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)]

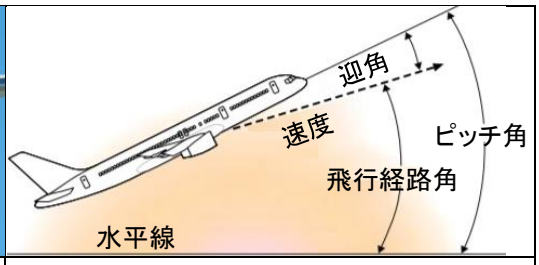

図 2 ピッチ角と迎角[6)]

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。

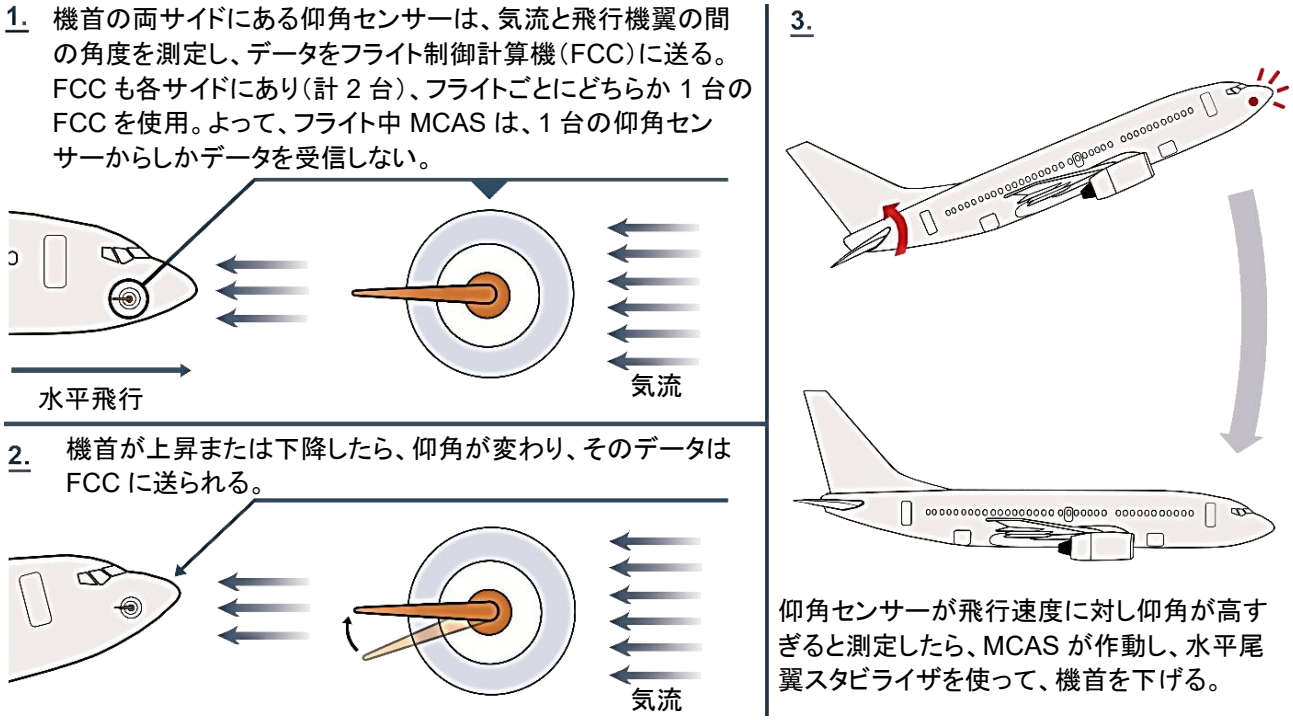

図 3 MAX 8 の MCAS の機能 [5]

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。