解説概要一覧に戻る

29-4　航空機システム／構成品の開発プロセス

１．はじめに

日本の航空機産業では、防衛省による P-1 機及び C-2 機の開発に続き、半世紀ぶりの民間旅客機である MRJ（Mitsubishi Regional Jet）の開発が進められており、機体会社は確実に航空機開発のレベルを上げてきている。一方、航空機に搭載されるシステムや構成品については、防衛省機では主要な国内装備品メーカーが開発に携わってきたが、MRJ 開発ではその殆どを海外メーカーに頼らざるを得ない状況となっており、「国内民間航空機産業は空洞化している。」とも言われている。

このような状況となっている主な理由としては、①民間航空機システム／構成品の開発経験不足、②コスト競争力の弱さ、③量産対応能力の弱さ　などが挙げられる。これらの課題の中で、②コスト競争力の弱さや③量産対応能力の弱さは、メーカーへの資金面での支援、製造現場作業の合理化や品質向上活動などを進めることで対処可能になるものと思われる。しかし、その前に①の開発経験不足の課題については、新規開発案件の機会を得るために技術者が熟知しておかなければならない開発プロセスがあり、そのプロセスに則った開発を行わなければ、機体会社は航空機の型式証明を取得することが出来ない。この開発プロセスは、海外のシステムメーカーや構成品を開発する装備品メーカーにとっては今や当然のこととして扱われているが、国内のシステム／装備品メーカーの技術者にはまだ浸透しておらず、ここ数年で各社とも調査／研究を始めているところである。

本稿では、民間航空機のシステム／構成品を開発する技術者が知っておかなければならない開発プロセスの全体概要について調査した結果を報告する。

２．開発プロセス

２．１　背景、関連文書及び相互関係

1980 年代頃から、航空機の構成品にコントローラが搭載されるようになりソフトウェア制御が主流となるにつれ、ソフトウェアの不具合による事故が多発し、それを防ぐ為に RTCA（Radio Technical Commission for Aeronautics）より DO-178[1]としてソフトウェア開発プロセスのガイドラインが制定された。そのガイドラインを改訂する際、ソフトウェアへ要求仕様を規定しているシステムや航空機レベルに対しても安全性の観点から開発プロセスを規定する必要があるということになり、SAE（Society of Automotive Engineers）から ARP（Aerospace Recommended Practice）として ARP4754[2]が制定された。

ARP4754 では、開発プロセスの規定と同時に、ARP4761[3]で規定されている安全性解析プロセスも並行して進めなければならないことが規定されている。また、ARP4754 では、コントーラの開発プロセスに関しては、電子機器ハードウェアのガイドラインとして RTCA が規定している DO-254[4]や、ソフトウェアのガイドラインである DO-178 に従うよう規定されている。さらに統合化されたコントローラやモジュールに対する開発プロセスのガイドラインとして DO-297[5]に従うことも規定されている。

