

航空管制における統合情報管理システム要件開発工程に関する一考察

藤田 雅人[†]

(独) 電子航法研究所[†]

1. 導入

航空管制においては様々な情報—航空機の予定飛行経路等を示した飛行計画情報・空域の経路情報・高層気象に関する気候情報・レーダやその他の監視手段による航空機の位置監視情報—が用いられる。これらのデータは、効率的な空域使用のための飛行時間帯や飛行経路の事前調整等の戦略的活動、航空機が飛行中にそれらの間の安全な間隔を維持する等の戦術的行動、過去の飛行実績等のレビューによる継続的改善活動に用いられるべきである。

現在においてはこれらの情報は完全に統合されておらず、いくつかの独立なシステムがこれらの業務の一部を実施している。

米国においては上記の情報を統合的に提供するシステムの開発を進めている^[1]。これは SWIM (System Wide Information Management) プログラムと呼ばれている。基本となる設計思想にはサービス指向アーキテクチャ (SOA, Service-Oriented Architecture) を採用する予定である。

欧州における管制機関を管理する EUROCONTROL でも同様のプロジェクトを立ち上げている^[2]。

(当該プロジェクトも SWIM と呼ばれている。) 欧州においては複数の国・地域が異なる管制システムを用いている。欧州における SWIM プロジェクトの目的は、機能ごとに分かれたシステム・情報の統合を目的とせず、国・地域間のシームレスな情報共有が目的である。欧州においては 5 つの WP (ワークパッケージ) が定められている。WP1 は要件定義・WP2 はプロトタイプ構築・WP3 がユーザテストによる改良・WP4 が妥当性検証・WP5 が費用便益分析である。WP5 の結果、前のワークパッケージに戻る場合もある。

本稿では、欧州型の要件開発工程を参考に、本邦での将来の情報統合に際し行われるシステム要件開発工程についての一考察を示す。

2. 便益分析の必要性

データ統合に伴うシステムアーキテクチャの簡略化により、保守コストの低減等の便益が期待できる。また、航空機の飛行計画と当該航空機の監視データや、着陸滑走路と滑走路の整備情報等、関連するデータを管理番号等で統一的に管理することにより、データが断片化してあちこちのシステムに保存されていたときには困難であったサービスの提供が可能になると見込まれる。

一方で、航空管制システムはその故障や不具合が人命・財産に大きな損失を与えるセーフティクリティカルシステムである。したがって、航空管制システムのような大規模システムにおいて、完全に網羅的な試験や検証は不可能^[3]であっても、可能な限りのリスク分析・安全対策をとる必要がある。

航空管制システムも他のセーフティクリティカルシステム同様、広範なソフトウェアハザード分析や完全性分析等を含めた要求分析・安全性検証等の実施が望まれる^[4]。

ソフトウェアハザード分析では危険源を特定し、その効果を推定する。ハザード分析の結果如何では、ハザードの除去・低減・制御のため、更なる機能の追加が必要となるであろう。情報統合を行い、多くのシステムがデータにアクセスできるようになった場合、それらのシステムの故障・不具合によりデータが破損・改変・消去される可能性について考えなければならない。多くのシステムがアクセス可能になるほど、システムの取りうる状態の数は増加し、ハザード分析の作業量は増大していく。

また、要件の完全性分析等のため、形式仕様記述などが用いられる場合もある。これらの適用には、他の仕様記述言語と異なり、数学の専門知識を有する分析者が必要となる。管制情報システムへの VDM-SL (Vienna Development Method - Specification Language) の適用^[5]や空中衝突防止システム TCAS II への RSML (Requirements State Machine Language)^[6]の適

