Automotive Software Tester の紹介

2019/10/4

JSTQB CTFL-AuT翻訳WG

1章：イントロ

Learning Objective
AUTFL-1.1.1 多様化するプロジェクト目標やプロダクトの複雑さの増大により発生する自動車プロダクト開発の課題を説明し、例をあげる。（K2）
AUTFL-1.2.1 時間、コスト、品質、プロジェクト/プロダクトリスクなどの標準により影響されるプロジェクトの側面を想起する。（K1）
AUTFL-1.3.1 ISO/IEC 24748-1 [1]で定義されているシステムライフサイクルの6つの一般的なフェーズを想起する。（K1）
AUTFL-1.4.1 リリースプロセスにおけるテスト担当者としての貢献と協力を想起する。（K1）

1章：イントロ

Learning Objective概略
AUTFL-1.1.1 自動車プロダクト開発の課題（K2）
AUTFL-1.2.1 標準（standards）により影響を受けるプロジェクトの側面（K1）
AUTFL-1.3.1 ISO/IEC 24748-1 [1]で定義されているシステムライフサイクルのフェーズ（K1）
AUTFL-1.4.1 リリースプロセスにおけるテスト担当者としての貢献（K1）

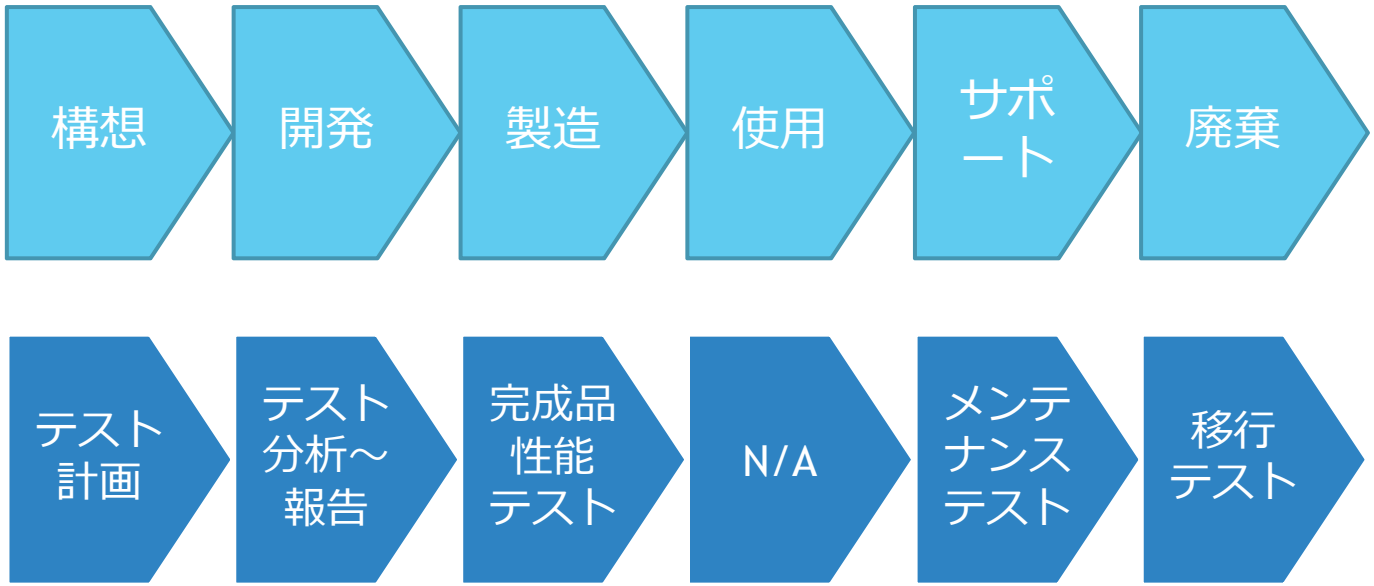
テストは条件次第

- 7原則の一つ
- そのため、車におけるテストを語る、ということ

Standardsに影響を受ける

- 各種目的のために標準（Standards）を参照する
- 紹介するのはISO26262、Automotive SPICE、AUTOSAR（2章参照）

システムライフサイクルのフェーズ



リリースプロセスへの関与

- テスト済みアイテムと性能特性
- 既知の欠陥
- プロダクトメトリクス
- リリース推奨の情報

2章：標準（Standards）

章構成
2.1章　ASPICE
2.2章　ISO26262
2.3章　AUTOSAR
2.4章　各標準の比較

2.1章：ASPICE

Learning Objective
AUTFL-2.1.1.1 Automotive SPICE（ASPICE）の2つの座標軸を想起する。（K1）
AUTFL-2.1.1.2 ASPICEの3つのプロセスカテゴリーと8つのプロセス群を想起する[情報提供]。（K1）
AUTFL-2.1.1.3 ASPICEの能力レベル0～3を説明する。（K2）
AUTFL-2.1.2.1 ASPICEの5つのテスト関連プロセスの目的を想起する。（K1）
AUTFL-2.1.2.2 テストの観点から、ASPICEの4つの評定尺度と能力指標の意味を説明する。（K2）
AUTFL-2.1.2.3 リグレッションテスト戦略を含むテスト戦略に関するASPICEの要件を説明する。（K2）
AUTFL-2.1.2.4 テスト文書に関するASPICEの要件を想起する。（K1）
AUTFL-2.1.2.5 ユニット検証用の検証戦略（テスト戦略との対比）と基準を設計する。（K3）
AUTFL-2.1.2.6 テストの観点からASPICEとは異なるトレーサビリティ要件を説明する。（K2）

