつものアップグレードの一つであり、エアロダイナミクスの設計変更に対処するものである。米国連邦航空局（FAA）は、2012 年に設計変更型認証（ATC）申請を審査し、2017 年 3 月に認証した。

地上とのクリアランス制約のため、物理的に大型のエンジンの位置を翼の最先端より前に置く必要があった。その結果、特に迎角（翼と空気流との角度）が大きい時のエアロダイナミクスが変わった。もし、迎角が大きいときに推力を上げたら、飛行機のピッチ角がより大きくなり、失速（ストール）し得る。これに対処するには、パイロットが機首を下げる必要がある。

こうした状態を自動的に補償するため、ボーイング社はフライト制御計算機上で動くMCASソフトウェアを開発し、MAX 8 が高仰角に関する飛行構成限度に達したときの手動飛行時の速度トリム（飛行を安定させるために行われる操縦装置）を調節できるようにした。つまり、仰角センサーが対空速度と高度をもとにしたしきい値を超えた時、飛行機のピッチ角をもとに下げるようスタビライザーを制御することで、大型エンジン搭載の結果としてのピッチ角増大に自動的（無操作）で対処できるように MACS は設計された。この開発のゴールは、世界中のパイロットが慣れ親しんだ 737 先行機と全く同じように操縦できるようにすることにより、パイロットのシミュレータ訓練の必要性をなくすことであった。

確率的な影響評価にもとづき、ボーイング社は、その ATC 要求において MCAS のリスクを「高」とはランク付けしなかった。ボーイング社による機能ハザード評価には、パイロットが操作するまで継続するMCASの誤作動が含まれてはいた。意図的ではないが、パイロットによる対処がなければ、故障条件下では MCAS は機首を下げ続ける効果がある。しかし、ボーイング社と設計者は、職業パイロットならば意図しない MCAS 作動を「暴走スタビライザー」状態（パイロット訓練で取り扱われるシナリオ）と認識するだろうと想定していた。ボーイング社は、単一の意図しない MCAS 作動をテストしたが、MCAS の複数作動は単一作動より価値がないと想定していた。

FAA は、その安全認証業務代行権限制度（ODA）プログラムを介する自己認証プロセスを用いて、ボーイング社に MCAS の設計認証を委託できると決定していた。ボーイング社は、MCAS のライフサイクル開発プロセスにおける設計、実装、統合、試験を実施した。飛行テストの結果を

[1] BOEING 737 CRASHES: LESSONS LEARNED FOR NRC DIGITAL INSTRUMENTATION AND CONTROLS EVALUATION PROCESS, 2022-09-22, ML22241A039

受け、MCAS はその後、仰角センサー情報にもとづきピッチ角の低下率をより高めることが認められ、偶発的な低速度ストールに対処できるようプログラムされた。

MAX 8 には、仰角センサーは 2 つあるが、MCAS は 1 つの仰角センサーからの入力しか用いてなかった。ボーイング社は 2 つの仰角センサーが 10 秒間以上 10 度以上異なっていた場合は、パイロットに警報を出す機構をすべての MAX 8 の航空電子機器につける意図はあった。しかし、FAA 認証の後、全ての MAX 8 にその警報機能が具備されているわけではないことを発見したものの、安全運航のためにはコックピットにその警報は不要と決定した。理由は、その警報に伴い要求される操作がないためである。ボーイング社はこの問題を修正しようと思ったが、運航への影響はないとみなしたことから FAA の監督署に公式通知を出すことを要求されなかった。FAA は、2018 年の MAX 8 の墜落事故まで、この問題を知ることはなかった。

パイロットは、このような MCAS の特性に関するフライトシミュレータ訓練を受けることはなかった。その理由は、MCAS 関連のエラーは全て、馴染みのある水平尾翼の自動トリム制御における故障（暴走スタビライザー）と同じように扱えると仮定したためである。しかし、MCAS 故障にパイロットが適時応答するのは難しい。なぜなら、そのような状態を認識するのが困難だから。その上、強いエアロダイナミクスに対応して、パイロットは水平スタビライザーを手動調整するのも難しかった。

