

航空機開発グローバルプロジェクトリーダー養成講座（略称：GPL 講座）
航空機開発とプロジェクト・マネジメント
——航空機関係テキスト集——

教材 09： 複雑なシステムの開発

ARP4754 OVERVIEW (1/2)

ARP4754とは、

1990年代にソフトウェア開発プロセスDO-178の改訂作業の結果、要求事項として、システムレベルの情報が必要である事が明らかになり、航空機システムの安全性と機能は、システムレベルで多くの判断をしており、この判断プロセスを纏める必要が生じた。この背景からFAAがSAE(Society of Automotive Engineers)に依頼し、航空宇宙向けのガイドラインとして発行したARP(Aerospace Recommended Practices)である。

高度統合化もしくは複合化システムの中でも、特に重要なソフトウェア要素を持つシステムの認証(開発プロセスでの安全性保障)のガイドとして作成。

Initial Release(1996-11) ; “Certification Considerations for Highly-Integrated or Complex Aircraft Systems”

出典: SAE ARP4754 REV.NC

ARP4754 OVERVIEW (2/2)

ARP4754は2010年に改定したがタイトルまで変えている。

Initial Release(1996-11) ; “Certification Considerations for Highly-Integrated or Complex Aircraft Systems”

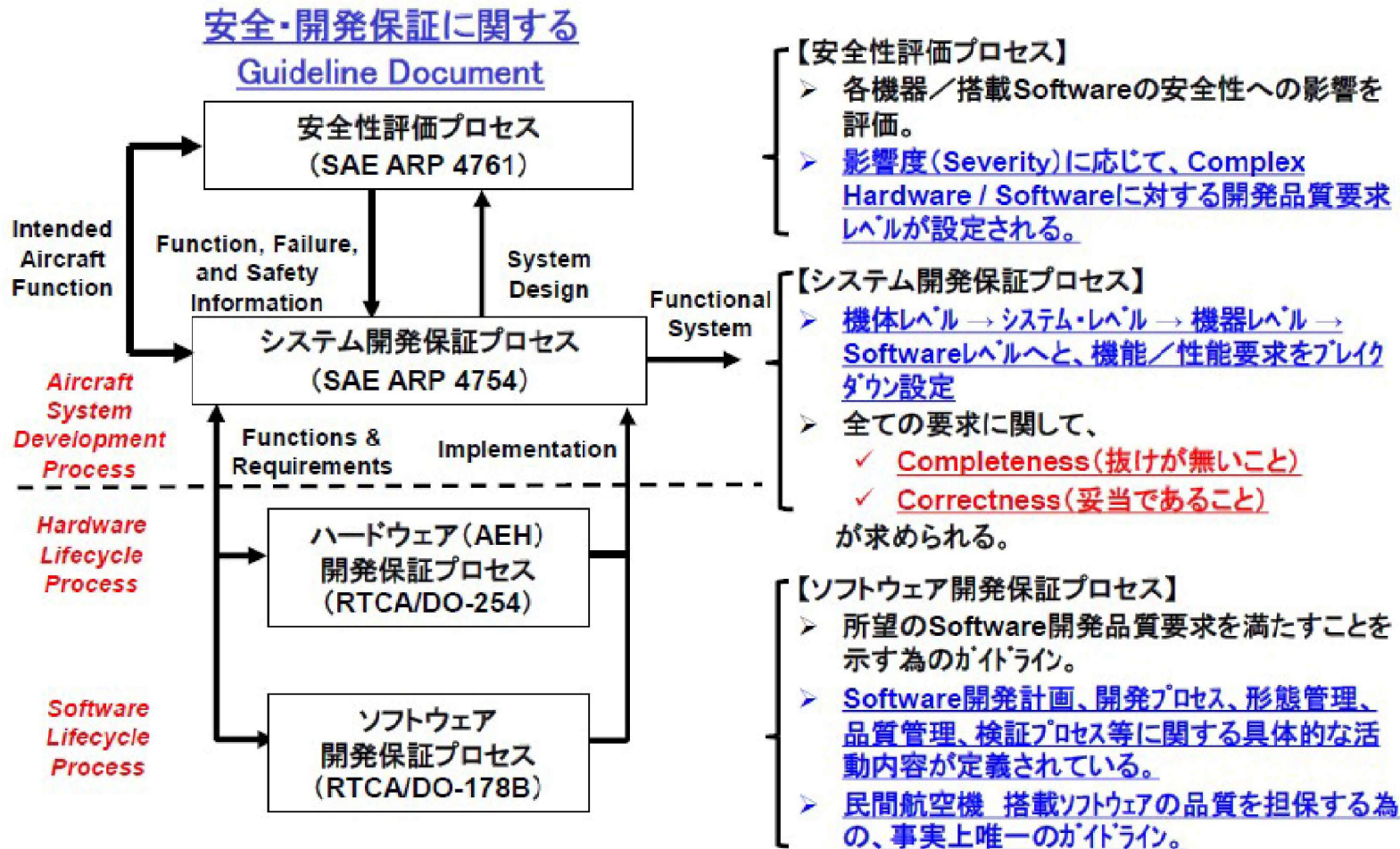
Rev.A(2010-12) ;
“Guidelines for Development of Civil Aircraft and Systems”

