第1回航空機装備品認証技術オープンフォーラム

装備品認証に関わる活動報告

平成31年3月

MHIエアロスペースシステムズ株式会社
各務博之

目次

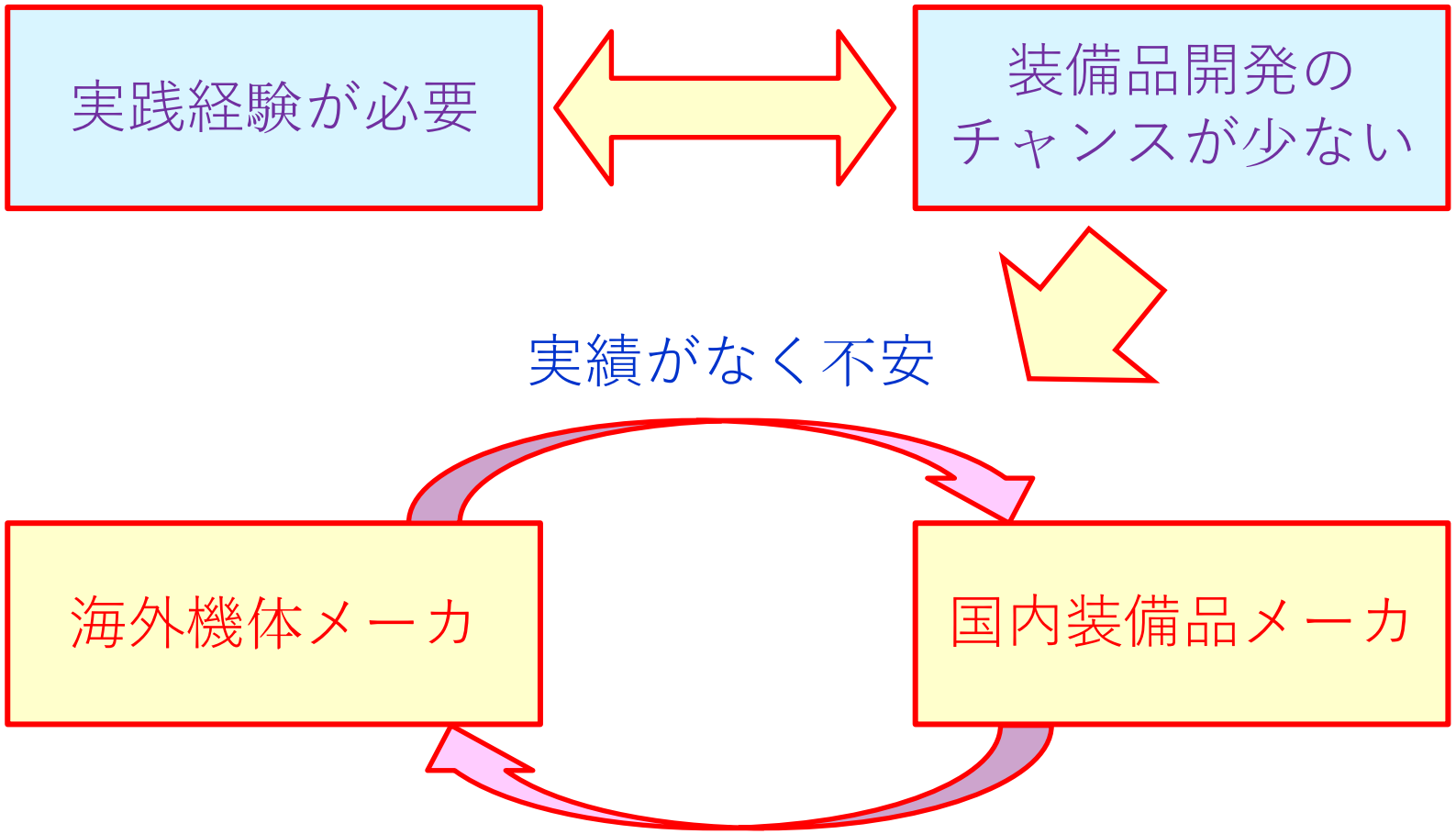
1. イニシアティブ設立の背景と概要

1.1 国内装備品メーカの声

- ソフトウェア搭載装備品を開発するチャンスが少ない
- ソフトウェア技術者を常時維持できるほど開発の機会がない
- 開発案件が少なく国内でノウハウが蓄積されていない
- 開発時の投資が高く回収に時間がかかる
- 初期に作らなければならないドキュメントにコストがかかる