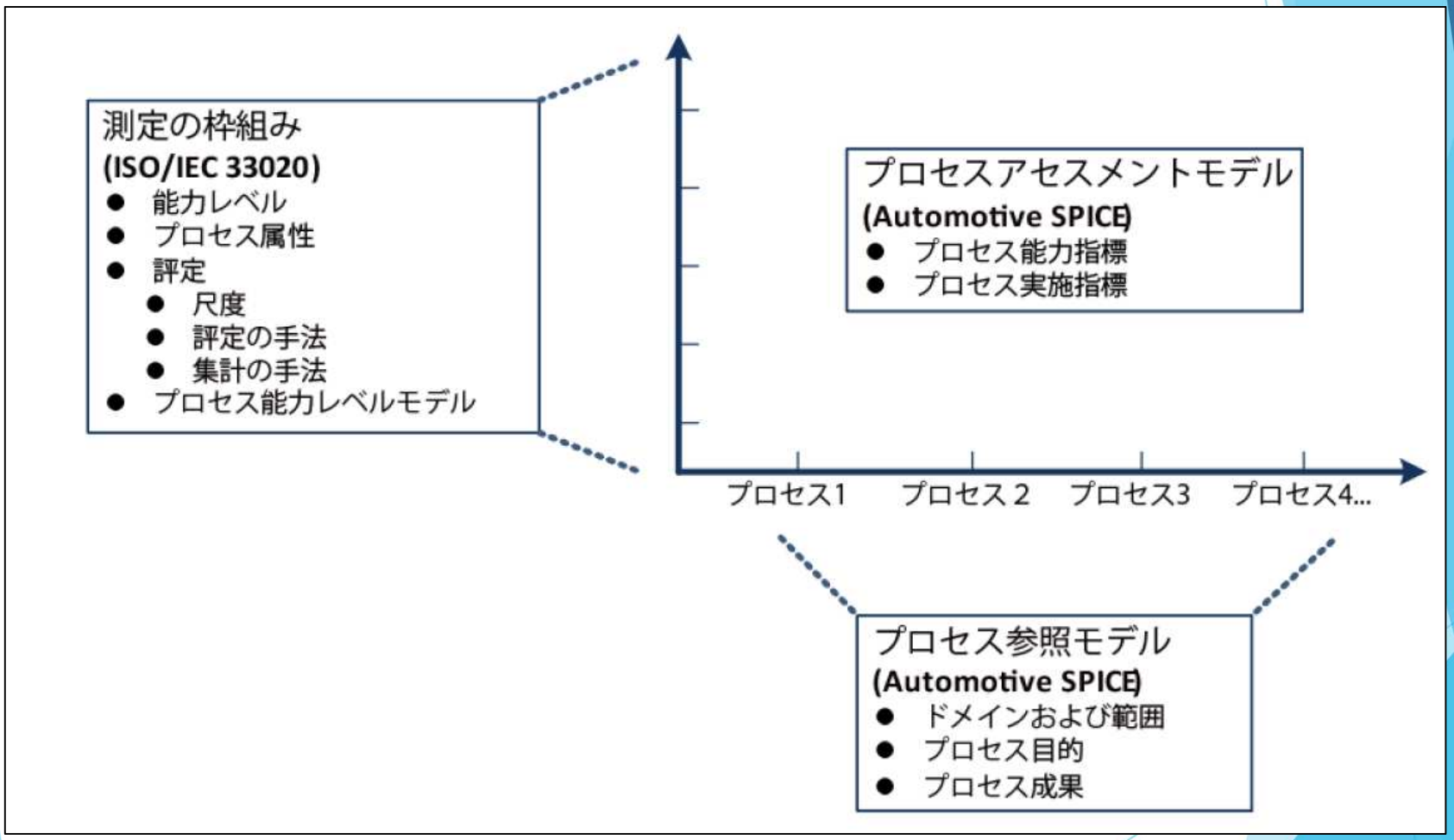
2.1章：ASPICE

Learning Objective概略
AUTFL-2.1.1.1 ASPICEの2つの座標軸（K1）
AUTFL-2.1.1.2 ASPICEのプロセスカテゴリーとプロセス群（K1）
AUTFL-2.1.1.3 ASPICEの能力レベル（K2）
AUTFL-2.1.2.1 ASPICEのテスト関連プロセス（K1）
AUTFL-2.1.2.2 テストの観点からのASPICEの評定尺度と能力指標の意味（K2）
AUTFL-2.1.2.3 テスト戦略に関するASPICEの要件（K2）
AUTFL-2.1.2.4 テスト文書に関するASPICEの要件（K1）
AUTFL-2.1.2.5 ユニット検証の検証戦略（K3）
AUTFL-2.1.2.6 テストの観点からのトレーサビリティ要件（K2）