基本的な考え方は変わっていないが、高度統合・複合化システムを開発するには、機体レベルのシステム開発から検討する事を求めており、タイトルから意図を明確化した。

民間航空機に携わる海外の多くの企業は、ARP4754を適用すると言わないまでもARPに従って活動しており、システム開発のガイドラインとして定着している。

出典: SAE ARP4754 REV.A

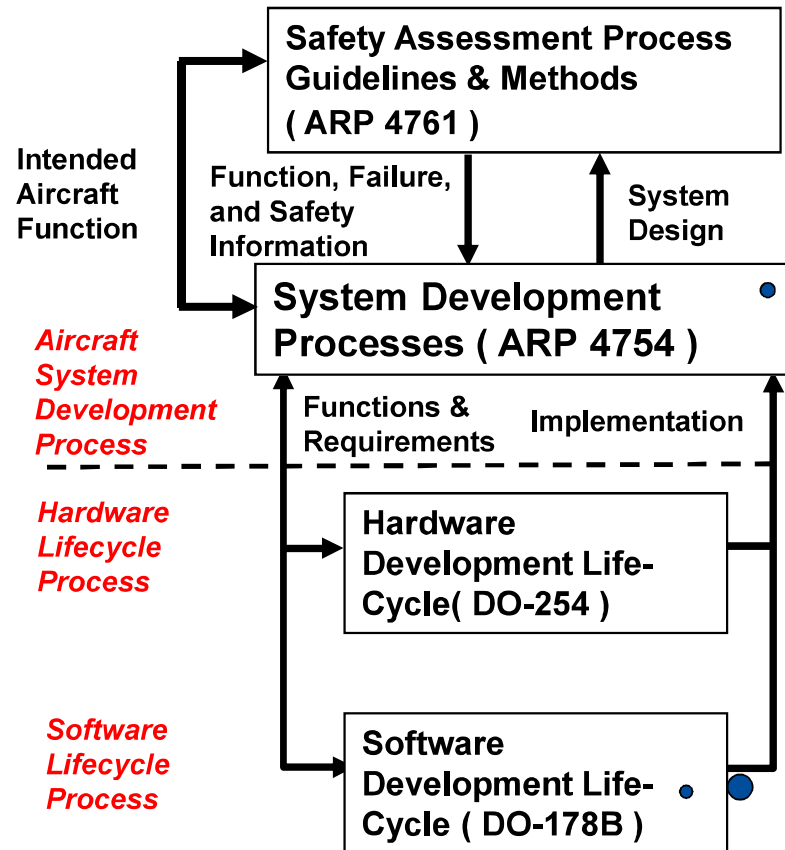
安全性・開発保証プロセス (1/2)



出典: SAE ARP4754 REV.A

安全性・開発保証プロセス (2/2)