1.2 装備品メーカの抱えるジレンマ

DO-178Cに準拠した開発プロセス構築は・・・



1.3 イニシアティブの設立

- 民間航空機搭載ソフトウェアの認証(DO-178C)に関しては日本は欧米と比べて遅れている。
- 国内装備品メーカはソフトウェア搭載装備品の開発に逡巡している。
- これを打開するには個々の企業努力だけでなくALL JAPANで臨む必要がある。

ソフトウェア認証技術を集結した拠点として、
「航空機装備品ソフトウエア認証技術イニシアティブ」
を設立する

目標とするイメージ・・・

そこに行けば、DO-178Cのソフトウェア認証に必要となる人、技術、情報、設備が揃っており、国内装備品メーカが安心して装備品開発に取り組める拠り所となる場所。

1.4 イニシアティブの概要

名称：航空機装備品ソフトウエア認証技術イニシアティブ
(Software Certification Technology Initiative for Aircraft Equipment)

目的：

本イニシアティブは、民間航空機装備品に必要なソフトウエア等の認証活動を支援し認証基盤と連携体制の構築を先導することにより、航空機産業の発展に資することを目的とする。

幹事メンバー：

<発起人>
国立研究開発法人宇宙航空研究開発機構
東京航空計器株式会社
住友精密工業株式会社
シンフォニアテクノロジー株式会社
多摩川精機株式会社
MHIエアロスペースシステムズ株式会社

<オブザーバ>
経済産業省　航空機武器宇宙産業課
中部経済産業局　航空宇宙産業課
関東経済産業局　航空宇宙産業室
文部科学省　航空技術戦略室
国土交通省　航空局
新エネルギー・産業技術総合開発機構
日本航空宇宙工業会
中部航空宇宙産業技術センター

設立：平成30年4月24日
会員：28社(平成31年3月時点)

1.5 イニシアティブにおける活動の定義

イニシアティブ規約第3条より

第3条 前条の目的を達成するため、本イニシアティブは次の事業を行うことができる。
(1) 会員間の情報交換及び連携強化に向けた方策の検討
(2) ソフトウエア認証規格の技術テーマに関するワーキンググループの開催
(3) ソフトウエア認証に必要となるデータと情報の整備及びその提供
(4) トレーニングの提供
(5) 各種支援ツールの整備と試用サービスの提供
(6) シンポジウム開催等による情報発信
(7) 海外との連携に向けた活動
(8) その他、前条の目的を達成するために必要な事業

2. 装備品認証活動のロードマップ

2. 装備品認証活動のロードマップ

▼イニシアティブ設立

活動内容	H27	H28	H29	H30	H31
1. 教育プログラムの提供 (1) セミナー	DO-178C	DO-254	ARP4754A	DO-178C入門 DO-254入門	中級コース 設立
(2) トレーニング			DO-331実践	DO-178C実践	実践資料整備 コース設立
2. DO-178C技術テーマ議論			SA・DC/CC	Requirements	・・・・
3. 認証支援データの提供		Plan/Std文書	Plan/Std文書 標準ライブラリ	設計データ 標準ライブラリ	Verification 標準ライブラリ
4. コンサルティング実施		DO-178C	DO-178C ARP4754A	個別案件	個別案件
5. 支援ツール整備		DO-178ツール	DO-331ツール	DO-178/333 ツール	DO-178/ 安全性解析
6. 海外連携		調査		協力要請・ 技術協議	技術協議・ トレーニング

：経済産業省事業　：JAXA事業　：JAXAプロジェクトと連携　：愛知県補助金

3. イニシアティブの活動の詳細

3.1 教育プログラムの提供
3.2 DO-178C技術テーマ議論
3.3 認証支援データの提供
3.4 コンサルティング実施
3.5 支援ツール整備

3. イニシアティブの活動の詳細

3.1 教育プログラムの提供
3.2 DO-178C技術テーマ議論
3.3 認証支援データの提供
3.4 コンサルティング実施
3.5 支援ツール整備

3.1 教育プログラムの提供(1/5)

民間航空機認証に関わる教育プログラムを作成しセミナー、トレーニングを実施する。航空機産業参入を目指す企業から技術習熟を目指す企業まで幅広くサポートする教育プログラムを構築する。

3.1 教育プログラムの提供(2/5)

初期段階(平成27年度～28年度)は、勉強会の形式で認証に関する規格の解釈を参加者間(日本の主たる航空機装備品メーカ)で議論し合い、その解釈論について有識者(FAA DER)に確認する形式で実施した。その結果を解説書としてまとめた。