ASPICEの座標軸

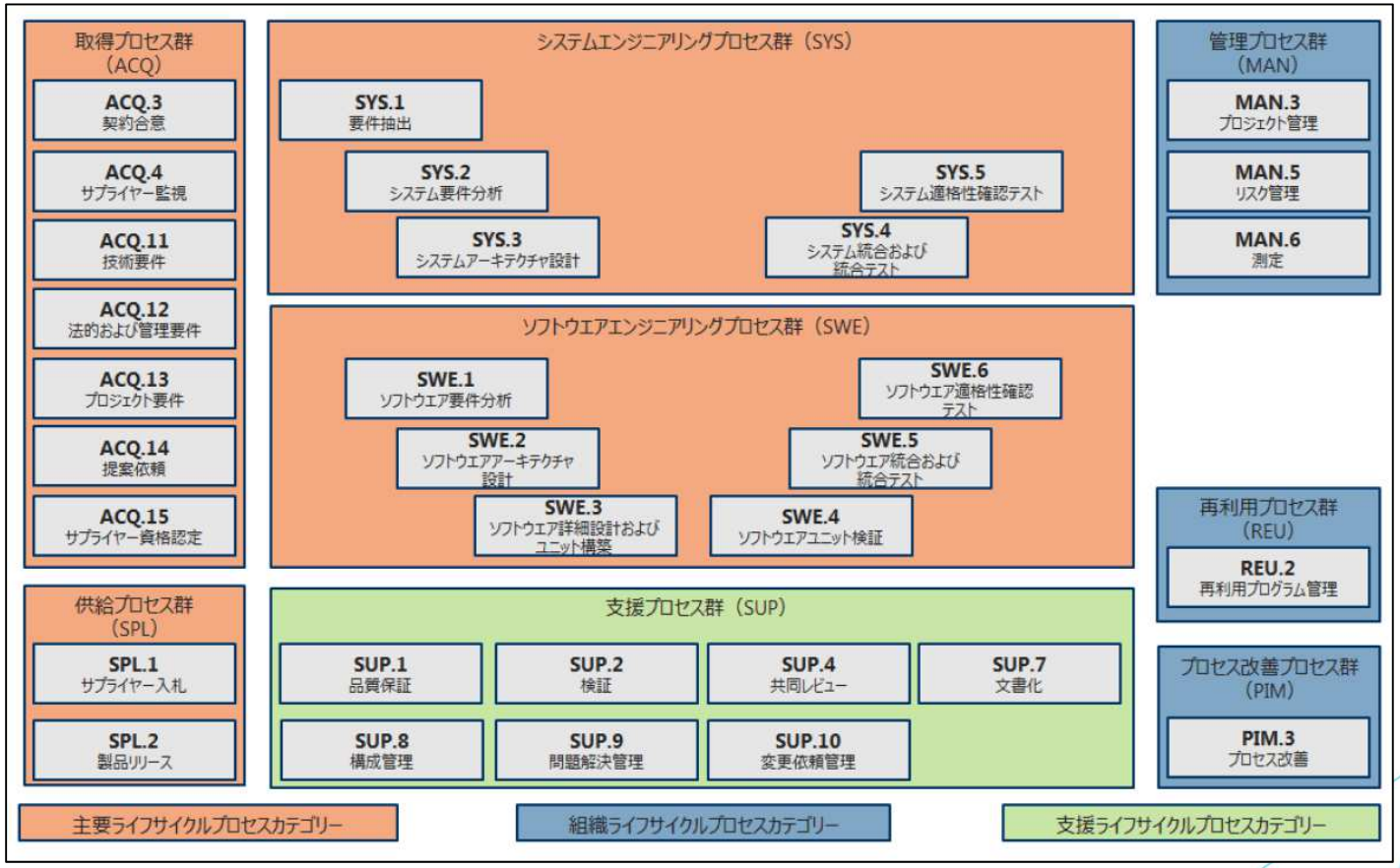
- プロセス座標
  - ソフトウェア統合とテスト、など。
- 能力座標
  - 「プロセス実施」プロセス属性、など。

ASPICEの座標軸



Automotive_SPICE_PAM_31_Japanese.pdfより

ASPICEのプロセスカテゴリーとプロセス群



Automotive_SPICE_PAM_31_Japanese.pdfより

ASPICEの能力レベル

- レベル0：不完全なプロセス
- レベル1：実施されたプロセス
- レベル2：管理されたプロセス
- レベル3：確立されたプロセス

ASPICEのテスト関連プロセス

- ソフトウェアユニット検証（SWE.4）
- ソフトウェア統合テスト（SWE.5）
- ソフトウェア適格性確認テスト（SWE.6）
- システム統合テスト（SYS.4）
- システム適格性確認テスト（SYS.5）

テストの視点からの能力指標

- PA1.1 テスト担当者は基本的なテストプロセスに従ってプロセスを実施する
- PA2.1 テスト担当者は、主にテスト活動の計画、管理、制御を行う
- PA2.2 テスト担当者は、主にテスト文書の品質チェックを行う
- PA3.1 テストプロセスの責任者は主に全般的なプロジェクト戦略の定義を行う
- PA3.2 テスト担当者は、PA3.1で定義されたテスト戦略を適用する

ASPICEのテスト戦略

- ASPICEは各テスト固有のプロセスに対してテスト戦略を必要とする
- リグレッションテスト戦略は、テスト戦略の重要な部分
  - 例えばリスクベース

ASPICEのテスト文書

- WP 08-50：テスト仕様書
- WP 08-52：ISO/IEC/IEEE 29119-3に従ったテスト計画書と、それに含まれる戦略（WP 19-00）
- WP 13-50：テスト結果、テストログ、インシデント/逸脱レポート、テストサマリレポート

検証戦略

- ソフトウェアユニット検証（SWE.4）について、ASPICEは検証戦略を必要とする
  - コードレビューと静的解析も考慮する
- SWE.5/SWE.6/SYS.4/SYS.5のテスト固有のプロセスについて、ASPICEはテスト戦略を必要とする