安全性／開発保証に関する Guideline Document



Softwareバグの大部分は、
Software開発そのものよりも、
上位要求の設定／検証の不備に
より生じる事が多い。

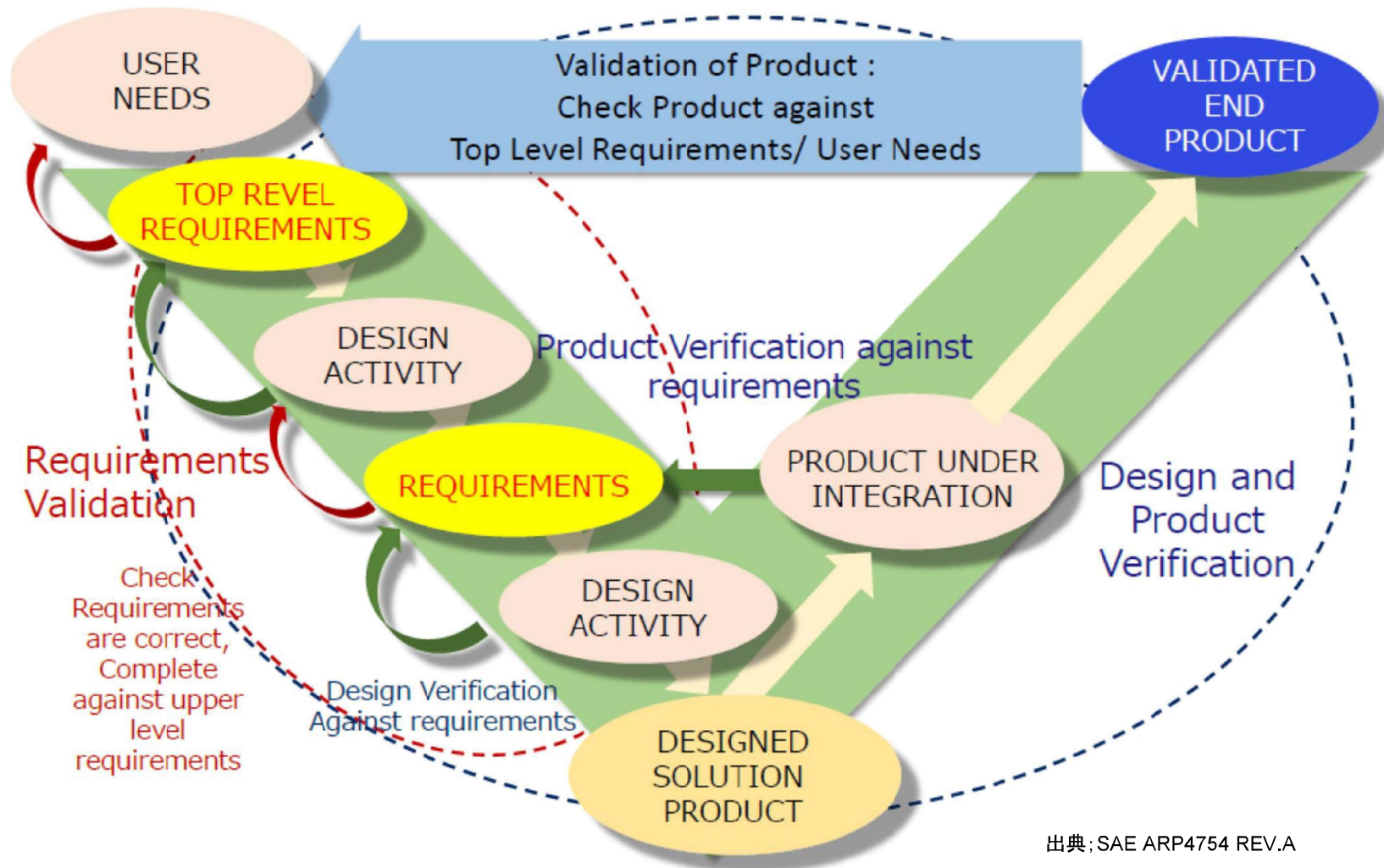
1996年
Arian5打上失敗

ソフトウェア不良による航空機の
不安全状態を防止するには、
ソフトウェアに対して適切な設計要求を
設定する事が重要。

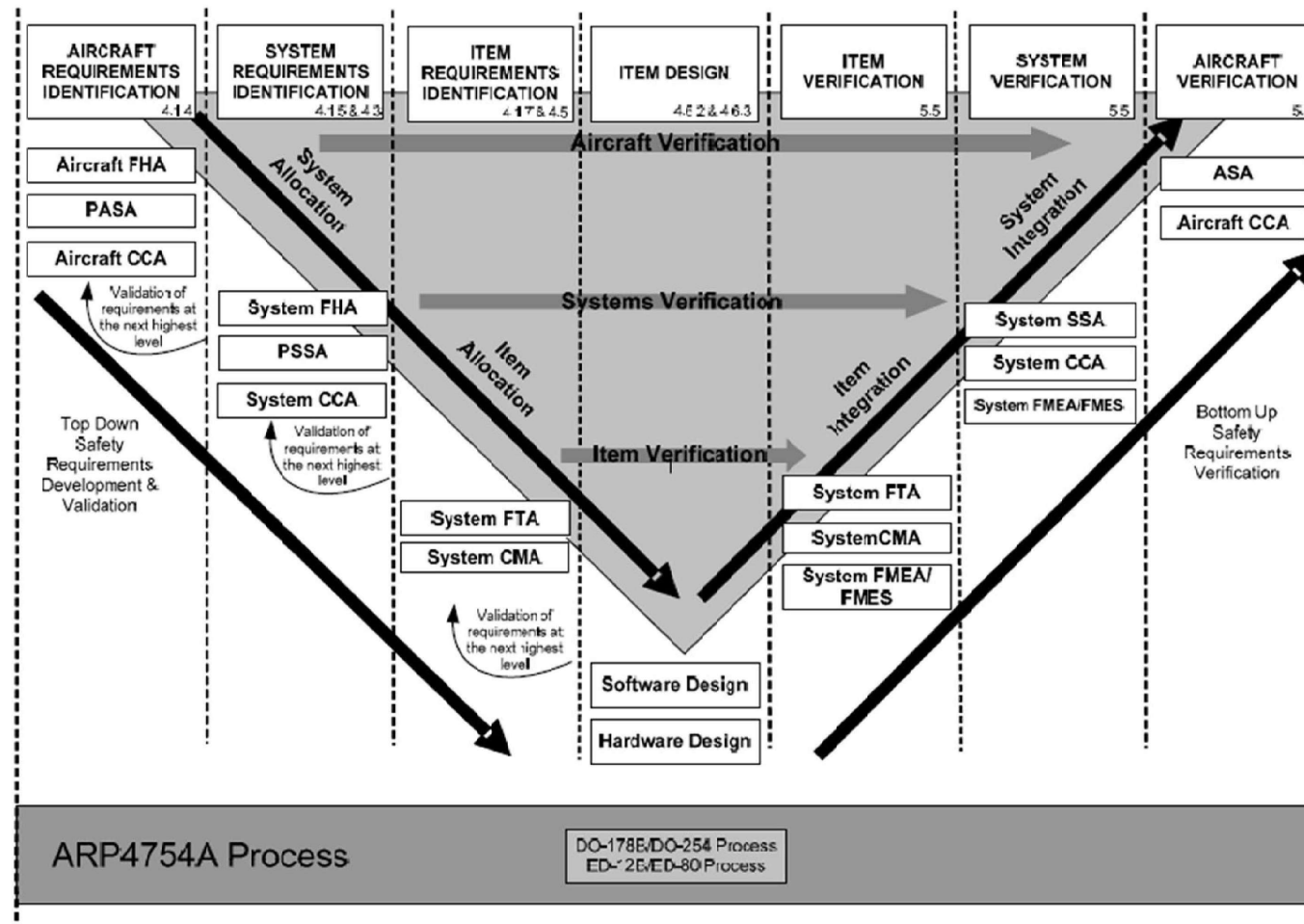
設定された設計要求に従い、適切な
プロセス管理を通じて高品質の
ソフトウェアが開発／検証されている
事を示すプロセス。

出典: Nuseibeh, Bashar : Arian 5, Who Dunnit ?, IEEE Software, May-June 1997, Volume: 14, Issue: 3.

SEC.4 AIRCRAFT AND SYSTEM DEVELOPMENT PROCESS



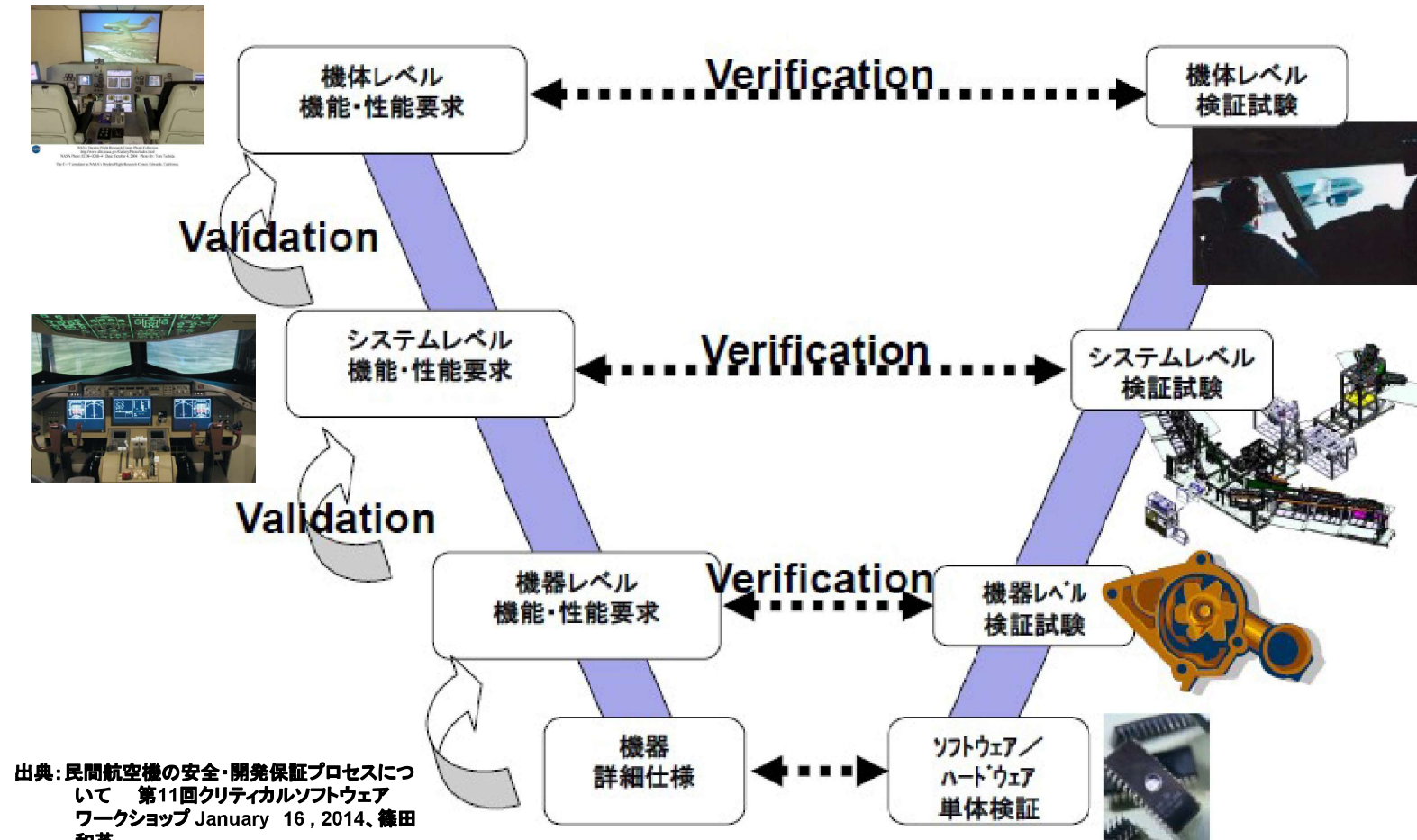
SEC.4 AIRCRAFT AND SYSTEM DEVELOPMENT PROCESS