MCAS の故障

2018 年 10 月 29 日に、ライオン・エア 610 便がジャカルタのスカルノ・ハッタ国際空港を出発した直後にジャワ海に墜落し、189 人の死者を出す悲劇的な事故が起きた。2 つの仰角センサーの 1 つから欠陥データを受信してから、飛行中に MCAS は約 24 回作動したことから、MCAS の反応が、事故の重大要因であると判断された。数か月後の 2019 年 3 月 10 日、エチオピア航空 302 便がアディスアベバ・ボレ国際空港を出発した直後に墜落し、157 人が死亡した。本報告書に記載されている報告書には、事故事象の詳細、技術設計や人的要因の問題、規制上の問題などに関する情報が含まれている。

評価概要

主要な規制、及び技術テーマの評価

- 安全評価（ハザード分析とリスク評価を含む）：ある報告書が特定しているのは、「何がうまくいく必要があるか（性能と設計仕様）」、「何がうまくいかない可能性があるか（人間と装置の故障モード）」、「何がうまくいかないことを防げるか（制御と障壁）」、「人－システム・インターフェイス（HSI）が機能しなければならない事象とシナリオの組み合わせ」を理解することの必要性である。この推奨事項は、安全評価を扱う際の NRC のアプローチに適用可能である。
- 装置の設計と実装：ある報告書が特定しているのは、安全マネジメントシステムの必要性である。これにより、設計、手順書及び訓練の組み合わせが、効果的な安全性能に役立って

いるかどうかを包括的、先見的に評価できる。

- 設計変更型認証プロセス（既存のアーキテクチャ上の新設計）：ある報告書が考察したのは、ボーイング社の設計が ATC として評価されることを決めるために規則やガイダンスに従った一方で、次の 3 分野において規則改善の機会があることである：①「設計変更のパフォーマンスに対するパイロットの期待」及び「パイロット訓練の必要性の有無」に関して使用した想定の理解と図書化、②既存の設計認証に対する複数の変更の累積的影響の評価、③包括的なシステム運転リスク評価の提供と内部コミュニケーション。
- 認証の代行：ある報告書が推奨したのは、ODA 部門に対する潜在的な圧力に対処できるように、FAA と航空産業界が協力すること。これにより、ODA 部門が組織内の他部門からの圧力や影響なしに運営され、FAA 管理者の代表として機能することを保証する意思決定構造を維持できる。NRC の I&C 規制基盤は認証のための ODA プログラムと直接の関係はない。NRC は各認可取得者に対して、デジタル I&C の設計、許認可と運転に対する独立した検証・妥当性確認（V&V）のための品質保証プログラムを持つことを要求している。これは、NRC 検査とも独立している。
- 安全文化：ある報告書が推奨したのは、安全な製品の作成に主眼を置く安全文化を促進することである。これら製品は、認証要件に準拠することになる。

洞察と推奨事項

A 設計と実装の問題

- NRC は、デジタル I&C と原子力発電所（NPP）の全体設計に、深層防護アプローチを適用する必要性を引き続き強調すべきである。アプローチの例：①共通モード故障（CMF）に対する脆弱性に十分対応していることを示すために、提案されたデジタル I&C のシステム設計を分析する。②損害を起こし得るハザードを特定するために、デジタル I&C システムを試験する。③ハザードを除去、防止、制御するための I&C 機能要求及び手段を実装する。
- 体系的なハザード分析技術は、本質的に高度に統合された新しいデジタル技術に対処するために重要である可能性がある。NRC のハザード分析ガイダンスには、例えば、分析対象のケースが、いつ最悪または境界〈bounding〉ケースになるかを適切に特定するための指針を含むべきである
- 運転経験と関連する故障率データは、デジタル設計の信頼性要求を正当化するためにも、また、そのような要求が運転中も有効であることを保証するためにも重要である。
- 承認、検証及び装備された I&C 設計が、意図したシステム機能を備えていることを確認するためには、概念設計から運転、保守に至るまで、最新のシステムエンジニアリングアプローチと人的要因評価を導入することが重要である。NRC は、新デジタル設計の最重要コンポーネントとして、人間工学（HFE）に継続して焦点を当てるべきである。安全上重要なデジタル I&C レビューにおいて、設計や HFE の技術問題をたどり、解決するために、NRC

