情報システムの障害によるリスクの想定

2013年1月25日

航空運航システム研究会（TFOS.SG)
航空システム部会　松田　宏

前回のテーマ

ソフトウエア品質とシステム信頼性を考える

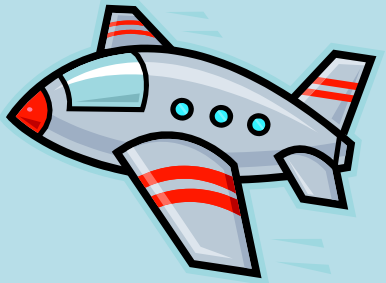
＜障害事例に学ぶ＞

Part-1　システムの基礎知識
Part-2　システム障害の事例
Part-3　ソフトウェア品質の向上策

2012年10月27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

ご提案した研究課題



- 適切な信頼性要件の設定方法
- 障害時の対応方法（人的な対応を含む）
- 要員の教育訓練（利用者、運用者、管理者、開発者）
- 標準化と陳腐化の矛盾の解決方法
- インターオペラビリティ（相互運用性基盤）の確保

今回のテーマ

- 航空情報システムの障害事例（前回の復習）
- 適切な信頼性要件の設定方法（考え方）
  - 信頼性を追求すると高くつく
  - 社会的に許容できるリスクは？
- 障害時の対応方法（人的な対応を含む）
  - あらゆる事態に対応することはできない
  - 白黒ではなく灰色と適切な「あきらめ」を！

障害事例1：システム障害でコンフリクト？

- 1975年頃、羽田空港のARTSシステムと東京管制部のFDPシステムとの間のデータ交換開始直後、ARTS側から未定義の文字コードが送信されたためFDPシステムが停止。

  たまたま新潟上空でシベリア方面行と札幌行と福岡行の航空機が輻輳しており、管制官が障害に気をとられている間にコンフリクト（規定の管制間隔が無くなる状況）が発生した。

  ［原因］

  ARTSシステムとFDPシステムの間にあるデータ伝送システムの文字コード変換テーブルに誤りがあった。

障害事例2：システム障害で欠航・遅延

- 2003年3月1日午前7時頃、東京航空交通管制部が運用する飛行計画情報処理システム（FDP）が障害で停止。欠航215便、大幅な遅延1500便、足止めされた客30万人。
- 午前1時に防衛庁と東京航空交通管制部で飛行計画をやり取りする「防衛庁システム対応プログラム」が追加され稼働。
- 午前7時に「オンライン統計処理プログラム」が自動起動され、「防衛庁システム対応プログラム」と矛盾が発生。
- 原因はメーカーの仕様があいまいで、起こりうる競合状況が想定されていなかったため。

