＜新規Webページ公開＞Automotive SPICE 4.0の詳細解説

先月のメルマガでは、VDA Automotive SYS カンファレンスの速報として、Automotive SPICE 4.0 に関する動向についてご紹介いたしました。
今回のメルマガでは、Automotive SPICE 4.0 の内容について、もう少し詳細にご紹介いたします。

[Automotive SPICE 4.0 の対象プロセス]

Automotive SPICE 4.0（以下、バージョン 4.0）では以下のプロセスに追加と削除が行われました。

追加されたプロセス：

・HWE.1～4：ハードウェアエンジニアリングプロセス群
・MLE.1～4：機械学習エンジニアリングプロセス群
・SUP.11：機械学習データ管理
・VAL.1：妥当性確認

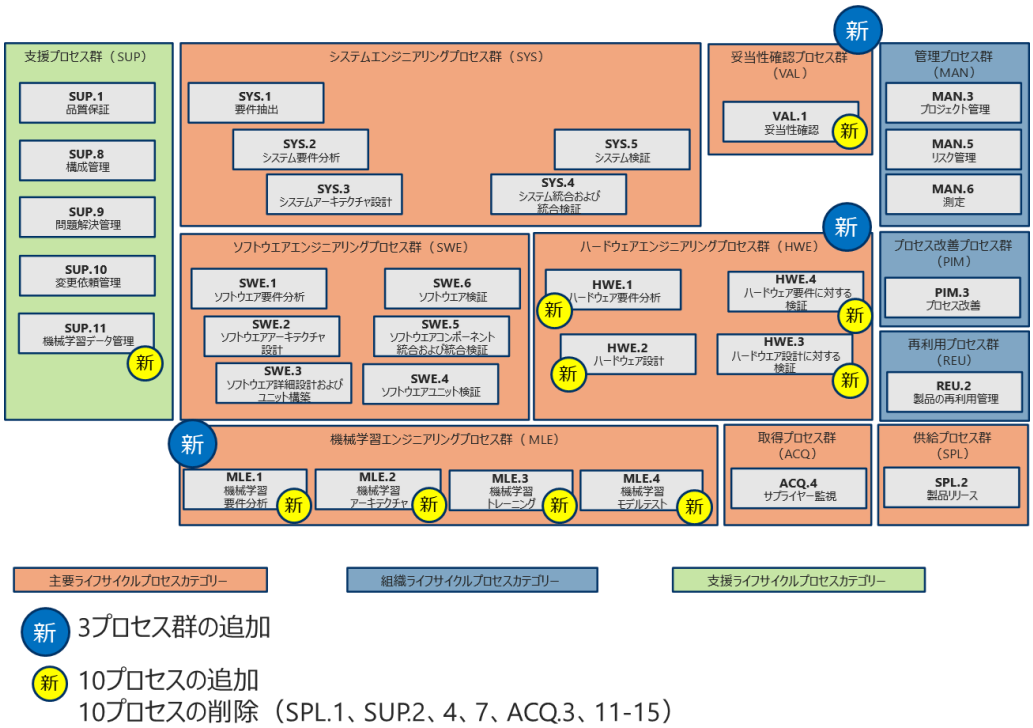
削除されたプロセス：

・SUP.2：検証
・SUP.4：共同レビュー
・SUP.7：文書化
・SPL.1：サプライヤー入札
・ACQ.4 以外の取得プロセス
※削除された取得プロセスの内容は、Automotive SPICE for Cyber Security の ACQ.2 に集約

位置づけが変更されたプロセス：

・REU.2：再利用のためのプロダクト管理
※バージョン 3.1 までは組織的な再利用の仕組み（再利用プログラム）に基づいた再利用を想定していましたが、バージョン 4.0 ではベースモデルに基づいた再利用を想定する位置づけに変更されました。

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.