Consideration on Integrated Information Management System in Air Traffic Control

[†] Masato Fujita, Electronic Navigation Research Institute

用などが報告されている。

管制情報処理システムにおいては要件定義工程において上記の作業が必要となるため、他のセーフティクリティカルでないシステムと比較して、コストがかかることとなる。

Chaos Report^[7]にある通り、プロジェクトの失敗の50%以上が要求分析・要件定義の失敗に起因する。(不完全な要求:13%・利用者とのコミュニケーション不足:12%・もはや必要とされないシステム7.5%等) 要求分析・要件定義をおろそかにし、多大なコストを費やして望まれないシステムを構築することは避けなければならない。また、仮に直接的な利用者が導入を望むとしてもとしても、社会的な費用が便益を上回る場合には導入すべきではないであろう。したがって、高度な専門性やリソースを大量に必要とするハザード分析や詳細な要件定義工程に入る前に、利用者の要求と要求分析者の要求に対する理解が乖離していないか確認し、さらには、便益が費用を上回るか分析することが望ましい。

先に述べたように、欧州のSWIMプロジェクトにおいてはBoeing社による費用便益分析がワークパッケージとして定義されている。

3. プロトタイプの必要性

先進的な管制情報管理システムの導入により、管制機関が独占していた情報の一部が、運航者等の他のステークホルダーにも利用可能となる。航空管制システムはこれまで主に航空交通管制官のみが利用者であったが、その利用者の範囲が広がることとなる。このことは、要求分析工程における利用者とのコミュニケーションの困難性が増すことを意味している。そのような条件下で、利用者から要求を引き出し、利用者へ便益を見積もってもらわなければならない。さらには、ハザード分析に協力して貰わなければならない。これらの作業に際して、システムに対する正しい利用者の理解は不可欠であるが、それを得ていくことは難しいと想定される。

自然言語の文や形式仕様記述による仕様定義では専門家以外の利用者にもその内容を理解して貰うことは困難である。簡単な図による仕様記述では、詳細な運用イメージが掴みにくく、詳細なハザード分析が困難になると考えられる。利用者がシステムの具体的なイメージを掴みながら便益見積りや要求分析に参加できるようにするためにはプロトタイプ構築が必要であろう。プロトタイプの構築は、仕様定義工程に更なるリソースを要する手法であるが、システムの規

模・便益見積りやハザード同定への幅広い範囲の利用者の参加の必要性を考え、要件定義失敗によるプロジェクト失敗のリスクを考えれば、考慮に値すると考える。

4. まとめ

本稿では、まず、欧米での航空管制における統合情報管理システムの開発目的と開発工程の差異について紹介した。

次に、セーフティクリティカルシステムである管制情報管理システムの要件開発においては、ソフトウェアハザード分析や完全性分析等を含めた要求分析が必要であることを述べた。これらの工程はセーフティクリティカルでないシステムに比べ、多くのリソースが必要となる。望まれないシステムや、費用が社会的便益を上回るシステムの構築を避けるため、利用者の要求と要求分析者の要求に対する理解が乖離していないか確認し、さらには、便益が費用を上回るか分析する必要がある。高度な専門性やリソースを大量に必要とするハザード分析や詳細な要件定義作業はその後に行うほうが望ましい。

統合情報管理システムにおいては利用者の範囲が広がるのが想定される。最後に、幅広い利用者とのコミュニケーションを行いながらの要求の獲得・便益見積り・ハザード分析にはプロトタイプの使用が望ましいことを述べた。

参考文献

- [1] <http://www.swim.gov>
- [2] <http://www.swim-suit.aero/swimsuit>
- [3] Hamlet, R.: Testing for trustworthiness, In Jackey, J.P. and Schuler, D.: Direction and Implications of Advanced Computing, pp.97-104, Ablex Publishing Company (1989).
- [4] Leveson, N.G.: Safeware -System safety and computers, Addison-Wesley Professional (1995).
- [5] Praxis, A.H.: Using formal methods to develop an ATC information system, IEEE software, Vol. 13, No.2, pp. 66-76 (1996)
- [6] Leveson, N.G., Heimdahl, M.P.E., Hildreth, H. and Reese, J.D.: Requirements specification for process-control systems, IEEE transactions on software engineering, vol. 20 No. 9, (1994).
- [7] The Standish Group: CHAOS Report (1994).