出典: SAE ARP4754 REV.A

FIGURE 5 - INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES

開発保証プロセス



出典: 民間航空機の安全・開発保証プロセスについて 第11回クリティカルソフトウェアワークショップ January 16, 2014、篠田和英

機体システムのレベルにおいて機能・性能の検証を実施

開発保証プロセス

➤ フライトシミュレータを用いたValidation

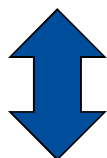
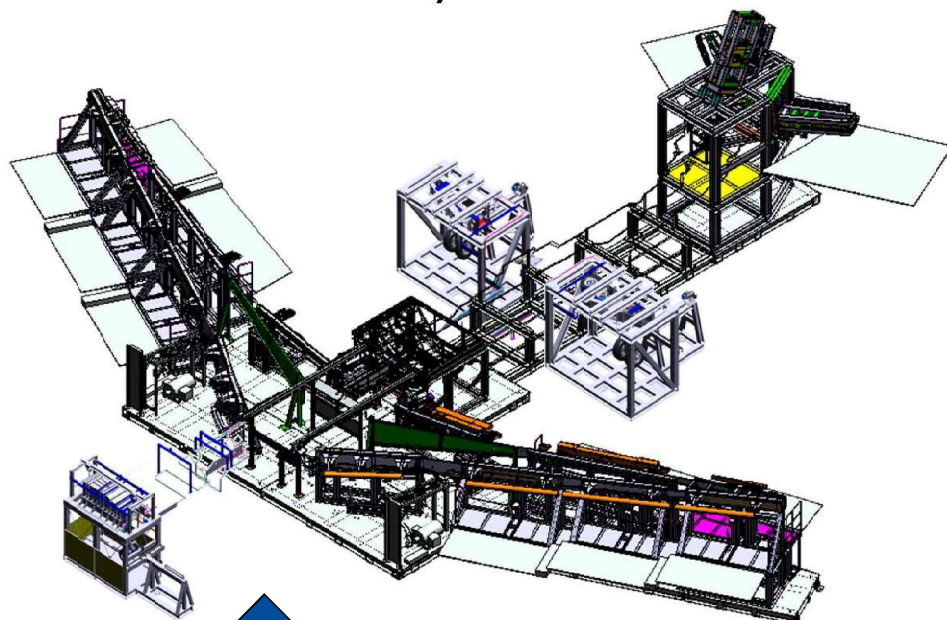
- ✓ フライトシミュレータ装置を準備のうえ、機体の操縦性を開発初期段階から評価
- ✓ 通常、Fixed Based(地上固定)の汎用シミュレータを準備(Motion付(可動型)シミュレータを用いることもある)
→ Motion有無による操縦性の違い？
- ✓ 数名の(社内)Test Pilotとともに評価／設計修正作業を繰り返し実施
- ✓ エンジン、油圧、電源、舵面等の故障状態を模擬した操縦性評価試験も実施
- ✓ 設計が進展した段階から、エアラインPilot／社外Test Pilotなどの評価を受け、サンプル数を増やしていく
- ✓ Flight Testに向けた、Test Pilotの操縦習熟のためにも活用される

出典:Pilot-Induced Oscillation Research : Status
at the End of the Century, NASA Dryden
Flight Research Center



開発保証プロセス

➤ Iron Bird (操縦RIG)を用いたVerification



Data Interface



Flight Deck
Connected with
Iron Bird

操縦関連システムを機体に搭載する前に
地上にて組み合わせ、機能／性能を検証

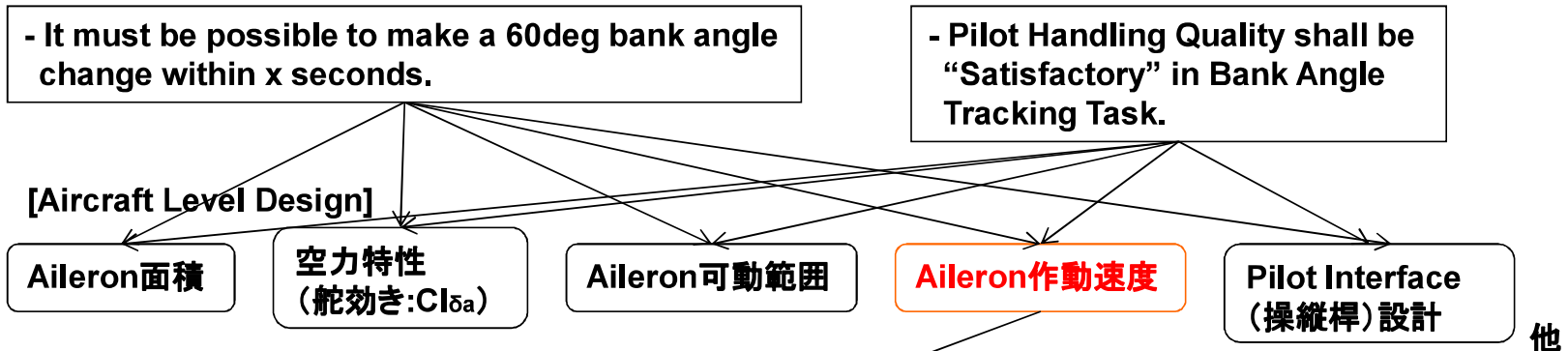
- ✓ Primary Flight Control
(Elevator, Aileron Rudder, Spoiler)
- ✓ Secondary Flight Control
(Flap, Slat, Stabilizer)
- ✓ Hydraulic
- ✓ Gear (含 Brake)
- ✓ Pilot操縦装置