出典：VDA Automotive SYS Conference 2023、VDA WG13 発表資料

なお、Automotive SPICE for Cyber Security は、バージョン 4.0 に内包されておりませんが、バージョン 4.0 の構造に合わせて更新される予定です。
また、当初予定されていた MEE（機械エンジニアリングプロセス）は、他プロセスを優先させる都合によりバージョン 4.0 への内包は見送られました。
次バージョン以降では、この MEE に加えて ISO 26262 に対応した機能安全 PAM の導入が検討されています。

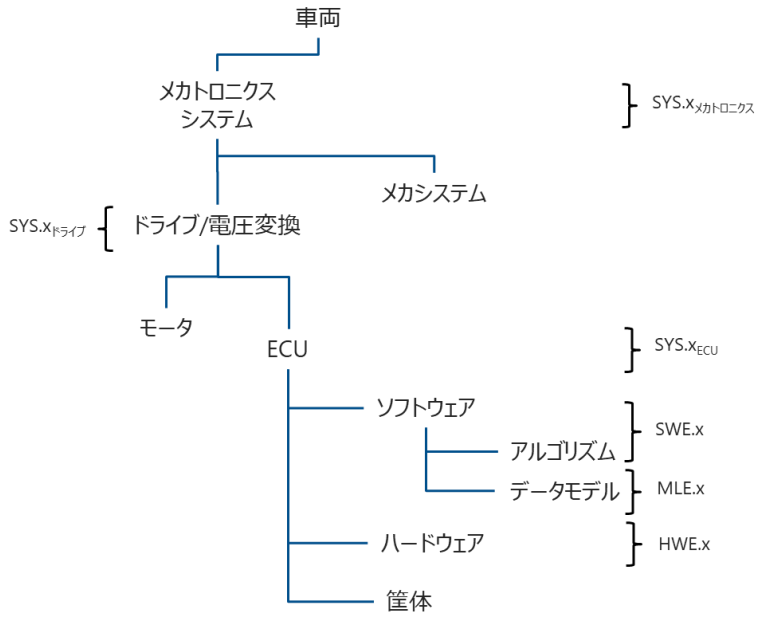
[新設プロセスの詳細：HWE]

従来、intacs からリリースされていた電気・電子系ハードウェア向けのエンジニアリングプロセスの PAM、Hardware SPICE が、Automotive SPICE のバージョン 4.0 に内包されることになりました。
intacs の Hardware SPICE バージョン 2.1 と Automotive SPICE バージョン 4.0 の HWE のプロセス群が対応関係を持つ形となります。

HWE の位置づけ：

Automotive SPICE バージョン 3.0 で導入されたプラグインコンセプトにより、システムエンジニアリング（SYS）を形成するドメインエンジニアリングの一つとしてハードウェアエンジニアリングのプロセスが Automotive SPICE のプロセスと共に利用できるようになりました。
バージョン 4.0 では、このコンセプトが継承されます。
HWE は、下図のように、サブシステム化された下位レイヤーの電気・電子系ハードウェアに対して適用されます。

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.



出典：Automotive SPICE ガイドライン 2.0

また、図には記載されていませんが、図中の HW は一般的にセンサ、コントローラ、アクチュエータドライバ等を含みます。
このうち、SoC（System On Chip）のようなパッケージは、それ自体をさらに下位のサブシステムと捉え、その構成要素に対して HWE（SoC 上の回路）、SWE（ファームウェア）、MEE（パッケージのハウジング）の PAM がアセスメントで適用されます。

なお、上記のように階層化されたサブシステムにおいては、組織によって HWE と MEE の境界が異なる場合があります。
例えば、アンテナのように、筐体の形状によって筐体自体に電気的な特性を持たせている場合、筐体の設計がメカチームではなくハードウェアチームによって行われる組織があります。
これが合理的なアプローチであれば、Automotive SPICE において弱みと捉えることはありません。その場合、アセッサーはアセスメント対象の設計意図に基づいて、Automotive SPICE 上の評定対象プロセスの割り当てを判断する必要があります。

HWE として含まれる４つのプロセスについて以下に解説します。

HWE.1 ハードウェア要求分析：

HWE.1 の構造は、既存の SWE.1 と変わりません。
ただ、ハードウェアにおいて扱われる要求には、State-of-the-art 特性も含まれます。
なお、State-of-the-art 特性には、ISO 26262-5 6.4.2 に挙げられているセーフティメカニズムに関する特性も含まれます。
また、HWE において環境に関する影響分析では、コネクタ、ケーブル、電源、通信ライン等のインターフェースに加えて、電圧変動、搭載スペース、EMC 等の影響の確認も求められます。