トレーサビリティ

- CTFLシラバスと同じく、ASPICEも双方向トレーサビリティを必要とする
- ASPICEは、垂直トレーサビリティと水平トレーサビリティを区別する

2.2章：ISO26262

Learning Objective
AUTFL-2.2.1.1 E/Eシステムの機能安全の目的を説明する。（K2）
AUTFL-2.2.1.2 安全文化におけるテスト担当者の役割を想起する。（K1）
AUTFL-2.2.2.1 ISO 26262で規定されている安全ライフサイクルのフレームワークでのテスト担当者の役割を説明する。（K2）
AUTFL-2.2.3.1 ISO 26262の設計と構成を想起する。[情報提供]
AUTFL-2.2.3.2 テスト担当者に関連する、ISO 26262のパートのタイトルを想起する。（K1）
AUTFL-2.2.4.1 ASILの重要度レベルを想起する。（K1）
AUTFL-2.2.4.2 静的テストや動的テストに適用できるテスト設計技法やテストタイプに関するASILの影響および結果としてのテスト範囲を説明する。（K2）
AUTFL-2.2.5 ISO 26262の手法テーブルを解釈できるようになる。（K3）

2.2章：ISO26262

Learning Objective概要
AUTFL-2.2.1.1 機能安全の目的（K2）
AUTFL-2.2.1.2 安全文化におけるテスト担当者の役割（K1）
AUTFL-2.2.2.1 ISO 26262の安全ライフサイクルでのテスト担当者の役割（K2）
AUTFL-2.2.3.1 ISO 26262のつくり [情報提供]
AUTFL-2.2.3.2 テストに関連するISO 26262のパート（K1）
AUTFL-2.2.4.1 ASIL（K1）
AUTFL-2.2.4.2 テスト設計技法やテストタイプに関するASILの影響（K2）
AUTFL-2.2.5 ISO 26262の手法テーブル（K3）

安全文化への貢献

- テスト担当者は、ソフトウェア開発ライフサイクルの全フェーズに責任を持って参加し、プロダクト開発の全体的な状況を継続して把握しながら業務に従事することによって、安全文化に貢献する

安全ライフサイクルへの貢献

- 第1フェーズ：プロダクトコンセプト
- 第2フェーズ：プロダクト開発
- 第3フェーズ：プロダクト製造およびメンテナンス（「製造工程へのリリース」後）
  - テスト担当者は主に最初の２つのフェーズに貢献する
  - 第3フェーズへの移行時にも大きな役割を果たす

テストに関連するパート

- テスト担当者にとって、ソフトウェア検証と（少なくとも部分的に）システム妥当性確認は、最も重要なもの
  - パート４（システム開発）とパート６（ソフトウェア開発）
- パート８（支援プロセス）も検証、文書化、ツール認証など考慮すべき点がある

ASIL

- 機能安全の観点でのリスクの評価尺度
- 一番低いASIL Aから一番高いASIL Dまで、4つのレベル
  - ASIL Aにも該当しない場合は「QM」となる

テストへのASILの影響

- ASILは、テストの範囲に直接影響する
  - ASILに応じて特定のテスト設計技法とテストタイプを推奨する
  - テスト担当者が独自に判断できるのは、ASILで指定された枠内に限られる
  - 例えば、同値分割法と境界値分析の使用は、ASIL Aでは推奨されている。一方で、ASIL B以上では、これらの技法の使用は強く推奨されている

		ASIL A	ASIL B	ASIL C	ASIL D
1	Method x	o	+	++	++
2	Method y	o	o	+	+
3a	Method z1	+	++	++	++
3b	Method z2	++	+	o	o

CTFL AuT Syllabus 2018より

JSTQB FLとの対応

- テスト担当者に関連する以下の手法を記載している
  - テスト設計技法（例：同値分割法、境界値分析）
  - テスト実行の技法
  - テストタイプ
  - テスト環境
  - 静的テスト技法

2.3章：AUTOSAR

Learning Objective
AUTFL-2.3.1 AUTOSARの目的を想起する。（K1）
AUTFL-2.3.2 AUTOSARの全般的な設計を想起する[情報提供]。（K1）
AUTFL-2.3.3 テスト担当者の作業に対するAUTOSARの影響を想起する。（K1）