活動年度	テーマ	実施日数	参加メンバー		DER
			企業数	人数	
平成27年	DO-178C (ソフトウェア認証)	5	9	23	Charles Soderstrom
平成28年	DO-254 (ハードウェア認証)	6	9	24	Charles Soderstrom

FAA : Federal Aviation Administration
DER : Designated Engineering Representatives

3.1 教育プログラムの提供(3/5)

平成29年度は要望の強かったシステムレベル(ARP4754A、ARP4761)の技術習得を目的として日本国内の有識者による講演を開催した。また、DO-331に準拠したモデルベース開発に関してツールを用いた実践的なトレーニングを実施した。

テーマ	実施日数	参加メンバー		講師
		企業数	人数	
ARP4754A (システム開発) ARP4761 (安全性解析)	2	9	35	航空局、三菱航空機、 三菱スペースソフトウェア、 有人宇宙システム、MASC
DO-331 (モデルベース開発)	6	9	25	MASC

3.1 教育プログラムの提供(4/5)

今年度はこれから航空機産業参入を目指す企業を対象としてDO-178C、DO-254の初級編のセミナーを開催した。
また、上級者向けにDO-178Cの実践編としてツールを用いたトレーニング(トレーサビリティ、静的解析、テスト、カバレッジ分析)を4日間開催した。

テーマ	実施場所	参加メンバー		講師
		企業数	人数	
DO-178C(初級編)	東京	27	44	MASC
DO-178C(初級編)	名古屋	21	30	MASC
DO-254(初級編)	東京	33	46	MASC
DO-254(初級編)	名古屋	15	23	MASC
DO-178Cトレーニング	名古屋	7	13	MASC

3.1 教育プログラムの提供(5/5)

本活動の成果物として以下のセミナー、トレーニング用資料を作成した。

<セミナー>

(1) DO-178C セミナー(初級編) (4 hours)
(2) DO-178C セミナー(上級編) (3 days)
(3) DO-254 セミナー(初級編) (4 hours)
(4) ARP4754A/ARP4761 セミナー(初級編) (1 day)
(5) DO-330 セミナー(上級編) (1 day)
(6) DO-331 セミナー(上級編) (2 days)

<トレーニング>

(1) DO-178C トレーニング (3 days)
(2) DO-331 トレーニング (2 days)

<書籍>

(1) DO-178C 実践ガイドブック

3.1 教育プログラムの提供(例)

教育プログラムの例として平成30年度に実施したDO-178Cトレーニングから「静的解析編」を紹介する。

静的解析とは作成されたソースコードがコーディングルールに準拠しており、自己矛盾を含まず正確であり、一貫性があることを分析するものである。その活動を支援するツールが多く提供されている。

本トレーニングではDO-178Cとしてどのような静的解析が要求されているかを理解すると共に、いくつかのツールを実際に使用して各ツールの違いを体感する。

これにより、併せて今後のソフトウェア開発の際に使用すべきツール選定の一助とするものである。

目次

トレーニング資料より抜粋

1.1 静的解析ツールの概要

トレーニング資料より抜粋

静的解析ツールを用いると、ソースコード内の潜在的な不具合及びMISRA-C等のコーディングガイド違反等を検出することが出来るため、ソースコードの品質向上に大きく貢献する。代表的な静的解析ツールを下表に示す。

ツール	メーカー	Tool QualificationのCredit
TBvision	LDRA社	A-5 #2, #3, #4, #6
Bug Finder	MathWorks社	A-5 #3, #4, #6
Code Prover	MathWorks社	A-5 #3, #6
Klocwork Insight	RogueWave社	A-5 #3, #4, #6
C++Test	Parasoft社	―
PGRelief	富士通ソフトウェアテクノロジーズ社	―

今回はTool Qualificationに対応している静的解析ツールのうち、TBvision、Bug Finder及びCode Proverについて解説する。

3. イニシアティブの活動の詳細

3.1 教育プログラムの提供
3.2 DO-178C技術テーマ議論
3.3 認証支援データの提供
3.4 コンサルティング実施
3.5 支援ツール整備

3.2 DO-178C技術テーマ議論(1/3)

DO-178Cには、まだDERの間でも議論し尽されていない技術テーマが多くある。これらのテーマについて日本国内で議論し、日本としての考えをPosition Paperにまとめて国内外に発信する。