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

HWE.2 ハードウェア設計：

HWE.2 はハードウェアのアーキテクチャ設計と詳細設計を含む位置づけとなっています。
ただし、ハードウェアの規模が小さい場合など、アセスメント対象プロジェクトにおいてアーキテクチャ設計と詳細設計に分かれていなくても、それが合理的なアプローチであれば弱みとは捉えません。
ソフトウェアのアーキテクチャ設計との違いとしては、選択肢の評価に関する観点が含まれていないことが挙げられます。
バージョン 4.0 では、SYS.3、SWE.2 の BP からも選択肢の評価に関する BP が削除されましたが、SYS.3 と SWE.2 については、選択肢の評価に関する観点が分析に関する BP の中に残ります。一方のハードウェアは、設計の選択肢が一意に決まる場合もあるため、この観点は対象外となります。
また、Automotive SPICE の HWE には生産に関するプロセスが含まれませんが、HWE.2 は生産プロセスとの界面までを対象としており、特殊特性や EOL 要件を特定して生産の関係者へ伝達する行為も含まれます。
なお、BP の定義には直接的な記載がありませんが、本プロセスはアーキテクチャ設計と詳細設計を含むため、両設計間の一貫性および双方向トレーサビリティも求められます。

HWE.3 ハードウェア設計に対する検証：

まず、エンジニアリングプロセスにおいて、バージョン 4.0 では V 字右側の用語がテストから検証に変わりました。
これは HWE.3、HWE.4 も同様です。
従来の Automotive SPICE では、V 字右側においては最終製品に組込まれる実体として、サブシステムやソフトウェアを対象とするテストに焦点を当てていました。
しかし、実際には実体に対するテストだけでなく、計算やシミュレーションも V 字右側の確認行為として用いられることがあります。
そこで、バージョン 4.0 では従来のテストを検証という用語に改め、シミュレーション等も対象とすることになりました。
シミュレーションは、V 字左側の設計に対する検証や要求に対する実現可能性確認にも用いられますが、HWE.3 においては、リリース対象のサンプルを確認するための観点を対象とします。
なお、HWE.3 においては、ソフトウェアのような段階的な統合の観点は含みません。
これは、ハードウェアにおいて部品をアセンブルし直しながら検証を行うアプローチが一般的ではないためです。
HWE.3 において内部インターフェースに着目したテストは、ハードウェア内の各インターフェースに対して、ジャンパーピン等を用いた計測ポイントに着目したテストを想定しています。
ハードウェア対ハードウェアの統合が必要なケースについては、アセスメントでは HWE.3 ではなく SYS.4 の対象として扱います。

HWE.4 ハードウェア要求に対する検証：

HWE.4 は、リリース対象となるハードウェアのサンプルがハードウェア要求を満たしていることを確認するための検証を対象としています。
ハードウェア要求は、顧客や自社内から要求されるテスト要求も含まれます。
前述の能力レベルの整理において、能力レベル 1 から戦略に関する概念が削除された旨を説明しました。
HWE.3、4 でも BP1 からは戦略に関する記述が削除され、代わりに検証手段という用語が用いられます。

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

既存の管理・支援系プロセス：

MAN.3 や SUP.8 などの管理・支援系プロセスも同様にハードウェアプロセスへも適用されます。
基本的な考え方は変わりませんが、管理対象の人的リソース、物的リソース、技術などが広がります。
もし、ハードウェアチームが他チームと異なる方法でプロジェクト管理を行っているようであれば、アセスメントにおいて MAN.3 を別インスタンスとして扱うことも考慮が必要となります。
また、構成管理においては、ハードウェア固有の特徴として、実サンプルを扱う考慮が必要となります。
顧客に対して同一設計のサンプルを複数台納入するのであれば、個々のサンプルを識別するためのシリアル番号の管理も必要ですし、顧客からサンプルの長期保管を要求されている場合は、保管場所の管理も考慮に入れる必要があります。

[新設プロセスの詳細：MLE]

昨今、自動車の自動運転等に導入が進んでいる機械学習に関するエンジニアリングプロセスと、その機械学習データの管理に関する支援プロセスが新たに定義されました。

MLE.1　機械学習要求分析：

本プロセスにおける機械学習は、ソフトウェアとして実装されるものを想定しています。
そのため、機械学習要求に対する要求は、SWE.1 で扱うソフトウェア要求の一部として位置づけられ、SWE.1 と同様に機械学習要求としての実現可能性、検証可能性等の分析が求められます。
また、後述の SUP.11 機械学習データ管理のための管理要求として、機械学習データに対する要求もこのプロセスで扱われます。

