ソフトウェアの品質とリスク
（続々編）

2013年10月19日（土）

航空運航システム研究会（TFOS.SG)
航空システム部会　　松田　宏

本日の話題

- 事例-１：　国産哨戒機P-1の全エンジン停止
- 事例-２：　ソフトウェアのバグにより急降下
- 事例-３：　エンジンが起動せず
- 事例-４：　成田空港で出国審査システムなど障害
- 事例-５：　ネット予約で航空券をタダで販売
- 考察と今後の研究課題

事例-1：国産哨戒機P-1の全エンジン停止

（第1報：平成25年6月20日　防衛省）

固定翼哨戒機Ｐ－１（5号機・6号機）の納入の遅延について

- 本年（2013年）5月13日、川崎重工業株式会社において製造中の固定翼哨戒機P-1の5号機について社内飛行試験の際、通常の運用では想定されない、高高度における高速度での急激な機動を行ったところ、エンジンが停止するという事象が発生しました。
- 原因究明の結果、同不具合はP-1の量産化にあたりエンジンの形状を一部変更したため、前述の急激な機動を行った際に、エンジンの燃焼が一時的に不安定となり発生したと判明しました。
- これを受け、Ｐ－１の量産機（注：3号機以降が量産機に該当）に対して不具合対応策を講じることとなったことから、今月末に納入される予定であった5号機及び6号機について、納入が遅延することとなりました。
- 既に厚木基地に配備されている量産機2機（3号機及び4号機）については、現在、飛行を停止しておりますが、更なる原因究明を進めるとともに不具合対応策を講じた後、飛行を再開する予定です。

事例-1：国産哨戒機P-1の全エンジン停止(続)

（第2報：平成25年9月27日　防衛省）

固定翼哨戒機Ｐ－１のエンジン不具合への対応について

- 本年５月１３日、川崎重工業株式会社において製造中の固定翼哨戒機Ｐ－１の５号機について、社内飛行試験の際、通常の運用では想定されない、高高度における高速度での急激な機動を行ったところ、エンジン４発が停止するという事象が発生しました。
- 原因究明の結果、同不具合は、Ｐ－１の量産化にあたりエンジンの燃料噴射弁の肉厚を増加したことが原因となって、急激な機動を行なった際、エンジンの燃焼が一時的に不安定となったために発生したことが判明しました。
- これを受け、防衛省は、このような急激な機動を行った場合においてもエンジンの燃焼が不安定になることがないよう、エンジン制御ソフトウェアを改修することとしました。
- 今後、川崎重工業株式会社で製造中の量産機２機（５号機及び６号機）及び既に厚木基地に配備されている量産機２機（３号機及び４号機）について、上の改修を実施する予定です。これらの機体は、地上運転試験などを経て、飛行を再開する予定です。

事例-1：国産哨戒機P-1のエンジン停止(続々)

IHI社製　XF7-10エンジン

（公表の経緯と考察）

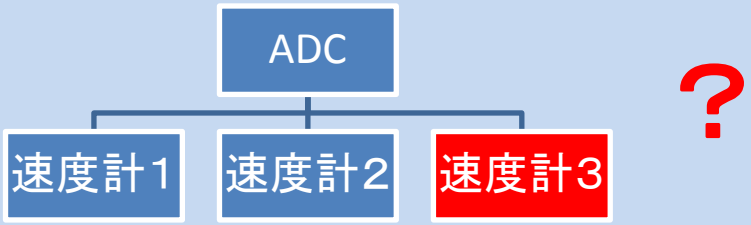
- 発生は5月13日、公式発表は6月20日。単に「エンジンが停止」と発表。
- 記者会見では「複数エンジン」とし、台数は答えなかったが、その後の取材で「4基あるエンジン全部」の停止であったことを認めた。
- 不具合の発生状況は、愛知県沖の太平洋上で高度10,000mから8,000mに急降下後、エンジン出力を急激に下げながら飛行姿勢を立てなおしたところ、エンジンが止まった。乗員が再起動し、無事着陸したというもの。（2013年6月21日　毎日新聞、他）
- 防衛省の公式発表および記者会見を踏まえた報道を見る限り、直接的なソフトウェア製造上の「バグ」ではないと思われる。
- 可能性が高いのは、エンジン形状（詳細不明）変更に伴う燃焼特性の変化を十分に確認（シミュレーションや実際の燃焼試験等で）せず、制御ソフトを変更しなかったということではないか。
- つまり、ソフトウエア仕様の変更管理上の問題と思われる。