Federal Aviation Administration

CAST Position Papers

CAST Number	Title
CAST 1 (PDF)	Guidance for Assessing the Software Aspects of Product Serv Airborne Systems and Equipment
CAST 2 (PDF)	Guidelines for Assessing Software Partitioning/Protection Sche
CAST 3 (PDF)	Guidelines for Assuring the Software Aspects of Certification V Obsolete Electronic Parts Used in Airborne Systems and Equi
CAST 4 (PDF)	Object-Oriented Technology (OOT) In Civil Aviation Projects: C Concerns
CAST 5 (PDF)	Guidelines for Proposing Alternate Means of Compliance to DO
CAST 6 (PDF)	Rationale for Accepting Masking MC/DC in Certification Projec
CAST 7 (PDF)	Open Problem Report (OPR) Management for Certification
CAST 8 (PDF)	Use of the C++ Programming Language
CAST 9 (PDF)	Considerations for Evaluating Safety Engineering Approaches Assurance
CAST 10 (PDF)	What is a "Decision" in Application of Modified Condition/Decis (MC/DC) and Decision Coverage (DC)?
CAST 11	Superceded by CAST 11A

Certification Authorities Software Team (CAST)

Position Paper
CAST-19

Clarification of
Structural Coverage Analyses of Data Coupling and Control Coupling

Completed January 2004

(Rev 2)

NOTE: **This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and**

3.2 DO-178C技術テーマ議論(2/3)

平成29年度より3件の技術テーマに関して日本国内のエンジニアと議論し3件のPosition Paperを作成した。

活動年度	技術テーマ	議論日数	参加メンバー	
			企業数	人数
平成29年	Software Architecture	2	13	23
平成29年	Data Coupling/Control Coupling Analysis	2	12	21
平成30年	Requirements	2	12	20

3.2 DO-178C技術テーマ議論(3/3)

作成したPosition Paper(日本語版/英語版)は、海外の有識者のレビュー結果を反映したのち公開予定。

1/42

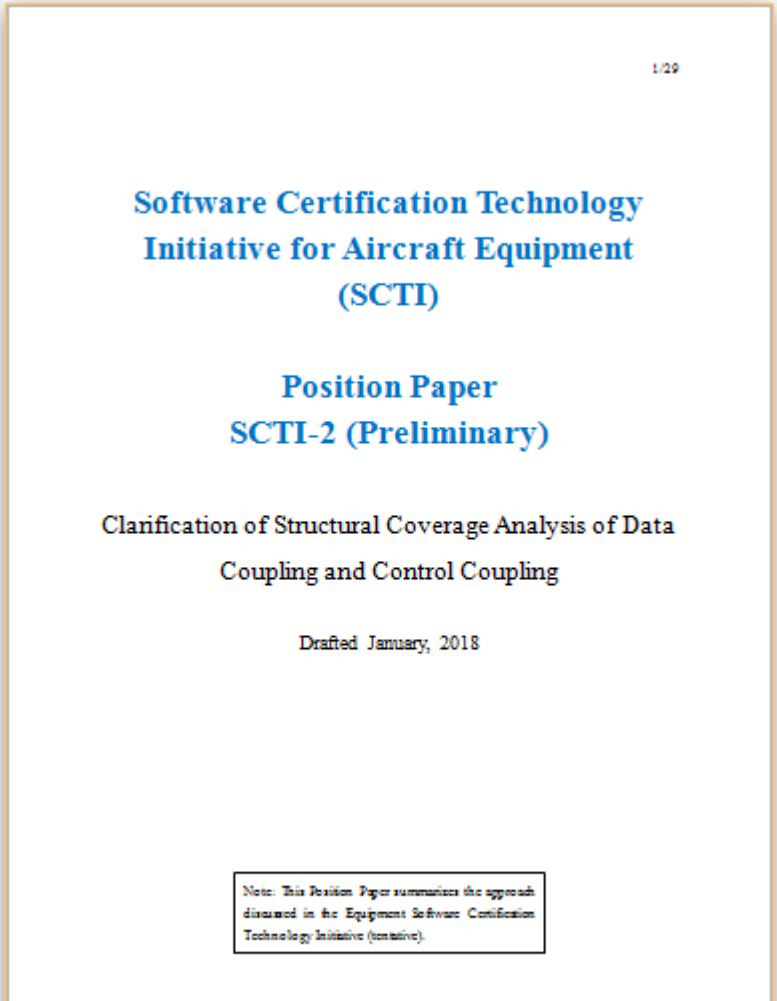
Software Certification Technology
Initiative for Aircraft Equipment
(SCTI)

Position Paper
SCTI-1(Preliminary)

Clarification of Software Architecture

Drafted December, 2017

Note: This Position Paper summarizes the approach discussed by the Equipment Software Certification Technology Consortium (tentative).