ARP4754 で謳われているこれらの文書による開発プロセスの相互関係を図１に示す。

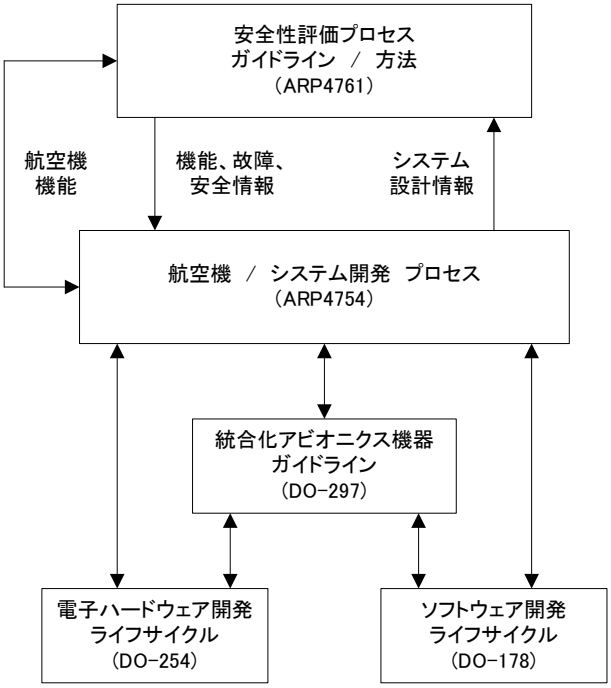

図１　高度統合化／複雑化されたシステム開発に適用すべきガイドラインの関係

２．２　開発プロセス概要

ARP4754 に基づく開発は、大きく分けて７つの開発活動に分かれており、安全性評価活動と密接に関連している。これらの関係を図２に示す。

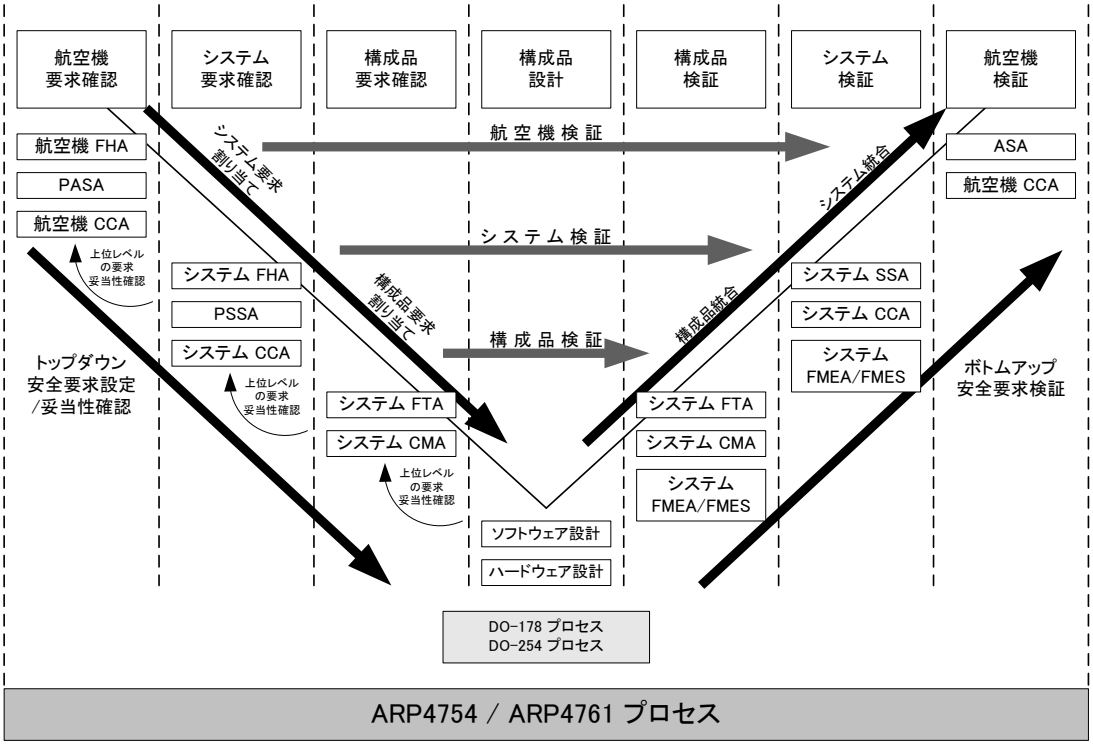

図２　開発プロセスと安全性解析プロセスの相互関係

ARP4754 の 7 つの開発活動は、以下の通りである。

① 航空機要求確認：航空機の機能／性能要求の決定
② システム要求確認：航空機要求から各システムレベルへの要求の割り当て
③ 構成品要求確認：システムに必要な構成品の検討及び各構成品への要求割り当て
④ 構成品設計：構成品内で必要なモジュール／部品の検討、モジュール／部品への要求割り当て、及び詳細設計
（電子機器の設計については、DO-297/DO-254/DO-178 による。）
⑤ 構成品検証：構成品レベルでの機能／性能／耐環境性等の検証
⑥ システム検証：システムレベルでの機能/性能/耐環境性等の検証
⑦ 航空機検証：航空機レベルでの機能/性能/耐環境性等の検証

ARP4754 の 7 つの開発活動と、これらの活動を実施する上で制定する必要がある文書、及び安全性評価との相互関係を以下で概説する。

(1) 開発計画（Development Plan）

機体会社は、航空機の型式証明を取得する為に認証計画他、各種計画書を制定し航空局の認可を受ける必要がある。その航空機レベルの計画書を受け、システムメーカーもシステムを開発する上での開発計画、妥当性確認計画、検証計画、形態管理計画及び、プロセス保証計画を制定し、航空局もしくは機体会社の認可を受ける必要がある。その後、計画に従った開発作業を進めることになる。