スタッフは統合技術チームに継続して重きを置くべきである。

B 規制監督の問題

- デジタル設計規制プロセスにとって重要なのは、設計レビュー、HFE レビュー及び規制監督プロセスの間での調整とコミュニケーションである。この洞察が強調するのは、進化するデジタル設計ならびに概念設計から実装に至るまでに I&C と HFE 分野で用いる仮定を包絡的に評価する必要性である。
- 許認可審査段階において、各々の審査分野において他者が用いた仮定を疑いながら、NRC の I&C 及び HFE の技術部隊は、より緊密にコミュニケーションすべきである。
- 大規模なデジタル更新に対する NRC 許認可スタッフと規制検査スタッフの間で、安全上重要な技術問題に関するコミュニケーション、交流及び引き継ぎをプログラム的に改善する予定である。デジタル許認可審査の最終段階において、I&C 技術スタッフは、推奨検査事項を明確に図書化し、デジタル装置の試験・据付け期間中に現地検査官とコミュニケーションする予定である。
- 10CFR50.59 に基づく NRC 事前承認不要なデジタル I&C 改造に対する規制検査優先事項は、戦略的かつリスク情報を活用したものであるべきである。NRC では、デジタル更新に対して、リスクや実経験にもとづく最も重要な更新に、規制検査リソースを集中するよう、スマートサンプルを使い始めている。事前承認不要なデジタル I&C 改造に対する規制検査においては、追加の検査訓練が役に立つかどうか、NRC スタッフが評価すべきである。
- NRC は、高度に統合されたデジタルシステムを備える進化する技術などリスクの大きいデジタルシステムに、引き続き焦点を当てるべきである。許認可審査においては、リソースが安全上重要なものに向けられるように、安全に焦点を当てたアプローチに従うべきである。NRC は、適合性、深層防護、安全余裕、PRA と運転パフォーマンスに基づく「リスク情報原則<risk-informing principles>」を適用し続けるべきである。
- 効果的でまっすぐな安全文化が最重要であり、NPP におけるデジタル I&C の安全使用をサポートする NRC の規制・監督使命の全うに不可欠である。
- デジタル I&C 分野における専門機関スタッフの長期的な減少に対処するため、NRC の組織能力と知識管理活動は、強化されるべきである。
- デジタル技術情報や洞察を国内外の規制当局と共有・検討することで、より堅牢な安全プログラムが実現する。NRC のデジタル I&C スタッフは、他のデジタル I&C 規制者とのセミナーや情報交換を継続すべきである。NRC は、国内外の基準機関に参加継続すべきである。

結論

2018 年と 2019 年の MAX 8 の墜落事故は、設計、計画、安全文化の不良の結果であり、MCAS の設計、実装と訓練に関係する欠陥であった。NRC チームによると、MAX 8 の航空電子

機器改造に関わる安全機能、故障影響、深層防護とリスクを、原子力施設のデジタル制御安全システムにおける改造に関わるそれらと、掘り下げた技術比較することは困難であったものの、航空機事故に関する調査報告書からの主要な勧告の評価において、デジタル I&C の許認可及び規制検査に対する NRC の規制基盤に重大なギャップ（課題）は見つからなかった。しかし、NRC チームは、NRC のデジタル I&C 規制評価プログラム、規制監督プログラム及び NRC スタッフ組織能力の将来の改善に向けて考慮するのが適当ないくつかの推奨事項を特定した。このような改善は、原子力施設における進化するデジタル I&C 技術の継続的な安全使用を確かなものとするのに役立つと考える。

添付

資料５４－２－３－２

NRC 報告「ボーイング 737 MAX 8 事故から得たデジタル I&C 規制課題に関する予備的洞察」（案）

令和 4 年 7 月 28 日

技術基盤課

RIS2016-05「安全関連システムに組込まれたデジタル装置」[1]は、第 43 回技術情報検討会（令和 2 年 10 月 29 日）にて直ちに国内規制に反映させる必要はないと評価された[2]。ただし、当該 RIS に記載された原子力施設におけるデジタル計装制御（デジタル I&C）に対する米国 NRC の規制基盤近代化活動は、技術基盤課調査・評価班において継続注視することとした。