2.3章：AUTOSAR

Learning Objective概要
AUTFL-2.3.1 AUTOSARの目的（K1）
AUTFL-2.3.2 AUTOSARの構造（K1）
AUTFL-2.3.3 テスト担当者へのAUTOSARの影響（K1）

AUTOSARの目的

- 車載ECUのソフトウェアアーキテクチャの標準
- 「標準内でのコラボレーション、実装での競争」の原則
  - 常にアップデートされ続ける、全ECUに使えるアーキテクチャの提供
  - アーキテクチャの共通化による移植性等の維持

AUTOSARの構成

- ハードウェアから独立したソフトウェアコンポーネント（SW-C）
- 抽象化のためのAUTOSAR Runtime Environment（RTE）
  - SW-C間およびSW-CとBSW間のデータ交換を実現する
- 標準化された基盤ソフトウェア（BSW）
  - ハードウェア指向
- OEM-サプライヤ間の情報交換のためのARXMLファイル
  - ECU Configuration Description(EcuC)
  - System Configuration Description
  - ECU extract of System Configuration Description(EcuEx)

テストへのAUTOSARの影響

- テストレベルに応じて、SW-C/RTE/BSWにアクセスしてテストを行う必要がある/ことができる
- システム統合テストを（部分的に）早期に実施できる

2.4章：比較

Learning Objective
AUTFL-2.4.1 ASPICEとISO 26262の目的の差異を想起する（K1）
AUTFL-2.4.2 テストレベルに関するASPICE、ISO 26262、CTFLの間の相違を説明する（K2）

ASPICEとISO 26262の両立

- それぞれ開発の異なる側面に重点を置いている
- ISO 26262は機能安全におけるリスク回避のための要件とプロセスを定義
- ASPICEはプロダクト開発プロセスの能力を判定するためのフレームワークを提供

テストレベルの比較

ISTQB®	ISO 26262	ASPICE 3.0
Acceptance test	Safety validation (4-9)[19]	No equivalent
System of systems test[20]	Item integration and test (4- 8)[21]	System qualification test (SYS.5)
System integration test		System integrations test (SYS.4)
System test	Verification of the Software-safety requirements (6-11) Software integration and test (6-10)	Software qualification test (SWE.6)
Component integration test		Software integration test (SWE.5)
Component test	Software-Unit-Test (6-9)	Software unit verification (SWE.4)

CTFL AuT Syllabus 2018より

3章：仮想環境でのテスト

Learning Objective概略
AUTFL-3.1.1 自動車開発におけるテスト環境の背後にある目的/モチベーションを想起する。（K1）
AUTFL-3.1.2 自動車固有のテスト環境の一般的な構成要素を想起する。（K1）
AUTFL-3.1.3 クローズドループシステムとオープンループシステムの相違を想起する。（K2）
AUTFL-3.1.4 車載制御ユニットにとって重要な機能、データベース、およびプロトコルを想起する。（K1）

3章：仮想環境でのテスト

Learning Objective概略
AUTFL-3.2.1.1 MiLテスト環境の構成を想起する。（K1）
AUTFL-3.2.1.2 MiLテスト環境の適用領域と境界条件を説明する。（K2）
AUTFL-3.2.2.1 SiLテスト環境の構成を想起する。（K1）
AUTFL-3.2.2.2 SiLテスト環境の適用領域と境界条件を説明する。（K1）
AUTFL-3.2.3.1 HiLテスト環境の構成を想起する。（K1）
AUTFL-3.2.3.2 HiLテスト環境の適用領域と境界条件を説明する。（K2）

3章：仮想環境でのテスト

Learning Objective概略
AUTFL-3.2.4.1 XiLテスト環境（MiL、SiL、およびHiL）の基準を使用してテストすることの長所と短所を概説する。（K2）
AUTFL-3.2.4.2 1つ以上のテスト環境に対して、基準を適用して、特定のテスト範囲を割り当てる。（K3）
AUTFL-3.2.4.3 3つのXiLテスト環境（MiL、SiL、およびHiL）をV字モデルに対応づける。（K1）