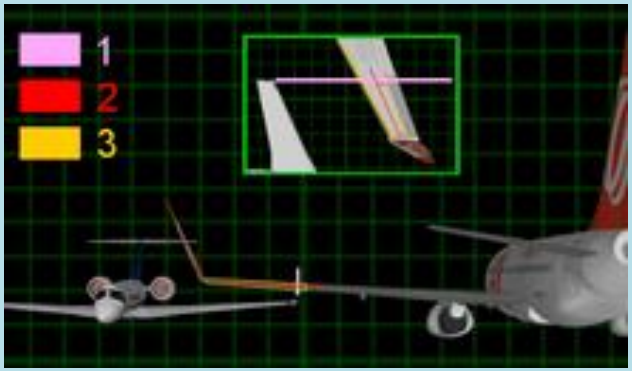
障害事例3：システム障害で遅延

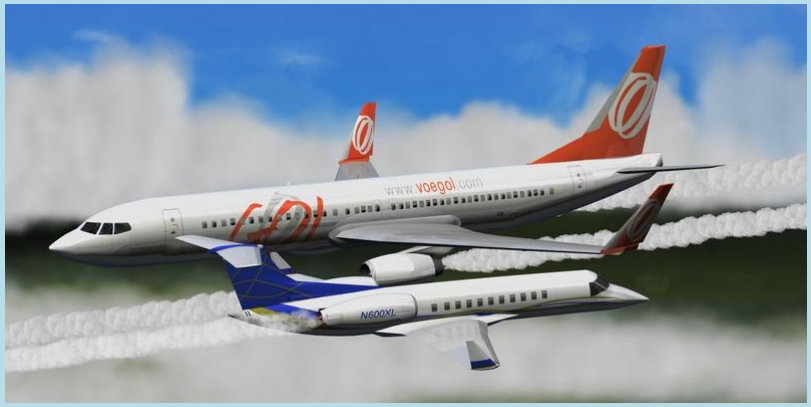
- 2004年4月8日19時11分に航空路レーダー情報処理システム（RDP）がダウンした。
- 名古屋発福岡行きの便の飛行計画情報にあり得ない経由地が含まれていたため、異常処理として自動再起動したがデータが残っていたためダウンと再起動を繰り返した。
- 予備系システムが稼働したが、業務の一部を人手で行ったため、国内便だけで130便に30分以上の遅れが出た。

- 国土交通省は、「FDPが持つデータや、RDPのハードディスクに書き込まれたデータの中に、不正なデータはなかった。メモリにデータを展開した際にソフトウエアを原因とする不具合が起こったと考えている」とした。

障害事例4:システム不具合で空中衝突？

- 2006年9月29日にブラジル内陸部でブラジル・ゴル航空のB737-800と米エクセルエアのエンブライエル・レガシー600が、同一経路を同一高度で飛行して空中衝突。
- エンブライエルは近くの空港に緊急着陸したが、B737-800は空中分解して墜落。乗員乗客154名全員が死亡。
- 原因は調査中。管制システムが管制官の指示高度と航空機の飛行高度を混同した仕様になっていたから、との説がある。





信頼性とコストのせめぎあい

- 一般にシステム信頼性を高めるとコストが急増する。ただし、技術進歩や量産効果によって価格は低下する。
- 本当はどのレベルの信頼性が必要なのか、科学的、合理的に検証し、数値的に要件を設定することは少ない。
- 「安全」について情緒的な表現がまかり通り、コスト要素は議論されないことが多い。
  - 「1000%の安全性が確保されるまでは飛行禁止」
  - 「どんな津波が来ても大丈夫なように高い堤防を作って欲しい」
  - 「原発は安全です」「いや、原発は危険です」
- 目的のために信頼性を犠牲にする、という選択もありうる。
  - 「無線機は重いし故障が多いので積まずに飛ぶ」
    （初めて大西洋横断飛行に成功したチャールズ・リンドバーグ）