2021 年 10 月に発行された当該活動の年次報告[3]によると、NRC スタッフは、ボーイング 737 MAX 8（以降 MAX 8 と呼ぶ。）の 2018 年と 2019 年の墜落事故に係る当局の調査報告書の結果と勧告を含め、当該機のデジタル改造に対するボーイング社の設計プロセスと連邦航空局（FAA）の認定プロセスから得られた教訓を体系的に評価している。以下は、2021 年 6 月に、米国原子力学会主催の技術会議で NRC が発表した「ボーイング 737 MAX 8 事故から得たデジタル I&C 規制課題に関する予備的洞察」[4]から抜粋し、補足説明を加えたものである。

要旨

2017 年、MAX 8 はボーイング 737 先行機の変更として運行認可された。MAX 8 は、新型大型エンジン、エアロダイナミクスの改善やフライト制御計算機の操縦特性向上システム（MCAS）ソフトウェアと言ったいくつもの設計変更を取り入れた。MCAS は、新エンジン搭載に伴うピッチ角（飛行機の機首の傾き角度）の増加に係る潜在的な失速（ストール）ハザードを補償するよう設計されていた。離陸後まもなく起こった MAX 8 の両事故は、MCAS の繰り返し作動とその結果としての飛行機の姿勢に拠るとされ、パイロットによる対応が間に合わなかった。

複数の米国や国際当局が、MCAS 設計や事故に寄与したであろう工学的・制度的因子を調査した。NRC はそれらの複数の調査報告書をレビューし、原子力発電所（NPP）におけるデジタル技術の実装に関わる一般的な規制課題を特定しようとしている。本予備的洞察は、設計・実装仕様、ハザード・リスク評価における仮定、及び設計変更に対する承認や検査監督に対する規制プロセス、と言った領域に関する報告書から得られたものである。さらに、許認可プロセス、規制検査・監督や安全文化を通じたデジタル I&C の安全性確保・維持に向けた規制改善や組織的な考慮も模索する。

---

1) RIS2016-05, Embedded Digital Devices in Safety-Related Systems, 2016, ML15118A015
2) 第 43 回技術情報検討会（令和 2 年 10 月 29 日）
3) SECY-21-0091, ANNUAL UPDATE ON ACTIVITIES TO MODERNIZE THE U.S. NUCLEAR REGULATORY COMMISSION'S DIGITAL INSTRUMENTATION AND CONTROLS REGULATORY INFRASTRUCTURE, 2021, ML21253A212
4) NRC, Paper ID 34348, PRELIMINARY INSIGHTS ON DIGITAL INSTRUMENTATION AND CONTROL REGULATORY LESSONS FROM THE BOEING 737 MAX 8 CRASH EVENTS, 2021, ML21063A231

1. 序論

MCAS の開発と実装における一連の失敗が、MAX 8 の 2018 年と 2019 年の墜落事故につながったと見られている。MCAS の設計プロセスと FAA の承認プロセスに関する報告書には、NRC が考慮すべき潜在的な規制教訓が含まれると考えられることから、NRC スタッフは、次の 2 点を特定することに集中した。(1)NRC のデジタル I&C 許認可及び検査プログラム及び関連するプロセスや文化におけるギャップ、(2)NPP でデジタル I&C を安全に使用し続けるために維持・改善すべきデジタル I&C 規制プログラムと NRC の組織能力における要素。

2. MCAS の開発と承認

2011 年、エアバス社 A320 との競合に直面したボーイング社は、時間的制約からゼロからではなく既存の 737 を改造して燃費を向上させることを選び、大型で燃費に優れるエンジンを 737 に搭載することとした。それが MAX 8 である。MCAS は、MAX 8 のエアロダイナミクスの変更に対処するためのいくつもの改造の内の一つである。FAA は 2012 年に 737 型式認証変更の審査を開始し、2017 年 3 月に承認した。

大型エンジンは地上とのクリアランスが十分に取れないおそれがあったので、機体の前方に移動し、上面も高く据え付けることとした。その結果、特に迎角(翼と空気流との角度)が大きい時の飛行機の操縦性に係るエアロダイナミクスが変わった。もし、迎角が大きいときにパイロットが推力を上げたら、飛行機のピッチ角がより大きくなりストールする。パイロットの是正処置は、機首を下げ翼にあたる空気流を増やすことで、揚力を回復することである。

図 1 エンジンの比較(左:737 先行機、右:MAX 8)[5)]