操縦システム全体の機能／性能を
事前に地上で確認

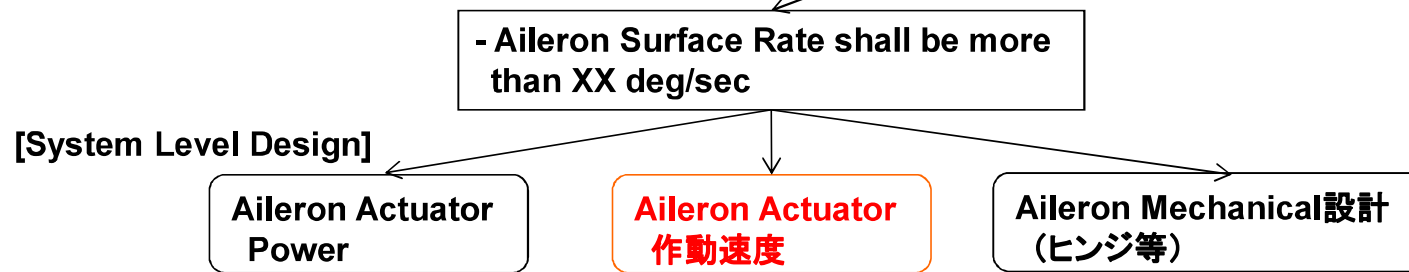
出典:MRJ Fly-By-Wire Development - Flying into the future -
SICE2013基調講演 (佐倉 潔)

開発保証プロセス

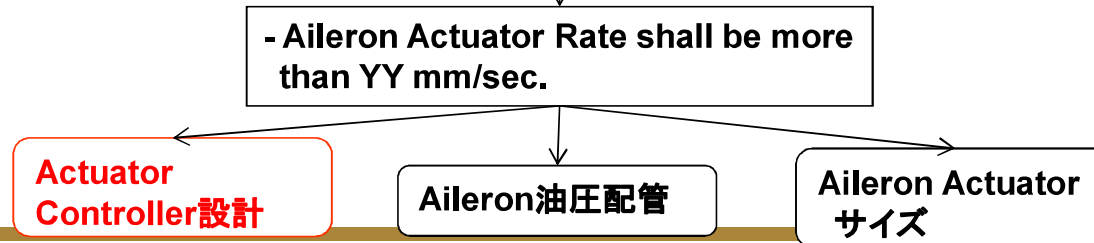
➤ Aircraft Level Requirementの例



➤ System Level Requirementの例



➤ Sub-System Level Requirementの例



SEC.5 INTEGRAL PROCESS

SEC.5.1 SAFETY ASSESSMENT

- ◎ 開発保証プロセスに従って、安全性評価が求められている。
Aircraftレベル／システムレベルでのFHAを実施しFC(Failure Condition)の設定が、その後の検証の起点となり重要である。

FHA ; Functional Hazard Assessment

- the effects of the Failure Condition(s)
- Classification of each Failure Condition (i.e., Catastrophic, Hazardous/Severe-Major, Major, Minor, or No Safety Effect)

PASA/PSSA ;

Preliminary Aircraft Safety Assessment /
Preliminary System Safety Assessment

ASA/SSA ; Aircraft Safety Assessment /
System Safety Assessment

CCA ; Common Cause Analysis

出典 ; SAE ARP4754 REV.A

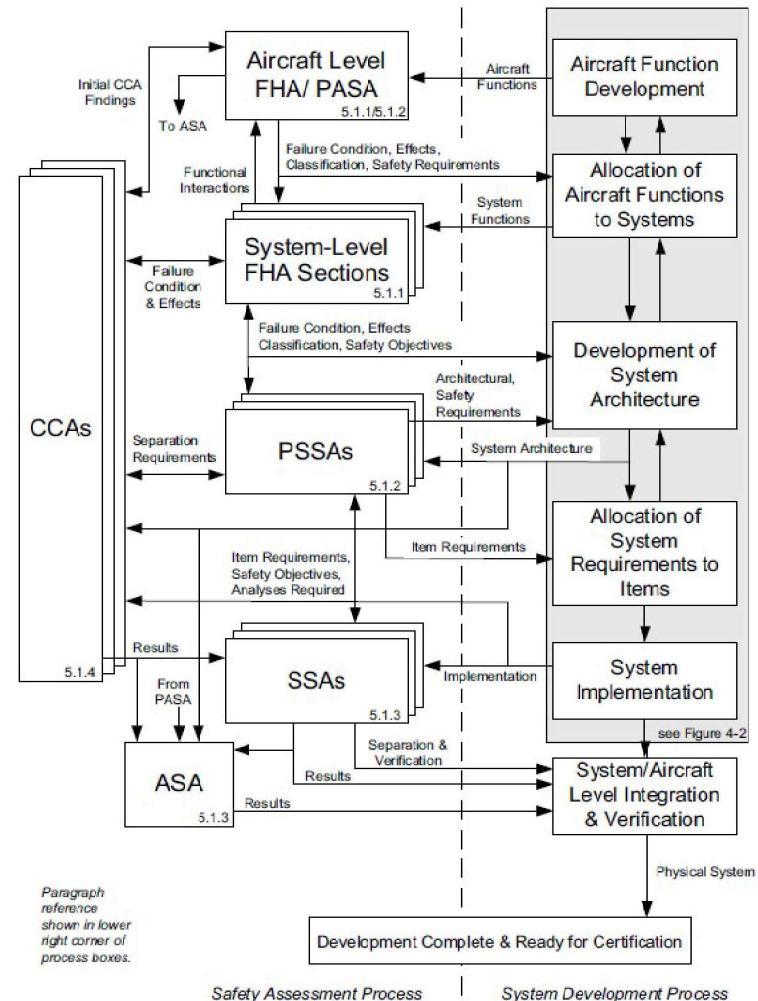
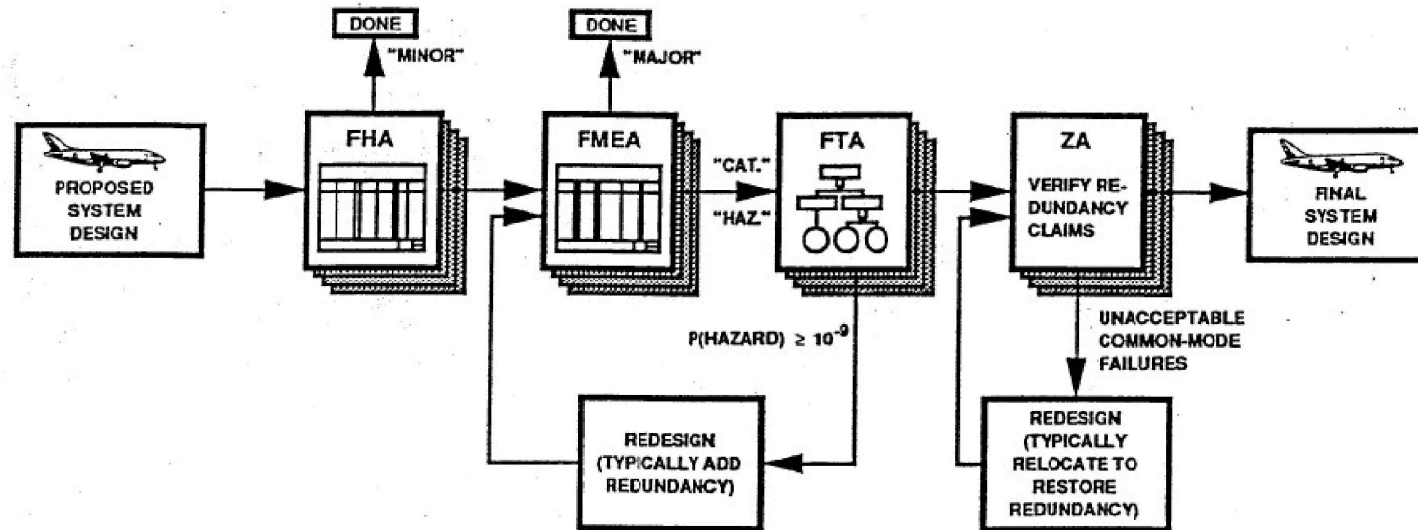