MLE.2 機械学習アーキテクチャ：

MLE.2 では、機械学習におけるトレーニングや機械学習のデプロイを行うためのアーキテクチャを決定すること。そして、その決定したアーキテクチャが意図通りであることを確認することが求められます。このアーキテクチャには、機械学習モデル、前後処理、ハイパーパラメータ（モデルのパフォーマンスを決定するためのパラメータ）も含まれます。
また、機械学習を行うためのハイパーパラメータの初期値の設定や、トレーニングおよび運用に必要なリソースの決定も含まれます。

MLE.3 機械学習トレーニング：

MLE.3 では、機械学習要求を満たすようにモデルに対するトレーニングを実施することが求められます。
そのため、トレーニングや妥当性確認の開始／終了基準、ハイパーパラメータの最適化方法、学習用データの作成／変更方法、実施環境などを決定し、作成された学習用データを用いてトレーニングを実施します。
なお、本プロセスで用いられる妥当性確認という用語は、VAL.1 の妥当性確認とは異なり、上記トレーニングにおけるハイパーパラメータの最適化を意味しています。

MLE.4 機械学習モデルテスト：

MLE.4 では、トレーニング済みのモデル、およびトレーニング済みのモデルから導出されたデプロイ用のモデルが、

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

機械学習要求を満たしていることを保証することが求められます。
そのため、テストの開始／終了基準、テストに用いるデータセット、期待されるテスト結果、テスト用データの作成／変更方法、実施環境などを決定し、モデルに対するテストを実施します。

SUP.11 機械学習データ管理：

一連の機械学習エンジニアリングプロセスに用いる機械学習データに対する管理プロセスとして、SUP.11 が新たな支援プロセスとして追加されました。
本プロセスでは、データ管理のための活動、データを管理するためのリソース、データのライフサイクル、利害関係者の窓口などを含んだデータ管理の仕組みを確立することや、データの品質を維持するため活動が求められます。

[新設プロセスの詳細：VAL]

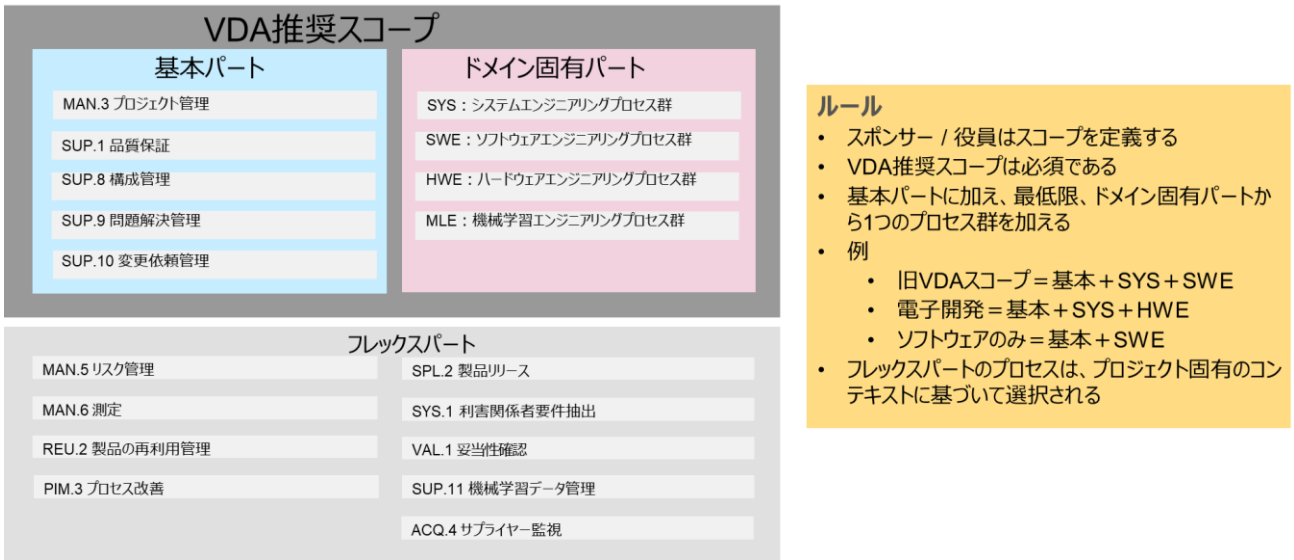
従来の Automotive SPICE では、“正しくものを作ったか”という検証の観点を中心に編成されており、“正しいものを作ったか”という妥当性確認の観点は直接的に含まれていませんでした。
そのため、妥当性確認に関する観点をアセスメントで確認したい場合には、ISO/IEC 12207 から妥当性確認プロセスを持ち込むか、Automotive SPICE の SYS.5 を拡大解釈して妥当性確認の観点を加えるという方法が intacs から示されていました。
ただ、機能安全やサイバーセキュリティを考慮する中で、妥当性確認の観点は重要となります。
そこで、バージョン 4.0 では新たに VAL 妥当性確認プロセス群を設置し、その中に VAL.1 妥当性確認プロセスが定義されました。
妥当性確認は、利害関係者要求との関係を持つため、SYS.1 と対を成すように SYS.6 とする案もありましたが、既存の構造を維持するため、SYS のプロセス群とは別で定義されています。