高信頼性のシステムは高くつく？

- 昔の電話機は、日本電信電話公社が非常に厳しい規格を定めていたので、ほとんど故障しなかった。しかしメーカーは、輸出用に普通品質の電話機を安く作っていた。

  （例）

  – 接点には金の小塊を溶着
  – 送話器の炭素粒はベトナム・ホンゲイ炭の最良品
  – 外部ケースは最高級のプラスチック

必要なお金はかけるべき？

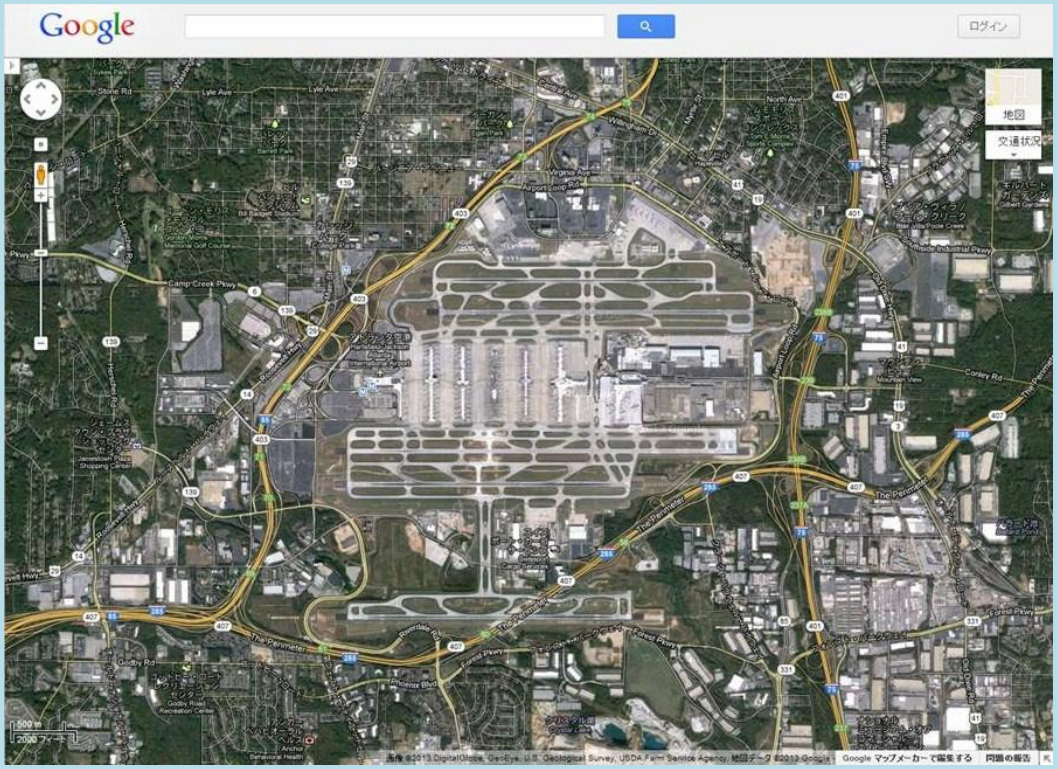
- 日本銀行が運営する日銀ネットは、日本銀行と全ての金融機関を結んで巨額のお金を動かす重要ネットワーク。「金に糸目をつけない」構築だったため信頼性が抜群に高く、障害はゼロとのこと。

- アメリカ大統領専用車は防弾ガラスと軍用装甲で覆われ、爆発物や携行ロケット弾が命中しても壊れない。各種通信システムも完備。ただし、お値段は1台30万ドル。

過剰な信頼性は無意味かも？

- アトランタ国際空港は年間95万回（羽田の約3倍）の離着陸があるが、レーダーは1台。気象条件で空港閉鎖になる確率の方が高いので、二重化の必要はないと判断したとのこと。
- 念のため隣接の軍基地からデータを送ってもらっている。

The Hartsfield-Jackson Atlanta International Airport



社会が許容するリスク（1）

（日本社会の場合）

- 事前加工した「ふぐ」をふぐ調理師がいない店で食べる
  （過去10年間のふぐ中毒者：2名、死亡者：なし）*1
  ⇒事前加工した「ふぐ」を扱う店ではふぐ調理師不要に
- 雷注意報が出ている日にゴルフに行く
  （落雷による被害者：年平均20人、うち死亡者は13.8人）*2
- 注意が出ている水辺で遊ぶ。遊泳禁止の川や海岸で泳ぐ。
  （平成23年の水難者：1,656人、死者・行方不明者：796人）*2
- 徒歩や自転車、自動車などで外出する
  （交通事故による死者：年間約4,800人）*2