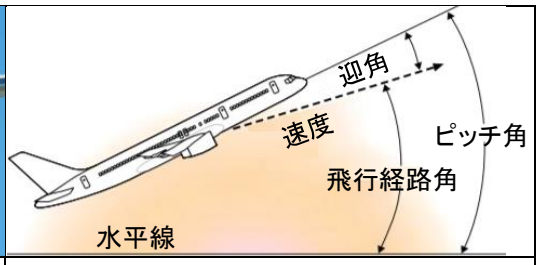

図 2 ピッチ角と迎角[6)]

こうした状態を補償するため、ボーイング社はフライト制御計算機上で動く MCAS ソフトウェアを開発し、手動飛行時の速度トリム(飛行を安定させるために行われる操縦装置の調節)に機能を追加した。MCAS は、MAX 8 が仰角に関する飛行構成限度に達したときに作動するよう設計された自動システムである。つまり、仰角センサーが対空速度と高度をもとにしたしきい値を超えた時、飛行機のピッチ角をもとに下げるようスタビライザーを制御する。具体的には、仰角を低減させるために機首を下向きにするよう水平スタビライザーを動かす。開発のゴールは、新たなパイロット訓練が最小になるよう、737 先行機と同じように操縦できるようにすることであった。

---

5) AV2021020, U.S. Department of Transportation Office of Inspector General Report -Weaknesses in FAA's Certification and Delegation Processes Hindered Its Oversight of the 737 MAX 8, 2021

6) The House Committee on Transportation & Infrastructure Final Report on the Design, Development & Certification of the Boeing 737 Max, 2020

ボーイング社による MCAS ソフトウェアのハザード評価には、パイロット操作があるまで意図せず自動起動した MCAS 機能が継続することが含まれていた。つまり、手動飛行時にパイロット対応がなければ、故障状態下で MCAS は機首を下げる効果がある。しかし、ボーイング社は、パイロットは MCAS の意図しない作動を、パイロット訓練のシナリオの一つとして馴染みのあるスタビライザの暴走と認識するはずと仮定した。また、ボーイング社は単一の意図しない MCAS 作動を試験したが、MCAS の多重作動は単一作動より悪くないと仮定していた。