1/29

Software Certification Technology
Initiative for Aircraft Equipment
(SCTI)

Position Paper
SCTI-2 (Preliminary)

Clarification of Structural Coverage Analysis of Data Coupling and Control Coupling

Drafted January, 2018

Note: This Position Paper summarizes the approach discussed in the Equipment Software Certification Technology Initiative (tentative).

3.2 DO-178C技術テーマ議論(例)

DO-178C技術テーマ議論の例として今年度議論した「Requirements」を紹介する。

DO-178C における基本的な考え方のひとつとしてRequirement Based という概念があり、ソフトウェア開発プロセスにおいてHigh Level RequirementsとLow Level Requirementsを作成することになっている。

しかしながら、そもそもRequirementsとは何か、

System Requirements/

High Level Requirements/

Low Level Requirements において

どこまでの詳細度でブレークダウンされるべきかが曖昧であり、

議論すべき必要がある。

◇ 資料目次

議論時の資料より抜粋

1. **Derived Requirements (※)**
   - 1.1 Derived Requirementsの定義
   - 1.2 Derived Requirementsとトレース
   - 1.3 Derived Requirementsの必要性
   - 1.4 Derived Requirements作成の全体像

   ＋アンケート結果についての議論／TQAの例
2. **FAA REMH (第1回研究会資料の抜粋)**

   ＋アンケート結果についての議論／TQAの例
3. **ソフトウェア開発プロセス**

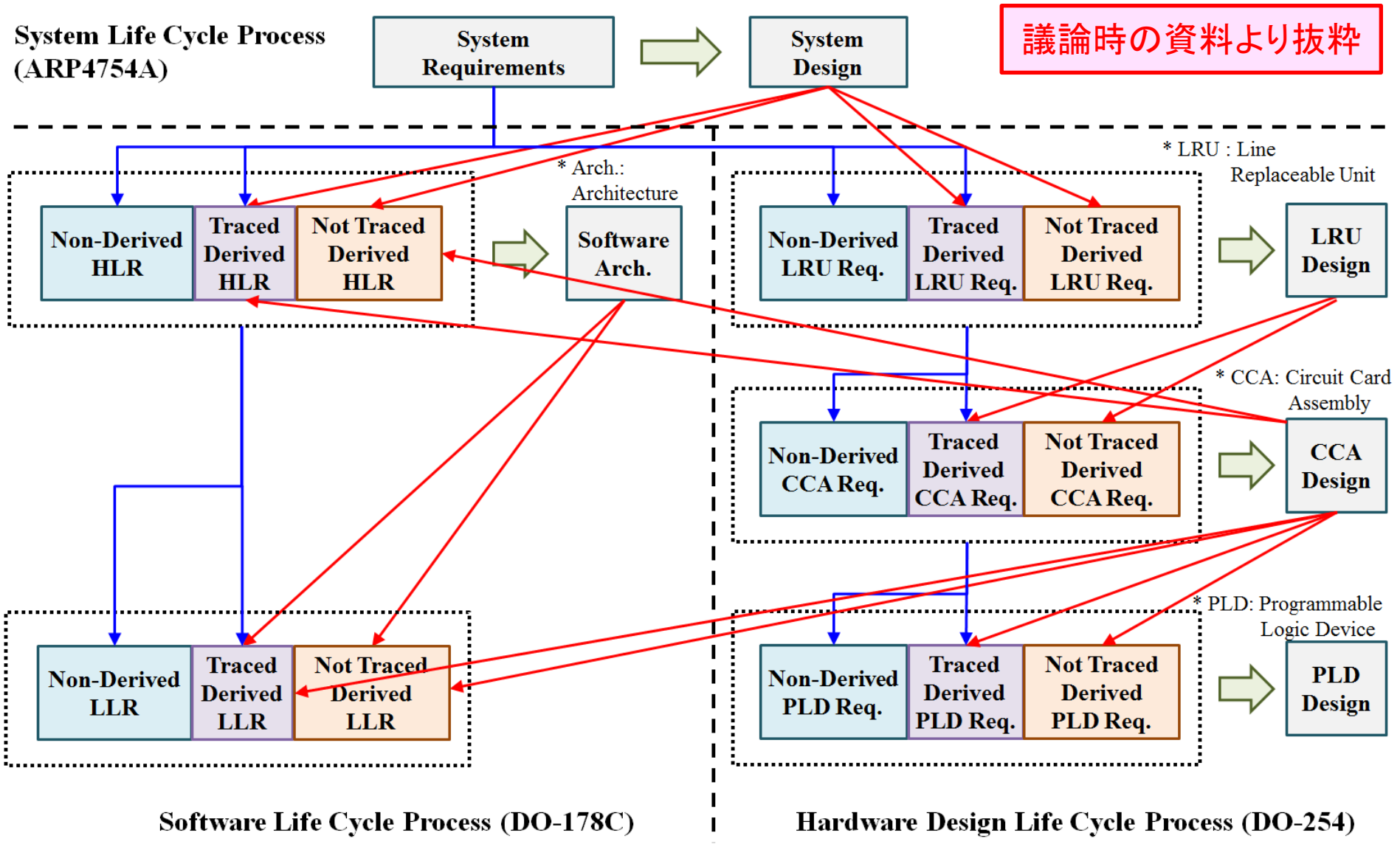
   ＋アンケート結果についての議論／TQAの例
4. **Pseudocodeの利用について**