事例-2： ソフトウェアのバグにより急降下

- 2008 年 10 月 7 日、豪カンタス航空のエアバス A330 が 急降下し、39 人が病院に運ばれ、うち 12 人が重傷を負った。調査したオーストラリア交通安全局の調査報告書によれば、事故の直接的原因は速度計の不具合で、飛行操縦システムのバグにより急降下したもの 。

http://it.slashdot.org/story/11/12/20/0127215/software-bug-caused-qantas-airbus-a330-to-nose-dive?sdsrc=rel

- 不具合を起こしたのは 3 つある速度計のうちの 1 つ。断続的に誤ったデータを飛行操縦システムに送信し続けていた。また飛行操縦システムのアルゴリズムは 1990 年代に書かれたもので、速度計からの誤ったデータにより急降下を起こす可能性があった。



事例-3： エンジンが起動せず

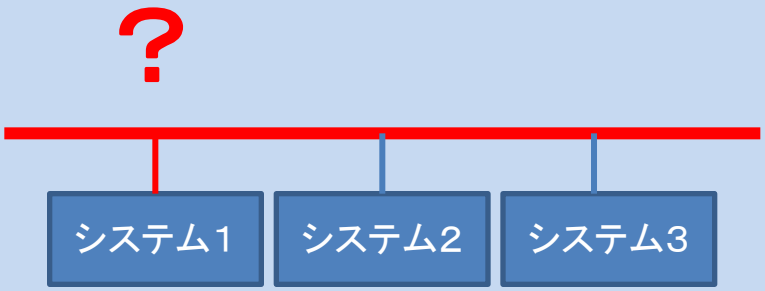
B787のエンジン起動せず欠航、山口

- 2013/6/12 12:47 (2013/6/12 13:30更新)　12日午前9時ごろ、山口宇部空港で、羽田行き全日空692便のボーイング787が駐機場を出発しようとした際、右エンジンが起動せず欠航した。乗客約140人は次の便や他社便に乗り換えた。
- 全日空によると、エンジン起動の際、電気を供給する機体の補助動力装置（APU）がうまく機能せず、地上電源からケーブルをつないでエンジンを起動しようとしたがかからなかった。
- APUの不具合とエンジントラブルの関連は不明でエンジン制御のコンピューターに問題があった可能性もあるという。
- 全日空787は10日にも、福岡空港で地上走行中にコックピットでエンジンの不具合が表示され、駐機場に引き返すトラブルがあった。〔共同〕

事例-4：　成田空港で出国システムなど障害

2013年7月11日午前7時過ぎ、成田空港第2旅客ターミナルの出国審査場や荷物検査場のシステムに障害が発生し、出発ロビーは保安検査を待つ乗客約600名が行列を作るなど、一時混乱した。

東京入管成田空港支局などが原因を調べている。障害が発生したのは出国審査場の出入国管理システムの一部と、航空機に積み込む受託手荷物の爆発部物を検査するシステム。



互いのシステムは独立しており、いずれも通信に不具合があった。

事例-５：ネット予約で航空券をタダで販売

- 米ユナイテッド航空が9月12日にインターネットを通じた予約販売で約１５分間、国内線の航空券を税別で無料、または10ドルの超格安で売り出す珍事がおきた。
- 原因は同社の手違いによるもの。ユナイテッド航空は「予約時に表示された価格で航空券を提供する」と説明。

(2013.9.15　日本経済新聞)

- 損害額は公表されていない。
- ユナイテッド航空の対応は、法的な義務（錯誤による取引契約は取り消し可能）を超えたもの。
- 日々変動する運賃の単純な入力ミスが原因と思われる。
- 事務手順にチェックプロセスがなかったか省略した？
- 機械系に妥当性チェック機能がなかった？

考察と今後の研究課題

- 電気系統に不具合が起きた、操縦室の計器に異常を示す表示が出た、エンジンが起動しなかった、などと報道されている航空機のインシデントの多くが、実は制御ソフトの問題によるものである可能性がある。
- 航空機と管制機関との間を結ぶデータリンクなど、搭載システムの不具合が頻発しているのに公式な報告がされず、記録情報が整備部門に眠っている可能性がある（同じようなトラブルが余りにも多いため？）。
- ネットに接続された複数システムが相互に干渉する障害が少なくないにもかかわらず、対策が講じられていない（高度計の障害による誤データの垂れ流し、成田空港での複数システムの同時障害など）。

- 情報処理推進機構（IPA)は、社会的インフラを支える情報システムの障害が原因となって広く国民に影響を及ぼすトラブルの発生を重視。「重要インフラ情報システム信頼性研究会報告書」を公開。
  ⇒　TFOSではどのような取り組みが可能か？