FIGURE 7 - SAFETY ASSESSMENT PROCESS MODEL

SEC.5 INTEGRAL PROCESS

SEC.5.1 SAFETY ASSESSMENT



- **FHA : Functional Hazard Analysis**
 - ✓ 機能上の異常事象を抽出して、機体に及ぼす影響と致命度を評価し、信頼度要求を設定
- **FMEA : Failure Mode and Effect Analysis**
 - ✓ 構成要素の故障モードを洗い出し、機体への影響を評価(ボトムアップ手法)
- **FTA : Fault Tree Analysis**
 - ✓ FHA/FMEAで抽出された異常事象のうち、致命度が“Hazardous”以上のアイテムに対し Fault Treeを作成し、発生確率を算出(トップダウン手法)
- **ZA : Zonal Analysis 【CCA : Common Cause Analysisの一部】**
 - ✓ 1つの要因により複数の機能が同時に喪失しないことを確認

出典 : Quantifying the Pilot's Contribution to Flight Safety Page, Gillette, Hodgkinson, Preston

SEC.5.1 SAFETY ASSESSMENT

SEC.5.1.4 CCA

機能、システムまたは品目間で独立性を求めている場合がある。このような独立性を確認すると共に、独立性が失われた状態が許容できることを保証する必要がある。

Common Cause Analysis(CCA)は次の3タイプの解析に細分化されている。

- a. Particular Risks Analysis ; PRA
- b. Common Mode Analysis ; CMA
- c. Zonal Safety Analysis ; ZSA

例) (a) Particular Risk Analysis (PRA)

機体の広い範囲、又はシステムや機器間に跨って影響を及ぼすParticular Riskの影響のために、Catastrophic/Hazardous に繋がる事象が発生しないことを評価する。

(参考) ARP4761では代表的なParticular Risk を以下の14件の項目が記載されている。

- a. Fire b. High energy devices c. High pressure bottles d. High Pressure Air Duct Rupture e. High Temperature Air Duct Leakage f. Leaking fluids(Fuel, Hydraulic, Battery acid, Water) g. Hail, ice, snow h. Bird strike i. Tire burst, flailing tread j. Wheel rim release k. Lightning strike l. High Intensity Radiated Fields m. Flailing shafts n. Bulkhead rupture