   ＋アンケート結果についての議論／TQAの例
5. **その他**

   ＋アンケート結果についての議論

※ 第1回 研究会におけるアンケートにて、「Derived Requirements」についてのさらなる議論を望む要望がいくつかあったため、議論用資料を用意した。

1.4 Derived Requirementsの作成の全体像 (3/5)



6.1.2.2 REMH §2.9 “DEFINE THE SOFTWARE REQUIREMNENTS”

議論時の資料より抜粋

図 6-3に、Software Requirements（SOFT）を3つの部分（IN’、REQ’、OUT’）に置き換えたものを示す。

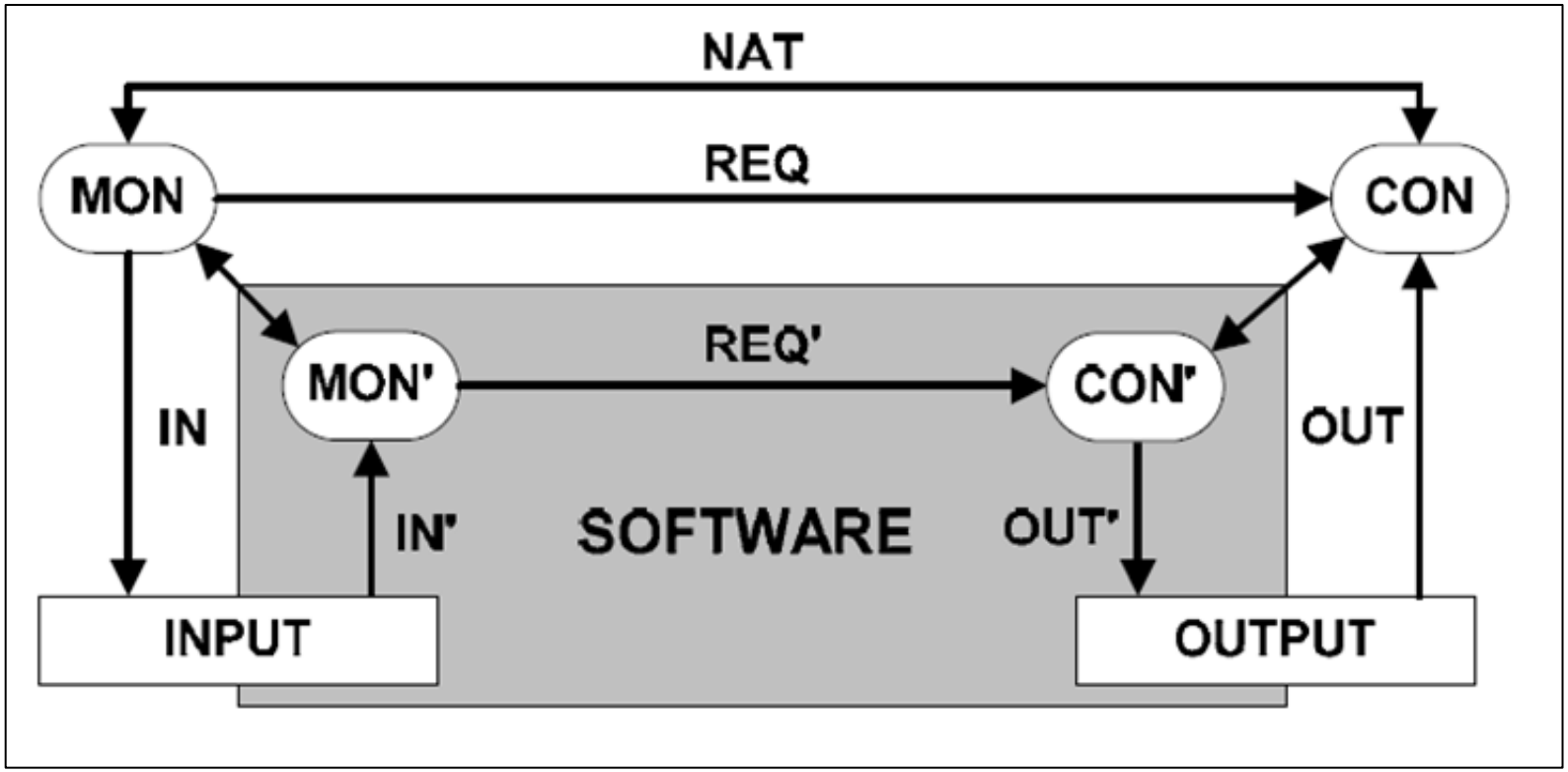


図 6-3：Extended Software Requirements（REMH page 55）

3. イニシアティブの活動の詳細

3.1 教育プログラムの提供
3.2 DO-178C技術テーマ議論
3.3 認証支援データの提供
3.4 コンサルティング実施
3.5 支援ツール整備

3.3 認証支援データの提供(1/4)

認証支援データとして以下の4種類のデータを整備、提供することによりソフトウェア認証のハードルを下げる取組みである。

- 計画文書のテンプレート
- 設計文書のテンプレート
- 検証用チェックリスト
- 標準ライブラリ

本活動はJAXA主導の装備品開発プロジェクトにおける実際の製品開発、航空局様によるソフトウェア認証と連携して実施している。

3.3 認証支援データの提供(2/4)

(1) 計画文書のテンプレート

DO-178Cでは計画段階で以下の8種類の計画文書・標準を作成し、認証当局の承認を得ることを求めている。そのテンプレートを提供することにより計画段階でのコスト低減を図るものである。

- Plan for Software Aspects of Certification(PSAC)
- Software Development Plan(SDP)
- Software Verification Plan(SVP)
- Software Configuration Management Plan(SCMP)
- Software Quality Assurance Plan(SQAP)
- Software Requirements Standards(SRS)
- Software Design Standards(SDS)