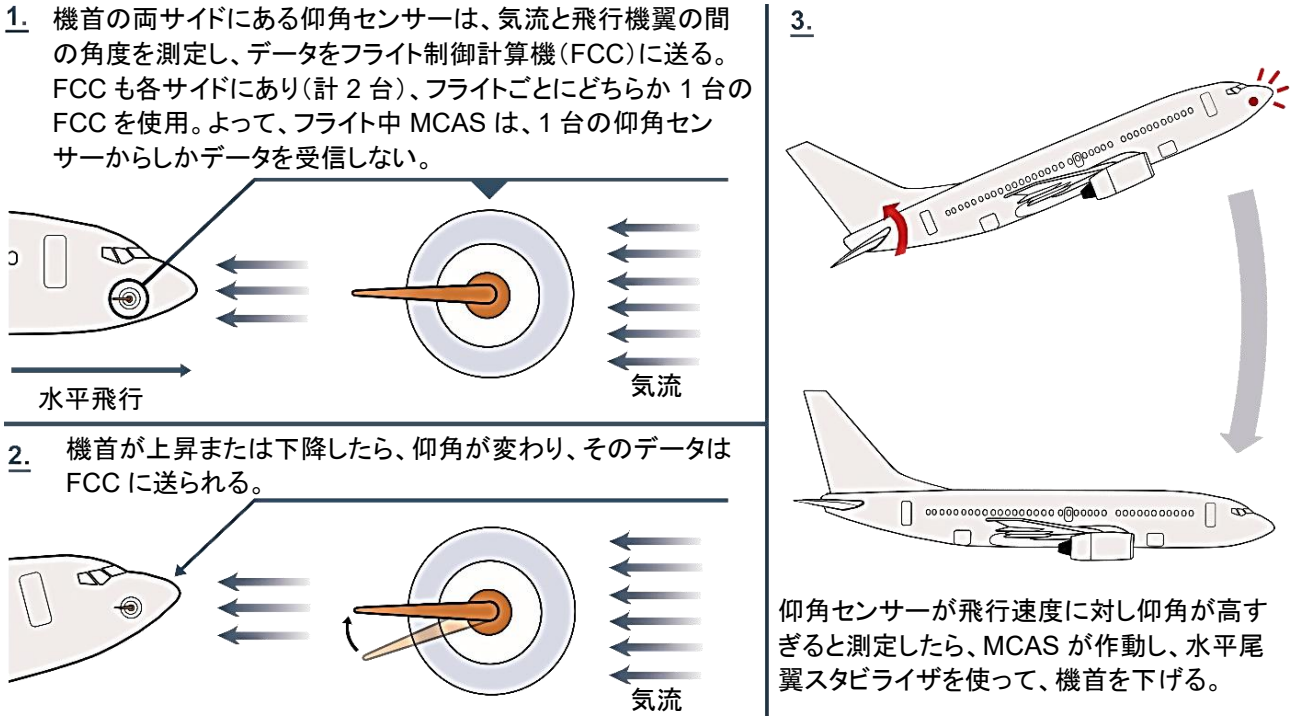

図 3 MAX 8 の MCAS の機能 [5]

FAA は、MAX 8 設計における MCAS パートの承認は、自己承認プロセスを用いるボーイング社に委託できるとみなした。ボーイング社は、MCAS のライフサイクル開発プロセスにおいて、詳細設計、実装、統合、試験を行った。飛行試験の結果、MCAS には予想外の低速ストールへの対応機能がプログラムされたが、これにより仰角センサー情報にもとづくピッチ角低減率を増加させることの正当性を高めることとなった。

MAX 8 には、仰角センサーは 2 つあるが、MCAS は 1 つの仰角センサーからの入力しか用いてなかった。この単一センサーに依存する決定は、故障状態で自動作動した MCAS は重大な影響をもたらさないという仮定にもとづいていた。さらに、ボーイング社は 2 つの仰角センサーが 10 秒間以上 10 度以上異なっていた場合は、パイロットに警報を出す機構をすべての MAX 8 につける予定であった。しかし、FAA 承認の後、全ての MAX 8 にその警報機能が具備されているわけではないことを発見し、安全運航のためにはコックピットにその警報は不要と決定した。理由は、その警報に伴い要求される操作がないためである。ボーイング社はこの問題を修正しようと思ったが、運航への影響はないとみなしたことから FAA に公式通知を出さなかった。FAA は、

2018 年の MAX 8 の墜落事故まで、この問題を知らなかった。

パイロットは、このような MCAS の特性に関するフライトシミュレータ訓練を受けることはなかったし、フライトマニュアルにも MCAS のことは特出されなかった。その理由は、MCAS 関連のエラーは全て、馴染みのある水平尾翼の自動トリム制御におけるエラー（暴走トリム）と同じように扱えると仮定したため。しかし、737 プログラムの初期に、暴走スタビライザトリムにパイロットが応答するには、10 秒以上掛かることをボーイング社は認識していた。さらに、自社のテストパイロットが、フライトシミュレータで意図しない MCAS 作動に対応するのに 10 秒以上掛かり、破局状態を見つけたことをボーイング社は認知していた。

2018 年の離陸直後のライオン航空の MAX 8 墜落事故では、MCAS が重大な寄与因子して特定された。2 つの仰角センサーの 1 つから誤ったデータを受信後、MCAS はフライト中に 24 回作動した。数か月後に、エチオピア航空の MAX 8 が離陸直後に墜落した。

3. 安全重要ソフトウェアに対する NRC の I&C 許認可と FAA 承認アプローチの特性

デジタル機器の安全性や信頼性を確保する上で、一般設計原則、開発方法、規制原則総論において NRC と FAA で概ね違いはない。FAA の最も重要な承認分野に焦点を当てるアプローチは、デジタル設計の安全重要度の高い項目にリソースを集中する NRC のリスク情報を活用したアプローチと概ね同等である。しかし、両機関の許認可・承認プロセスは異なっており、これ以上の直接比較は困難である。相違の例は次の通り。（1）デジタル航空電子工学に対する FAA の承認アプローチや具体的な基準は、デジタル I&C に対する NRC のリスク情報を活用したアプローチや決定論的アプローチもしくは基準と異なる。（2）航空電子工学と原子力デジタル I&C の間では、具体的な制御・安全機能ならびに関連する故障リスクが基本的に異なる。（3）米国の運転 NPP のデジタル I&C と比べて、航空機の運行規模や運転経験は、はるかに大きい。