3.1.1 自動車開発のテスト環境に対するモチベーション

- 可能な限り早期にテストを開始して、開発プロセスの早い段階で欠陥を見つける必要がある。
- その一方、実環境を使用してシステムをテストし、完成したプロダクトで出現する可能性がある欠陥を見つける必要がある。
- 異なる開発フェーズに適したテスト環境を使用して、この矛盾を解決するのがテスト担当者の役割。

3.1.2 テスト環境の一般的な構成要素

- テストを実行するために、不足している構成要素をシミュレーションできるテスト環境を必要とする。
- 制御ポイント（PoC：point of control）
  観測ポイント（PoO：point of observation）
- テスト環境の重要な構成要素は、環境モデルである。モデルは仮想テスト環境で重要な構成要素である。モデルは、燃焼機関、トランスミッション、車両センサー、電子制御ユニット、さらには運転手や道路状況など、実世界のある側面を表す。

3.1.3 クローズドループとオープンループの相違

- オープンループシステムでは、システムはオープンであり、出力から入力へのフィードバックがない。テストアイテムの入力はテスト担当者がテスト手順で直接定義する。
- クローズドループシステム（インザループを含む）の刺激はテストアイテムの出力を考慮する。環境モデルは出力を収集し、テストアイテムの入力に直接的または間接的にフィードバックする。

3.1.4 インターフェース、データベース、およびプロトコル

- 電子制御ユニットはさまざまなアナログおよびデジタルの入力を受け取り、環境データを絶えず収集する。
- 生成された出力はアナログまたはデジタルの出力ピン、バスシステム、または診断インターフェースを介して転送される。
- データベースは、制御ユニットの入力信号および出力信号を定義する。
- 通信プロトコルは、対応する物理インターフェースを介するデータ交換を定義する。

3.2 XiLテスト環境でのテスト

略称	名称	内容
MiL	モデルインザループ (Model in the Loop)	テストアイテム=モデル シミュレーション環境上で実行
SiL	ソフトウェアインザループ (Software in the Loop)	テストアイテム=ソフトウェア PC上で実行
PiL	プロセッサインザループ (Processer in the Loop)	テストアイテム=ソフトウェア ターゲットプロセッサ上で実行
HiL	ハードウェアインザループ (Hardware in the Loop)	テストアイテム=ECU ターゲットECU上で実行
ViL	ビークルインザループ (Vehicle in the Loop)	テストアイテム=車両（複数ECU） ターゲット車両上で実行

3.2.4 XiLテスト環境の比較

特性	MiL	SiL	HiL
実環境との類似性	低	低～中	高
デバッグにかかる時間と工数	低	中	高
実装とメンテナンスにかかる工数	低	中	高
テスト準備にかかる工数	低	中	高
テストアイテムの完成度	低	中	高
テストベース（仕様）に必要な完全性	中	中～高	高
テストアイテムへのアクセス容易性	高	中	低

- HiLは適用範囲が広いが一般的に高コスト。
- Hi-Loミックスが必要。

3.2.4 XiLテスト環境の比較

テストタイプ	内容	MiL	SiL	HiL
顧客要件のテスト	要求された機能が正しく提供されていることの確認。	可	可	適
故障検出と処理のメカニズム	故障の検出と、その後の安全状態への遷移	適	適	適
コンフィギュレーションデータへの応答テスト	テストアイテムの振る舞いに対するコンフィギュレーションデータの影響度の確認	可	適	適
診断機能のテスト	必要な診断機能が正しく提供されていることの確認	-	適	適
インターフェースでの相互作用のテスト	内部/外部インターフェースの確認	可	適	適
使用性の確認	要求通りかつユーザーの期待通りに使用できることの確認	-	可	適

4章：自動車ドメイン固有の静的及び動的テスト技法

静的テスト技法

Learning Objective概略
AUTFL-4.1.1 MISRA-C：2012ガイドラインの目的と要件について例を用いて説明する。（K2）
AUTFL-4.1.2 ISO/IEC 29148が定義するテスト担当者に関係する品質特性を使用して要件をレビューする。（K3）