また、制御装置を開発するメーカーは、上記計画を受け DO-297/DO-254/DO-178 に基づき、同様の計画書を制定し認可を受けて開発することになる。

なお、各種計画書は開発の初期段階で制定される為、開発進捗に伴い内容を逸脱した場合のことも考慮し、その時の対応プロセスも規定しておく必要がある。

(2) 要求の取り込み（Requirements Capture）

航空機からの要求には、安全性要求、機能的要求、耐空性上の付加的要求、派生要求等があり、機能的要求には、操作要求、性能要求、物理的インターフェイス要求、メンテナンス要求などが含まれる。

これらの航空機要求を受け、システム／構成品などの下位レベルでも上位要求を取り込むと共にさらに下位へ要求割り当てを決めていくことになる。ここで大事なことは(3)項で説明する安全性評価から導かれる要求がしばしばシステムや構成品のアーキテクチャに大きな影響を与えることである。従って、安全性評価は開発初期の要求取り込み段階から並行して実施しておく必要がある。

(3) 安全性評価（Safety Assessment）

安全性評価は、ARP4754 の開発プロセスと密接な関わりがあり、ARP4761 で解析手法が詳述されている。その概要を以下に示す。

航空機やシステムレベルでの潜在的な機能故障及びその故障が航空機へ及ぼす影響度を

確認する為に、FHA (Functional Hazard Assessment) が行われる。航空機に及ぼす影響度は「Catastrophic（破壊的)」から「No Safety Effect（危険無し)」までの５つのレベルに分類され、このレベルに応じて DAL（Development Assurance Level）と呼ばれる開発保証レベルが設定される。故障発生時の航空機への影響度と DAL の関係を表１に示す。

表１　故障発生時の航空機への影響度と DAL

故障発生時の航空機への影響度	DAL
Catastrophic	A
Hazardous/Sever Major	B
Major	C
Minor	D
No Safety Effect	E

表１の DAL に応じて開発プロセスの厳密さ、つまり要求の妥当性確認（Requirements Validation）や実施検証（Implementation Verification）の方法などが決まることになる。

また、各機能故障がどのようにして発生するかを調査する為に、PASA（Preliminary Aircraft Safety Assessment）や PSSA (Preliminary System Safety Assessment) を行い、機能故障の発生確率を要求値内に抑える為に、各機能や構成品、モジュールのレベルでの故障確率の割付を行う。

さらに、Common Cause Analysis（共通原因解析）として、Particular Risks Analysis、Common Mode Analysis、及び Zonal Safety Analysis と呼ばれる解析も行い、これらの安全性解析結果から、派生要求の設定や、場合によってはシステムアーキテクチャの変更等、設計へのフィードバックを行いながら開発を進める必要がある。

(4) 要求妥当性確認（Requirements Validation）

要求妥当性確認は、指定した要求が十分に正しく、完全で、その要求が顧客や航空機メーカー、システムメーカー、構成品メーカー、メンテナンス業者、認証機関などのニーズを満たしていることを保証する為のプロセスである。

要求妥当性確認のプロセスでは、航空機要求がシステムレベル、構成品レベルの要求へブレイクダウンされるときに、要求元が追跡可能なように要求のマトリックスを作成して管理／トレースする必要がある。

各要求内容には、正確性（Correctness）や完全性（Completeness）が求められる為、それぞれにチェックリストを用意して確認するなどの対応が必要となる。

また、例えばあるシステム性能要求を満足させる為に各構成品に要求を設定する際、シミュレーション結果から導かれた内容を構成品要求とする場合は、シミュレーション実施時に前提条件（Assumption）を設定することがある。この前提条件は正確性の面で保証された裏付けが必要となるため、事前試験等で確認する場合がある。そのような場合、要求妥当性確認プロセスでは、この前提条件も明確に管理し、最終的に正確であることが裏付けられるまで管理していくことが求められる。このような要求妥当性確認の厳密さは DAL

によって決められており、レベルA、Bでは複数の確認作業が要求されている。
これらの内容を含め、要求の妥当性を確認すべき内容、方法などを妥当性確認計画書として規定し、確認作業を行う必要がある。

(5) 構成品設計（Item Design）
(4)項で、航空機やシステムにとって妥当であることが確認された要求に基づき、各構成品の設計を行う。ARP4754では構成品設計に関する記述はないが、制御装置の設計に関しては、電子機器ハードウェアはRTCA発行のガイドラインであるDO-254に、ソフトウェアについてはDO-178に従った開発を行うことを推奨している。また、複数のシステムが統合化された制御装置を開発する場合は、DO-297にも従うことが記述されている。