4. 主要な規制テーマ及び技術テーマの評価

NRC の I&C スタッフは、MAX 8 の主要な報告書から MCAS 設計、開発、規制監督に係る課題に関する指摘事項や推奨事項を体系的に評価し、2 分野（①設計ならびに実装課題、②規制監督課題）を特定した。それぞれの分野に対して、考慮すべきテーマが以下のように抽出されている。

①設計ならびに実装課題	②規制監督課題
設計仕様と深層防護 運転仕様 ハザード分析やリスク評価を含む安全評価 機器設計と実装 性能監視 製造と承認	承認と許認可基準 変更承認プロセス 規制基準と承認機関との間の調整 承認委託と承認後設計変更プロセス 技術革新の管理 規制者の人的能力 安全文化

5. 予備的洞察

分野ごとに、維持・改善すべき規制項目や活動に関する主要な予備的洞察をリストアップす

る。

5.1. 規制監督課題

- ライフサイクルにわたるデジタル設計を理解・評価するためには、デジタル設計審査、人間工学審査及びそれに続く規制検査・監督プロセス間の統合と意思疎通が重要である。
- NRC の I&C と人間工学の技術分野においては、許認可審査の間、各々の審査領域におけるお互いの仮定に疑問を呈すると言う安全文化を保ちつつ、より一層の意思疎通を図るべき。
- 特に、新しい許認可プロセス（ISG-06[7)]）の下での大規模デジタル改造に対しては、許認可と規制検査スタッフ間で意思疎通、相互作用及び技術的課題の引継ぎを NRC が制度的に定義する意思がある。
- 10CFR50.59[8)]の下での NRC 事前承認不要のデジタル I&C 改造に対する規制検査優先度は、戦略的にリスク情報を活用して決めるべきである。
- NRC は、高度に統合されたデジタルシステムを含めリスク重要度の高いデジタルシステムに焦点を当てるべきである。
- NPP におけるデジタル I&C の安全使用のために、NRC の規制及び監督使命を効果的に果たすためには、効果的で率直な安全文化が最重要である。
- デジタル I&C 分野における専門機関スタッフ長期的な減少に対応するためには、NRC の組織能力と知識管理活動を維持すべきである。
- デジタル技術の関する情報や洞察を、国内外の規制者と共有し検討することは、より健全な安全プログラムの構築に資する。

5.2. 設計ならびに実装課題

- 深層防護アプローチは、デジタル機器や人的パフォーマンスにおける不確実性、特に、未知で予測不能な故障メカニズムや現象の可能性を説明するための効果的な工学的手段である。
- 高度に統合された新しいデジタル技術に対応するためには、体系的ハザード分析技術が重要となろう。NRC は、IEEE 7 4.3.2-2016[9)]の付録 D「ハザードの特定と管理」を新しいハザード分析技術としてエンドースするため、調査中である。
- 運転経験とデータは、デジタル設計に要求される信頼性を正当化し、運転中も有効であることを保証するために重要である。
- 設計から運転、保守、及び人的要因に至るまでの安全に対して、システム全体に及ぶ工

7) U.S. NRC, “Digital Instrumentation and Control - Interim Staff Guidance - 06 – Licensing Process, Revision 2, ML18269A259, 2018

8) 10CFR50.59, Changes, tests and experiments

9) IEEE 7 4.3.2-2016, “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, 2016.

学的アプローチを適用することは、承認され実装された I&C 設計が意図されたシステム機能を有することを証明するために重要である。

6. 結論

悲劇的な墜落事故は、一連の設計、制度、安全文化の失敗及び MCAS の設計、実装、訓練に関連する欠点の結果だった。安全機能、故障影響、深層防護とリスクに関して、航空電子工学及び航空機と NPP のデジタル制御の間で、NRC スタッフは技術的比較を行ったが、デジタル I&C の許認可と規制検査に対する NRC 規制基盤に有意なギャップは見つからなかった。しかし、NPP で進化を続けるデジタル I&C 技術を安全に使用し続けるために維持・改善すべきデジタル I&C 規制プログラムと NRC の組織能力の側面がいくつか特定された。NRC は、2021 年に最終評価を完了して発行する予定である。なお、このペーパーは、NRC の公式方針又は規制事項に関する見解を示したものではない。