*1：東京都、*2：警察庁

社会が許容するリスク（2）

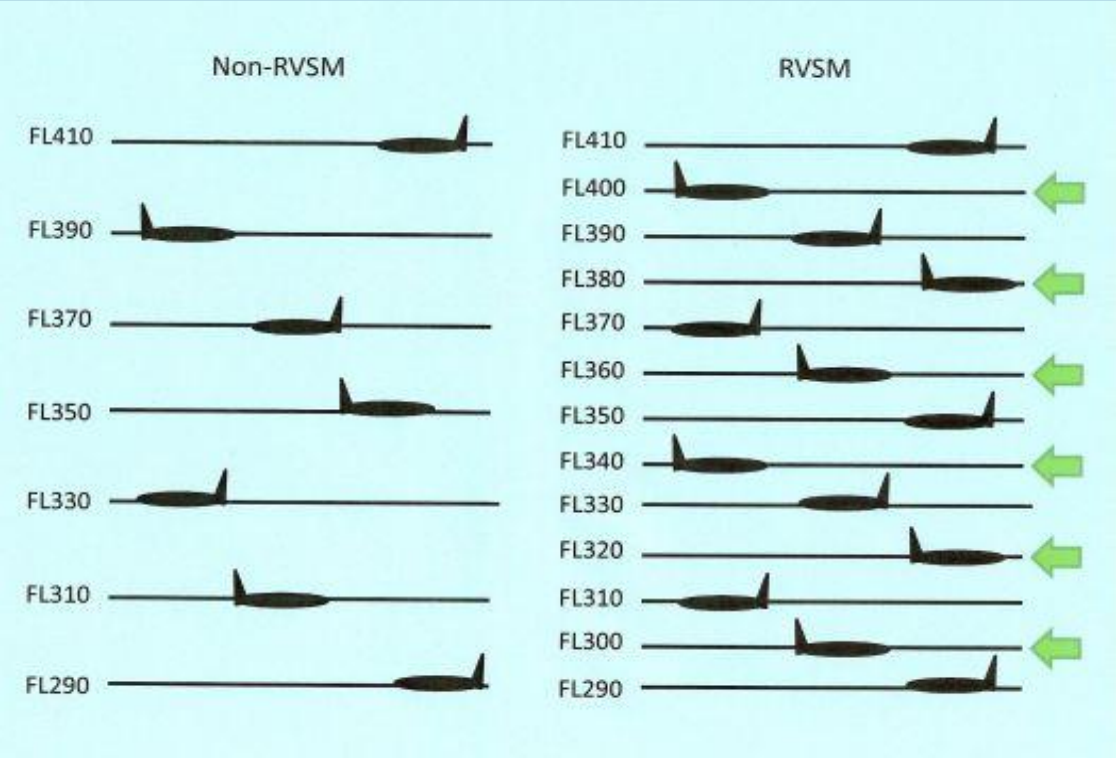
（アメリカの場合）

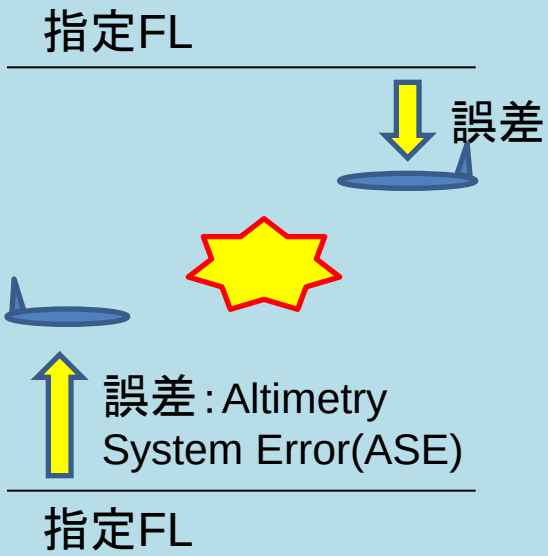
- 飛行機で旅行する
  （死亡率：0.0009%＝9.0×10^{-6}、
  米国内航空会社：0.000034%＝3.4×10^{-7}）*3
- アメリカ国内を自動車で旅行する
  （死亡率：0.03%＝3.0×10^{-4}）*3
- 銃器天国のアメリカに住む
  （銃による年間の死亡者：約3万人/3億人＝1.0×10^{-4}、
  うち殺人：40%＝4.0×10^{-5}
  自殺者55%、その他事故など5%）*4