- Software Code Standards(SCS)

3.3 認証支援データの提供(3/4)

(2) 設計文書のテンプレート

ソフトウェア設計の段階で必要となる設計文書のテンプレートを提供することによりコスト低減を図るものである。

- Software Requirements Data
- Software Design Description　　等

(3) 検証用チェックリスト

DO-178Cの大きな特徴のひとつとして検証プロセスがある。計画、設計、テストの各段階が終了時点でその結果を検証しその正しさを確認するものである。その検証の際に用いるチェックリストを提供する。

- 計画文書のレビューチェックリスト
- 要求設計結果のレビューチェックリスト
- 品質保証活動用チェックリスト　　等

3.3 認証支援データの提供(4/4)

(4) 標準ライブラリ

DO-178C準拠データ(認証エビデンス)を備えた標準ライブラリ(ソフトウェアコンポーネント)を開発・提供することにより、装備品開発時のソフトウェア認証のハードルを下げる取組みである。現在、以下の算術関数コンポーネントを標準ライブラリとして整備中である。今後、通信コンポーネント等拡充を計画している。

sin	cos	tan	asin	acos	atan	exp
sqrt	log	atan2	pow	fabs	abs	

これらの標準ライブラリはFAA(アメリカ連邦航空局)が定めているAC20-148(Reusable Software Components (RSC))に準拠して開発を進めており、航空局様により仕様承認として認証頂くことで調整を進めている。

3. イニシアティブの活動の詳細

3.1 教育プログラムの提供
3.2 DO-178C技術テーマ議論
3.3 認証支援データの提供
3.4 コンサルティング実施
3.5 支援ツール整備

3.4 コンサルティング実施(1/2)

各装備品メーカのニーズに合わせてコンサルティングを実施し、直接的に装備品メーカの認証活動をサポートする。またコンサルティングを通して各社のニーズを聴取し、イニシアティブとして共通的に整備すべき機能にフィードバックする。

平成28年度、29年度に経済産業省の事業として装備品メーカに対して個社対応のコンサルティングを実施した。

- 平成28年度　7社に対してのべ32回実施
- 平成29年度　7社に対してのべ12回実施

この2年間で各装備品メーカが抱える課題を克服し、技術レベルの向上を図ることができた。

3.4 コンサルティング実施(2/2)