妥当性確認は、検証と異なり技術的な観点だけでなく予見されるユーザーの振る舞いやユーザーが受けるフィーリングも含まれます。たとえば、自動車が走行中にもかかわらず、運転手がシフトレバーを R レンジに入れてしまうことが予見されます。機能安全では、合理的に予見可能な誤使用による危険事象も考慮対象としますが、危険事象に限らず利害関係者にとって不都合なことは、妥当性確認にて確認される必要があります。
そのため、妥当性確認のインプットは、明確に定義された利害関係者要求だけでなく、経験に基づいた探索的アプローチも対象となります。
探索的アプローチを用いた場合、利害関係者要求との間で完全なトレーサビリティの確立ができないことがありますが、これを許容することは評定ガイドラインの中で定義されています。

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

[VDA スコープ]

バージョン 3.0、3.1 には、旧 HIS スコープを継承する形で、アセスメント対象の基本スコープとして VDA スコープが定義されていました。
バージョン 4.0 では、下図の通り基本パートに含まれる管理・支援系の 5 プロセスに、SYS、SWE、HWE、MLE のうち 1 つ以上のエンジニアリングに関するプロセス群を加えた範囲を新たな VDA スコープと位置付けます。
この新たな VDA スコープに対して、必要に応じて図下部のフレックスパートのプロセスがアセスメント対象として追加されます。



出典：VDA Automotive SYS Conference 2023、VDA WG13 発表資料

[能力レベルの整理]

バージョン 3.0 では、エンジニアリングプロセス V 字左側における検証の概念を SUP.2 および GP2.2.4 に集約するなど、Automotive SPICE では、重複した指標を回避する試みが従来から行われてきました。
バージョン 4.0 では、さらに能力レベル 1 に残っていた体系的な文書化に関する概念が能力レベル 2 に移されました。
これにより、従来のテスト系プロセスや支援系プロセスの BP1 に存在していた戦略が、GP2.1.1 に集約されるなどの変更が行われました。
従来の戦略も、能力レベル 1 では体系的な定義を求めていたわけではありませんでしたが、一部のアセッサーは、戦略という PAM の記載に基づいて体系的な定義を期待してしまっていたことで、文書の欠落を能力レベル 1 の弱みと捉えてしまっていました。
この点に関するバージョン 4.0 での変更は、能力レベル 1 と 2 でそれぞれ期待される状態を明確に区別するための意図です。
それに伴い、従来の戦略にその一部として含まれていた当該プロセスの実施に必要な取り決めは、Measure（手段）という用語として能力レベル 1 に新たに定義されました。

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

検証系プロセス（旧テスト系プロセス）においては、従来のテスト戦略が検証手段という用語となり、この検証手段には検証技法、合否基準を含むテストケース、開始／終了基準、検証環境などが含まれます。