また、Survivability of Systems(Terrorism Threat)の検討も求められている。

SEC.5.1 SAFETY ASSESSMENT

SEC.5.1.4 CCA

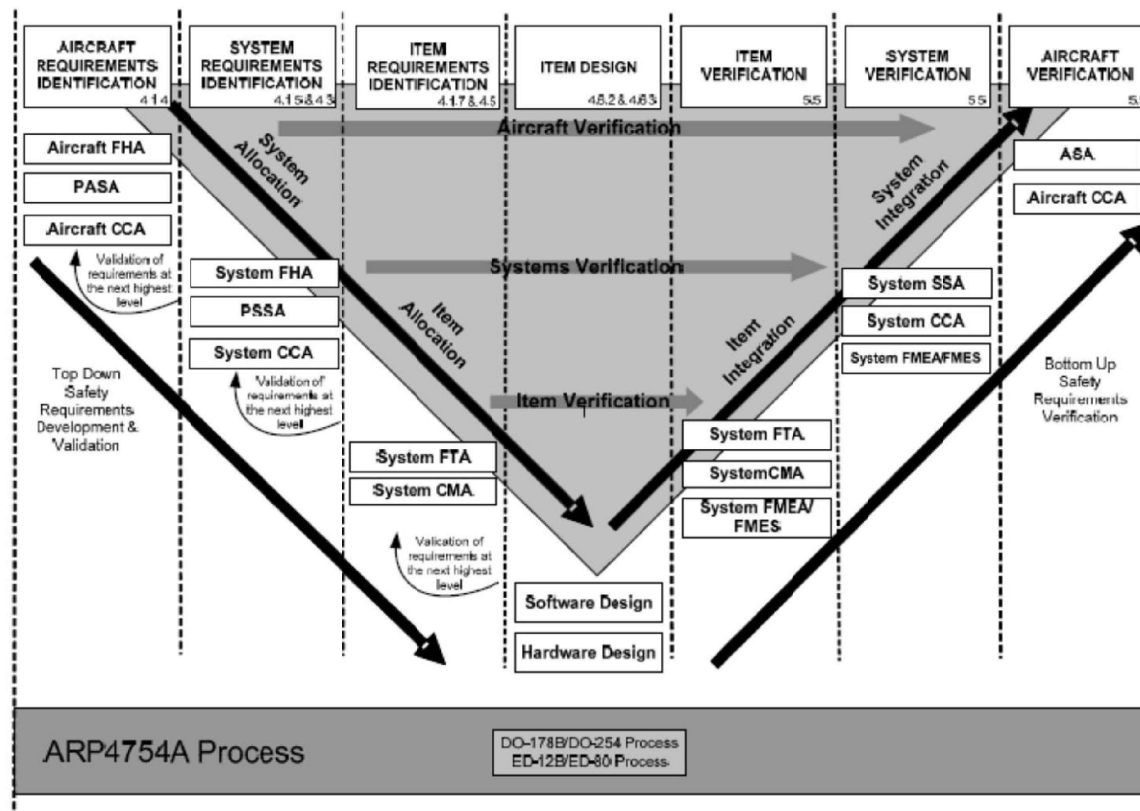
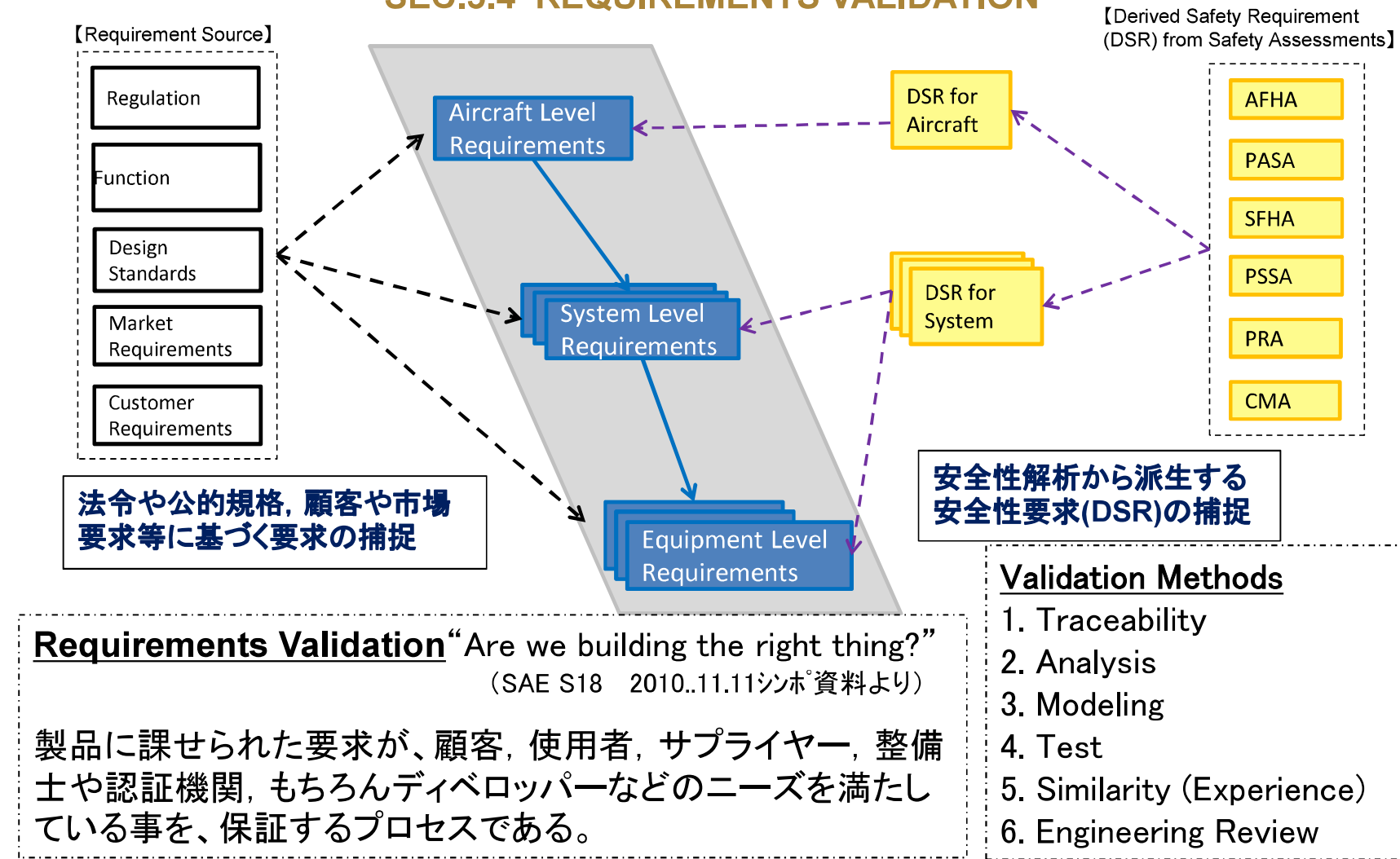


FIGURE 5 - INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES

ARP4754A 5.1.4 Common Cause Analysis

- a. Particular Risks Analysis
 - b. Common Mode Analysis
 - c. Zonal Safety Analysis
- These analyses may be performed at any stage of the design process. Obviously, the most cost-effective time is early in the design process because of the potential influence on system architecture and installation. However, confirmation may not always be feasible until implementation is complete.