*3：米国家運輸安全委員会(NTBS)、*4：TIME

高度計の誤差による空中衝突リスク

- FL290～410の垂直間隔を2000ftから1000ftに短縮した短縮垂直間隔（Reduced Vertical Separation Minimum: RVSM)の安全性許容レベル(Acceptable Level of Safety)は1飛行時間あたり5.0×10^{-9}の致命的事故（1事故＝2機の航空機）





ひとりの人の年間リスク

- 天が落ちてくる（杞憂）：小惑星が地球に激突し人類が絶滅
  6500万年に1回　＝　1.5×10^{-8}（1時間あたり1.7×10^{-12})
- 年末ジャンボ宝くじを買って1等（4億円）が当たる
  1000万分の1　＝　1.0×10^{-7}
- 交通事故で死ぬ
  4800人/1億2600万人　＝　3.8×10^{-5}
- 何らかの理由（病気、事故、自殺）で死ぬ
  114万人/1億2600万人　＝　9.0×10^{-3}

システム信頼性要件の考え方

- 「絶対安全」を実現するのは絶対に無理（技術＆費用）
- どのようなリスクがどの位の規模と確率で起こりうるかという「想定」が信頼性要件を設定する基礎となる。
（例：超高層ビルの設計でどの位の風速を想定するか）
- リスク（または安全性）に対する考え方は文化／国／地域によって異なる。ICAOでは地域ごとの合意を推奨している。
- システムの一部分だけ信頼性が高くても意味がない
（例：電池交換なしで1,000年間使える心臓ペースメーカー）

位置づけによる信頼性要件の違い

- 搭載システムの障害は個々の航空機単位。事故につながる場合が多いが、致命的ではない場合もある。
  - 飛行制御など飛行継続に絶対必要なシステム
  - 航法など、複数の代替手段があるシステム
  - 通信、監視など、止まっても飛行そのものは継続できるシステム
- 運航管理システムの障害は運航者単位。ただし、直接事故につながることは相対的に少ない。
  - 出発機は運休／遅延
  - 飛行中の航空機は監視／指示ができなくなる
- 交通管理／管制システムの障害は空域単位。飛行中の航空機については事故につながる可能性がある。
  - 出発機は運休／遅延で対応できる
  - 飛行中の航空機は管制間隔が維持できなくなる

障害時の対応方法を段階的に設定

- ひとつのシステムにすべてを委ねず、障害時のための代替手段や予備システムを準備しておく。
- システム障害時に全機能を喪失しないよう、分散配置したり段階的に機能縮退できるよう設計しておく。
- システム機能が低下したり停止したりした場合に、人手で対応する方法を決めておき、定期的に訓練しておく。
- これ以上は「あきらめる」という決心ポイントを決めておく。

情報システム障害 ≠ 事故発生

- 情報システムの障害が航空機の運休や遅延などの経済的損失をもたらす場合は少なくないが、必ずしも重大インシデントや事故につながる訳ではない。

- 情報システムの障害が事故の原因となる場合もあるが、運航乗務員や管制官など人間が介在することが多く、因果関係や責任の所在は不明確である。

- 情報システムの障害が設計や仕様設定に起因する場合、経済的損失や事故との因果関係が間接的で証明困難である。

高信頼性のパラドックス

- 昔の化学プラントでは頻繁にトラブルが起きたので、監視員は経験豊富で、適切に状況が判断でき、修理も迅速だった。

  最近は信頼性が向上してトラブルが少ない、何か問題が起きても経験不足で対応できず、復旧に時間がかかる。

- 業務をすべて情報システムに依存し、障害もめったに起きない状況では、ごくまれに起きる障害に対応できなくなる。

- 誤入力や誤操作によって間違った結果が出ても、気がつかずに見落としてしまう可能性が高まっている。

次回予告

- 標準化と陳腐化の矛盾の解決方法
  - 標準化とはどういうことか
  - 標準化のメリットとデメリット
  - 陳腐化しない標準化の進め方
- インターオペラビリティ（相互運用性基盤）の確保
  - インターオペラビリティとは何か
  - 標準化、互換性との違い
  - インターオペラビリティの実現方法

ご清聴ありがとうございました。