その他、冗長だったり、強い依存関係を持っていたりした BP も統合されました。
エンジニアリングプロセスに含まれる一貫性と双方向トレーサビリティもその一つです。
元々、バージョン 2.5 までは、一貫性と双方向トレーサビリティが一つの BP でしたが、一貫性を確保することよりもトレーサビリティを確立することに着目されがちであったことや、トレーサビリティの確立は一貫性を確保する以外の目的でも行われることから、バージョン 3.0 ではこれらが別の BP として定義されました。
しかし、これらが別の BP として定義されることで、アセッサーは評定時にこれら BP 間の依存関係を考慮する必要が出てしまいます。
バージョン 4.0 では、このような依存関係を極力無くすことで、アセスメントの労力を極力低減することを意図して、いくつかの BP の統合が行われました。

なお、BP の統廃合によって全体的に BP の数が減り、旧 VDA スコープでの比較でバージョン 3.1 の BP 数が 127 だったのに対し、バージョン 4.0 では 97 となります。
ただし、前述した能力レベル 2 へ移された観点を除いて、能力レベル 1 で考慮すべき観点が減ったわけではありません。

PAM v3.1					
プロセス	BP数	プロセス	BP数	プロセス	BP数
ACQ.4	5	MAN.3	10	SPL.1	8
SPL.2	13	MAN.5	7	ACQ.3	7
SYS.1	6	MAN.6	11	ACQ.11	10
SYS.2	8	SUP.1	6	ACQ.12	10
SYS.3	8	SUP.8	9	ACQ.13	15
SYS.4	9	SUP.9	9	ACQ.14	8
SYS.5	7	SUP.10	8	ACQ.15	5
SWE.1	8	REU.2	8	SUP.2	5
SWE.2	9	PIM.3	9	SUP.4	8
SWE.3	8			SUP.7	8
SWE.4	7				
SWE.5	9				
SWE.6	7				
VDAスコープ			127	合計	265

PAM v4.0					
プロセス	BP数	プロセス	BP数	プロセス	BP数
ACQ.4	5	MAN.3	10	HWE.1	6
SPL.2	8	MAN.5	7	HWE.2	6
SYS.1	5	MAN.6	11	HWE.3	6
SYS.2	6	SUP.1	6	HWE.4	6
SYS.3	5	SUP.8	9	MLE.1	6
SYS.4	5	SUP.9	9	MLE.2	7
SYS.5	5	SUP.10	8	MLE.3	5
SWE.1	6	REU.2	8	MLE.4	7
SWE.2	5	PIM.3	9	SUP.11	6
SWE.3	5			VAL.1	5
SWE.4	5				
SWE.5	7				
SWE.6	5				
旧VDAスコープ			97	合計	205

PAM v4.0:
VDAスコープにおいて
97個のBP vs 127個の BP

合計で
205個のBP vs 265個のBP

出典：VDA Automotive SYS Conference 2023、VDA WG13 発表資料

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

[共通プラクティスの整理]

バージョン 4.0 では、能力レベル 2 と 3 に関する GP の統廃合も行われました。
特に従来の PA3.1 と PA3.2 は概念的には正対称な位置づけであるにもかかわらず、GP の数が一致しておらず使い辛さがありましたが、バージョン 4.0 では GP が正対称になるように整理されました。

PAM v3.1		PAM v4.0	
PA 2.1	プロセス実施管理	PA 2.1	プロセス実施管理
GP 2.1.1	プロセスの実施に対する目標を識別する。	GP 2.1.1	プロセスの実施に対する目標を識別し、戦略を定義する。
GP 2.1.2	識別した目標を遂行するためにプロセスの実施を計画する。	GP 2.1.2	プロセスの実施を計画する。
GP 2.1.3	プロセスの実施を計画に基づいて監視する。	GP 2.1.3	リソースのニーズを定義する。
GP 2.1.4	プロセスの実施を調整する。	GP 2.1.4	リソースを識別し、利用可能にする。
GP 2.1.5	プロセスを実施するために責任および権限を定義する。	GP 2.1.5	プロセスの実施を監視し、調整する。
GP 2.1.6	計画に従ってプロセスを実施するためにリソースを識別し、準備し、利用可能にする。	GP 2.1.6	関係者間の窓口を管理する。
GP 2.1.7	関係者間の窓口を管理する。		