SEC.5.3 REQUIREMENTS CAPTURE SEC.5.4 REQUIREMENTS VALIDATION



VALIDATION – CORRECTNESS AND COMPLETENESS

✓ Validation → 要求が**妥当**であることを確認する行為

✓ **妥当**とは？

→ 要求がcorrectであり、かつcompleteであること。

✓ 「正確性Correctness」

(1) 1文に1要求が述べられているか？

(2) 曖昧さが無く明確な要求か？

(3) 検証(Verification)可能な要求か？

(4) 安全性解析からの派生要求

(Derived Safety Requirement)を

正しく反映しているか？

✓ 「網羅性Completeness」

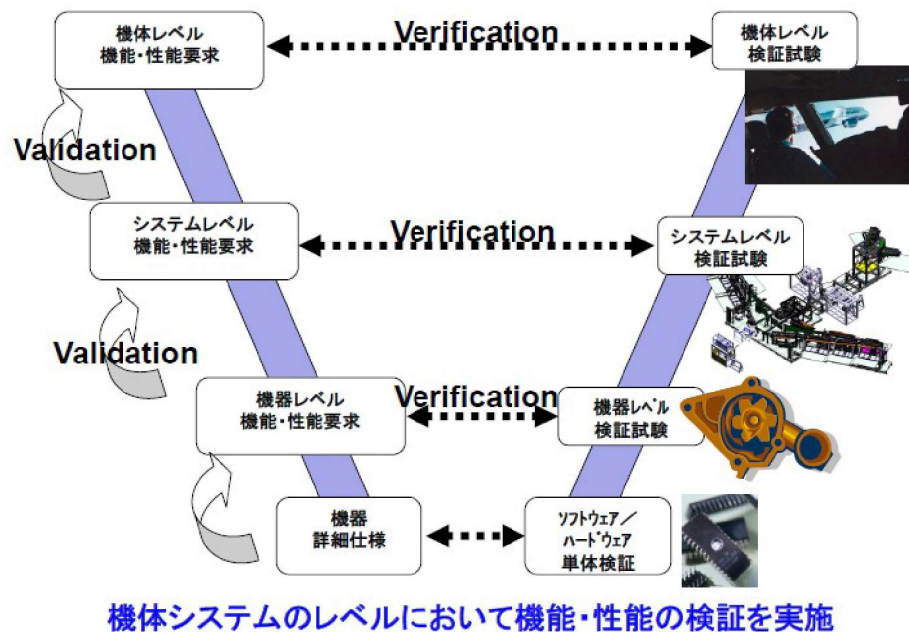
(1) 本要求の実現により上位要求を達成できるか？

(2) 規定／ガイドライン／スタンダード等の一般的
に必要とされる内容をカバーしているか？

(3) 実現すべき機能をハードウェア／ソフトウェア
等に明確に割り付けているか？

(4) 必要な全てのインターフェース要求は定義さ
れているか？

SEC.5.5 IMPLEMENTATION VERIFICATION



Implementation Verification

“Have we built the right thing?”
(SAE S18 2010.11.11シンポ資料より)

実装状態で製品が、課せられた
要求に適合している事を、確認
するプロセスである。

Verification Methods

1. Inspection or Review
2. Analysis
3. Test or Demonstration
4. Service Experience

VERIFICATION METHOD (例)

ベリフィケーション方法	内容
(1) 検査及びレビュー	
検査及びレビュー	文書及び図面のレビュー, 又は, ハードウェア及びソフトウェアの目視検査により要求への適合性を確認する。
(2) 解析及びモデリング	
解析及びモデリング	物理法則に基づき, 検討対象の挙動等を詳細に検討することによって要求への適合性を示す手法。 机上シミュレーションもこの分類に含める。
(3) 試験又は実証	
システム単体地上試験 (コンポーネント試験)	材料, 部品, 装備品などについて, 装備品・部品の設計及び材料が要求仕様に合致していることを確認する手法。装備品各部のシステムの性能を確認するコンポーネント試験, 耐久性を試験する部分構造試験などが存在する。全機地上試験, リグ試験, PS試験で行えない試験を全て行う。
リグ試験	検証対象を実機と同等の状態におくために, 対象の一部を模擬して試験することで, 要求への適合性を示す手法。複数のシステムを接続した地上試験が可能となる。
パイロット シミュレータ	実機の挙動を模擬した特定の型式の航空機シミュレータをパイロットが操縦することで, 要求への適合性を示す手法。パイロットが操縦しないものは解析, 又はリグ試験に分類する。
全機地上試験	実機(又は実機と同等の状態においた検証対象)を試験することで, 要求への適合性を示す手法。
飛行試験	実機を飛行させることによって, 要求への適合性を示す手法。タキシング, 離着陸ロールもこの分類に含める。ただし, 飛行試験では飛行条件を網羅的に変化させることは困難であり, かつ実施可能な試験ケース数に上限があるため, 解析やシミュレーションによる代表試験ポイントの選定が必要となる。
(4) シミラリティ	
シミラリティ又はサービス エクスぺリエンス	他機にて十分な運用実績があり, 解決に至っていない重大な故障が起こっていないことが実証できる場合は, シミラリティ又はサービス エクスぺリエンスによるベリフィケーションが認められることもある。

安全性解析を基にした検証レベル分け(PRACTICAL APPROACH)

TABLE 7 - VERIFICATION METHODS AND DATA

Methods and Data (see paragraphs 5.5.5 and 5.5.6)	Development Assurance Level			
	A and B	C	D	E
Verification Matrix	R	R	A	N
Verification Plan	R	R	A	N
Verification Procedures	R	R	A	N
Verification Summary	R	R	A	N
ASA/SSA (note 3)	R	R	A	N
Inspection, Review, Analysis, or Test (note 1)	R (Test and one or more of others)	R (One or more)	A	N (note 2)
Test, unintended function	R	A	A	N
Service Experience	A	A	A	A

Note: R - Recommended for certification, A - As negotiated for certification, N - Not required for certification

NOTE 1: These methods provide similar degrees of verification. The selection of which methods will be most useful may depend on the specific system architecture or the specific function(s) implemented. DO-178B/ED-12B and DO-254/ED-80 define applicable tests for software and electronic hardware depending on the IDAL.

NOTE 2: As necessary to show installation and environmental compatibility.

出典: SAE ARP4754 REV.A

⇒ 上記朱記; DAL“A&B”については、Testだけでなく、他に何らかの方法で Verificationする事を求めている。

SEC.5 INTEGRAL PROCESS

SEC.5.7 PROCESS ASSURANCE

プロセス保証の目的

- a. 必要な計画が策定され、これらが、航空機、システム及びアイテム開発での全ての局面においても維持されるようにする。
- b. 開発活動と開発プロセスがこれらの計画に従っておこなわれるようにする。
- c. 活動がこれらの計画に従うものであることのエビデンスを確立する。

プロジェクト計画のレビュー

- a. 該当する手続きや業務が文書化されていること。
- b. 定められたコミュニケーション方法が、該当するプロセスと影響を受ける要員の間の情報交換がタイムリーに実施できるものであること。
- c. プロセス、スケジュール、又は技術的な変更による計画の更新をおこなう手続きが設定されていること。
- d. 計画の更新は、適正にトラックでき管理されていること。

プロセス保証のエビデンス

- a. 日付があり認証されたプロジェクト計画
- b. プランで求められている報告、評価基準、検討概要
- c. 設計, Verification, Validation, 形態管理, 適合証明の各活動での実際のデータ
- d. プロセス保証レビューを行った時の確認書（終了チェックリスト、議事録など）