(6) 実施検証（Implementation Verification）
実施検証は、目的の機能が正しく実装され要求を満足していること、及び安全性解析結果の妥当性が保たれていることを確認するプロセスである。
実施検証のインプットは、航空機やシステム、または構成品に対する要求事項のすべてであり、各要求に対してどのように検証するかを示したマトリックスを作成して管理する必要がある。検証方法は、DALにより検査／評価、解析、試験等から複数の方法を実施する必要がある場合もある。例えば、レベルAやBでは、試験とその他の項目の計2つ以上の方法で検証しなければならない。
上記のような内容を含め、検証すべき内容、方法などを検証計画書として規定し、検証活動を行う必要がある。

(7) 形態管理（Configuration Management）
形態管理は、システム、構成品、特定施設または工具などの認証データを対象とし、それらのデータや記録を後から取り出すことができ、または同一データが再生可能となるように、解析や検査で使用するツールや方法も含めて管理する（ソフトウェアの場合はVersion管理を含む）ことが目的である。
形態の変更を適切に管理するため、基本形態を確定させた段階から管理を行い、変更や問題点等も残す必要がある。これらのデータや記録を適切に保管、管理する為のプロセスを形態管理計画書として規定し、管理する必要がある。
なお、航空機が運用の段階に入った後も、継続して形態変更を管理していく必要がある。

(8) プロセス保証（Process Assurance）
プロセス保証活動は、必要な計画がシステム／構成品の各レベルで規定され、開発プロセスが計画に則って実施されていることを証明することが目的である。
プロセス保証計画書では、開発計画、認証計画、妥当性確認計画、検証計画、及び形態管理計画のそれぞれの範囲や内容が、システム／構成品の各レベルでDALに適合した内容であることを確認する必要がある。
また、開発プロセスを評価する際、手続きや業務内容が文書化されているか、意思疎通面で適切なプロセスにより関係者に情報を伝えているか、計画の更新手続きが定められて

おり過去の計画も確認出来るようになっているか、などを確認する。

プロセス保証の証拠としては、認可日付のある各計画書、計画書で要求している報告書やレビュー結果、各活動の結果として得られたデータ、及び適切なタイミングで実施されたプロセス保証のレビュー結果などが含まれる。

３．おわりに

本稿では、民間航空機のシステムや構成品の開発に携わる技術者が熟知しておかなければならない開発プロセスについて概説した。従来の開発プロセスと比較すると、詳細設計までに要求の取り込みや要求妥当性確認のプロセスを確実に実施し、要すれば上位要求へフィードバックすることで詳細設計段階での作業の後戻りを極力無くすようになっている。また、要求取り込み段階から安全性評価も並行して実施することで、より後戻り作業を無くすことを確実にしていることが大きな違いである。

しかし、実際の開発に携わる技術者がこれらの合理的なプロセスを理解せず機械的に作業を進めても、派生要求の設定を見落すなど不完全な要求仕様となり、結果的に後戻り作業が発生してしまうことに変わりはない。従って、このプロセス改善の目的を十分に理解しておく必要がある。また、各アウトプットをレビューする技術者においても同様である。

更に忘れてはならないことは安全性評価を担当する技術者の育成である。この技術者は、発生する可能性のある各故障について、その故障が航空機に及ぼす影響度合を判断出来なければならず、豊富な知識と経験が要求される為、各社共、長い時間を掛けて技術者を育成していかなければならない。因みに、この安全性評価技術者は海外でも人材が不足しており、なかなか雇用出来ないようである。

以上、主に ARP4754 による開発プロセスについて述べたが、これらの開発プロセスを日本の各メーカーもしっかり理解し確実に実行することで、近い将来国際的な競争力を獲得できるものと期待している。

参考文献

1) RTCA DO-178：“Software Considerations in Airborne Systems and Equipment Certification”, Radio Technical Commission for Aeronautics
2) SAE ARP4754：“Certification Considerations for Highly Integrated or Complex Aircraft Systems”, Society of Automotive Engineers
3) SAE ARP4761：“Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”, Society of Automotive Engineers
4) RTCA DO-254：“Design Assurance Guidance for Airborne Electronic Hardware”, Radio Technical Commission for Aeronautics
5) RTCA DO-297：“Integrated Modular Avionics Development and Certification Considerations”, Radio Technical Commission for Aeronautics