4章：自動車ドメイン固有の静的及び動的テスト技法

動的テスト技法

Learning Objective概略
AUTFL-4.2.1 MC/DCテストカバレッジを達成するためのテストケースを作成する。（K3）
AUTFL-4.2.2 バックツーバックテストについて例を用いて説明する。（K2）
AUTFL-4.2.3 フォールトインジェクションテストの原則について例を用いて説明する。（K2）
AUTFL-4.2.4 要件ベーステストの原則を想起する。（K1）
AUTFL-4.2.5 適切かつ必須のテスト設計技法を選択する際にコンテキストに依存した基準を適用する。（K3）

4.1.1 MISRA-C:2012ガイドライン

- 自動車では本コーディングガイドラインに則ってプログラミングすることが必要。
- C言語向けのガイドラインであり、以下の2つから構成される。
  - ルール：静的解析ツールで検証できる
  - 指針：ツールでの検証が難しい

4.1.2 要件レビューのための品質特性

- 仕様は、開発とテストの土台である。このため、仕様に欠陥が存在すると、対処するための活動に多大なコストや時間がかかる。
- テスト担当者は仕様のレビュー時に品質特性を利用することで焦点を絞り、可能な限り多くの欠陥を検出できる。
- **ISO/IEC/IEEE 29148：2011**は、個々の要件および要件の集合に対する品質特性を定義している。

4.2.1 条件テスト・複合条件テスト・MC/DCテスト

- ホワイトボックステスト設計技法。
- 機能安全（ISO 26262）ではMC/DCカバレッジを求められるケースがある。（ASIL-D）
- 元は航空機のソフトウェア安全認証であるDO-178Bで用いられた手法。
- 複合条件テストでは増えすぎるテストケースを、実際にテストできる数に抑えることができる。

4.2.2 バックツーバックテスト

- 2つ以上のバリアントを比較する。
- テストアイテム間・環境間の差を明らかにする。
- 要件ベーステストの代わりとはならない。
- 以下のようなケースで用いる。
  - 同じソフトウェアの異なるバージョン間
  - 実行可能モデルと生成コード間

4.2.3 フォールトインジェクションテスト

- 欠陥を選択的に注入する。
- 堅牢かつ安全な方法でシステムが内部および外部の欠陥に対処できるようにすることを確認する。
- 外部コンポーネント・インターフェースの欠陥はHiLやSiL環境で実施される。
- ソフトウェアの欠陥はデバッガーなどが必要なことが多く、工数がかかる。

4.2.4 要件ベーステスト

- 要件を基にテストケースを作成する。
- テストケースで要件をカバーすることにより、テストアイテムが要件を満たしていることを確認する。
- 探索的テストなど経験ベースのテストも組み合わせることができる。
- 要件が不完全か一貫性がない場合、テストケースも同じ問題を抱える。

4.2.5 テスト技法の選択

- ISO 26262ではASILに応じてテスト（設計）技法を選択する。
- ただし、それ以外にもいくつかの要因を考慮する必要がある。

CTFL®-AuT バージョン2.0.2より

	テスト設計技法	ASIL A 推奨	テストベース適合性	欠陥見逃しリスク	テストレベル妥当性	選択
1	要件ベーステスト	++	適	++	適	○
2	同値分割法	+	適	++	適	○
3	境界値分析	+	否	-	適	
4	ステートメントテスト	++	適	++	否	

参考文献

- Automotive_SPICE_PAM_31_Japanese
  - http://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_31_Japanese.pdf
- CTFL AuT Syllabus 2018
  - https://www.istqb.org/downloads/send/56-foundation-level-automotive-software-tester-documents/225-ctfl-aut-syllabus-2018.html

EOF

JSTQBに関するお問い合わせ窓口
JSTQB（Japan Software Testing Qualifications Board）

E-mail： **query@jstqb.jp**

※1:本アドレスで受けられるメールの最大容量は50KBとなっておりますのでご注意ください
※2:お問合せの内容によっては、検討後に回答させていただくものもあり、お時間をいただく場合があります

FAQもあわせてご利用ください
http://jstqb.jp/faq.html