2年間で実施したコンサルティング内容を以下に示す。

<平成28年度>

- システムサプライヤに必要な認証と取り組み方
- DO-178C成果物評価及びCoding以降のVerificationについて
- DO-178C計画書類のブラッシュアップとツール評価
- DO-331(モデルベース開発)の解説及びディスカッション
- DO-178C詳細テーマ学習
- DO-178C及びDO-331 (モデルベース開発)の研修
- DO-178C教育及びパイロットプログラム成果物評価

<平成29年度>

- システム開発全体の進め方及び航空開発プロセスの確認
- DO-254の学習、DO-178C成果物評価
- DO-178の学習
- DO-178C、DO-254、ARP4754の学習
- DO-333 (形式手法) の解説
- DO-254の学習
- DAL (Development Assurance Level) 解説

3. イニシアティブの活動の詳細

3.1 教育プログラムの提供
3.2 DO-178C技術テーマ議論
3.3 認証支援データの提供
3.4 コンサルティング実施
3.5 支援ツール整備

3.5 支援ツール整備

DO-178C認証取得に必要となる各種支援ツールを整備し試用可能とする。これにより各装備品メーカの開発初期のツール選定を支援し、コスト削減に貢献する。
本整備は平成28年度より愛知県の補助金を利用して実施している。
また、これにより整備したツールを用いて平成29年度にDO-331トレーニング、平成30年度にDO-178Cトレーニングを実施した。

3.5 支援ツール整備

(1) DO-178Cプロセス支援ツール

メーカ	ツール名称	機能概要
LDRA	TBmanager	要求管理(トレーサビリティ管理)
IBM	DOORS	要求管理(トレーサビリティ管理)
LDRA	TBmisra	ソースコード静的解析
MathWorks	Polyspace Bug Finder	ソースコード静的解析
LDRA	TBsecure	ソースコードのCERT C準拠チェック
MathWorks	Polyspace Code Prover	形式手法によるソースコード静的解析
LDRA	LDRA Testbed & TBrun Tool Suite	ソースコードチェック、ソースコード解析、テストカバレッジ、テスト支援
Vector	VectorCAST	ソースコードのテスト、カバレッジ解析
LDRA	TBsafe	MCDCカバレッジ分析
LDRA	Target License Package	ターゲットCPUでのカバレッジ計測
LDRA	Dynamic Data Flow Coverage	Data/Control Couplingの動的解析
Vector	VectorCAST/Coupling	Data/Control Couplingの動的解析
LDRA	TBpublish	解析結果をHTML形式で表示

3.5 支援ツール整備

(2) DO-331(モデルベース)支援ツール

メーカ	ツール名称	機能概要
MathWorks	Embedded Coder	MatlabやSimulinkで作成したモデルからソースコードを自動生成
MathWorks	Simulink Code Inspector	モデルとソースコードの整合性検証
MathWorks	Simulink Design Verifier	作成したモデルを検証
MathWorks	Simulink Test	作成したモデルのシミュレーション実行
MathWorks	Simulink Verification and Validation	モデルのシミュレーションカバレッジを計測
MathWorks	MATLAB Report Generator	解析結果を見やすいHTML形式で表示
MathWorks	Simulink Report Generator	解析結果を見やすいHTML形式で表示
AdaCore	QGEN native toolset	Simulinkモデルからソースコードを自動生成(TQL-1取得)

3.5 支援ツール整備

(3) 安全性解析ツール

メーカ	ツール名称	機能概要
ANSYS	medini analyze Premium	FHA、FTA、FMEA等の安全性解析を統合

(4) トレーニング用機材

メーカ	機材名称	機能概要
多摩川精機	TQA(Throttle Quadrant Assembly)	オートパイロット時にフラコンからの指令によりスロットルを自動制御する

4. 今後の活動

(1) 民間航空機装備品産業の裾野を広げる活動を継続する
- ✓DO-178C、DO-254(初級編)セミナーの実施
- ✓ ARP4754A、ARP4761(初級編)セミナーの実施

(2) より専門性を追求する活動を進める
- ✓実践的トレーニングの実施
- ✓ DO-178C技術テーマ議論の継続

(3) システム領域のメニューを拡充する
- ✓ ARP4754A、ARP4761(初級編)セミナーの実施

(4) 認証支援データの拡充、ブラッシュアップを図る

(5) 海外連携を推進し日本からの発信力を高める

航空機産業の発展を直接的・間接的にサポートする