PAM v3.1		PAM v4.0	
PA 2.2	作業成果物管理	PA 2.2	作業成果物管理
GP 2.2.1	作業成果物に対する要件を定義する。	GP 2.2.1	作業成果物に対する要件を定義する。
GP 2.2.2	作業成果物の文書化および制御に対する要件を定義する。	GP 2.2.2	作業成果物の保管および制御に対する要件を定義する。
GP 2.2.3	作業成果物を識別し、文書化し、制御する。	GP 2.2.3	作業成果物を識別し、保管し、制御する。
GP 2.2.4	定義した要件を満足するために、作業成果物をレビューし、調整する。	GP 2.2.4	作業成果物をレビューし、調整する。

PAM v3.1		PAM v4.0	
PA 3.1	プロセス定義	PA 3.1	プロセス定義
GP 3.1.1	定義されたプロセスの展開を支援する標準プロセスを定義し、それを維持する。	GP 3.1.1	標準プロセスを定義し、それを維持する。
GP 3.1.2	プロセスが統合システムとして機能するように、プロセス間のシーケンスおよび相互作用を決定する。	GP 3.1.2	必要な能力を定義する。
GP 3.1.3	標準プロセスを実施するための役割、能力、責任、および権限を識別する。	GP 3.1.3	必要なリソースを決定する。
GP 3.1.4	標準プロセスを実施するために、必要となるインフラおよび作業環境を識別する。	GP 3.1.4	標準プロセスを監視するために、適切な手法を決定する。
GP 3.1.5	標準プロセスの有効性および適切性を監視するために、適切な手法および手段を決定する。		

PAM v3.1		PAM v4.0	
PA 3.2	プロセス展開	PA 3.2	プロセス展開
GP 3.2.1	標準プロセスの使用に際して特定の背景に関する要件を満足するように、定義されたプロセスを展開する。	GP 3.2.1	標準プロセスの使用に際して特定の背景に関する要件を満足するように、定義されたプロセスを展開する。
GP 3.2.2	定義されたプロセスを実施するために、役割、責任、および権限を割り当て、伝達する。	GP 3.2.2	定義された役割に必要な能力を確保する。
GP 3.2.3	定義されたプロセスを実施するために、必要な能力を確保する。	GP 3.2.3	定義されたプロセスの実施を支援するために必要なリソースを確保する。
GP 3.2.4	定義されたプロセスの実施を支援するために、リソースおよび情報を提供する。	GP 3.2.4	定義されたプロセスの実施を監視する。
GP 3.2.5	定義されたプロセスの実施を支援するために、適切なプロセスインフラを提供する。		
GP 3.2.6	プロセスの適切性および有効性を実証するために、プロセスの実施に関するデータを収集し、分析する。		

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

なお、能力レベル２と３に関する GP の数の変化は以下の通りです。

PA	V3.1	V4.0
PA2.1	7	6
PA2.2	4	4
PA3.1	5	4
PA3.2	6	4

[Automotive SPICE ガイドライン 2.0]

Automotive SPICE のバージョンアップに伴い、Automotive SPICE ガイドラインもバージョン 2.0 にバージョンアップします。
従来のガイドラインは、アセッサーの共通理解を深めることにつながったものの、多くのルール、推奨事項が定義されたことで、アセスメントにおいてそれらを確認するための労力が大きく増えていました。
バージョン 2.0 では、従来のガイドラインにおける課題を解消すべく以下の改良が行われました。
・アセスメント対象組織、プロジェクトにおけるプロセスの解釈に役立てるための情報の記載
・曖昧だったルールの明確化
・推奨事項の撤廃
　※適用条件が曖昧だったため、推奨事項に位置づけられたものは、ルールに移動するか削除となる
・アセスメントの再現性向上

なお、今回ご紹介した Automotive SPICE 4.0 の詳細は、9 月のトレーニングにて改めて詳細に解説いたします。
トレーニングの詳細は下記をご参照ください。

[Automotive SPICE 4.0 アップデートトレーニング　～ASPICE4.0 の活用に向けた勘所～]
開催日：2023/9/21(木) 9:00～12:00
お申込先：https://biz3.co.jp/publictraining/5295

2023/8/7 田渕 一成

※Automotive SPICE 4.0 の解説 WEB ページはこちら：
https://biz3.co.jp/lp_category/automotive_spice

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.