

機能安全開発の大幅コストダウンが可能！ パーティションOS一般公開開始

～異なる安全度水準(SIL/ASIL)の混在が可能に～

株式会社ウィッツ

組込制御開発部 Safety&SecurityPF開発室
片岡 歩



IEC61508 ISO26262
プロセス認証

【対象システム】

移動支援ロボット、介護ロボット、航空宇宙（飛行機、ロケット）、自動車等の高い信頼性が求められ、機能停止が許されない高信頼性システムでの使用を想定している

【問題】

高信頼性システムのすべての機能が安全性を求められている訳ではなく安全度の低い機能も混在している

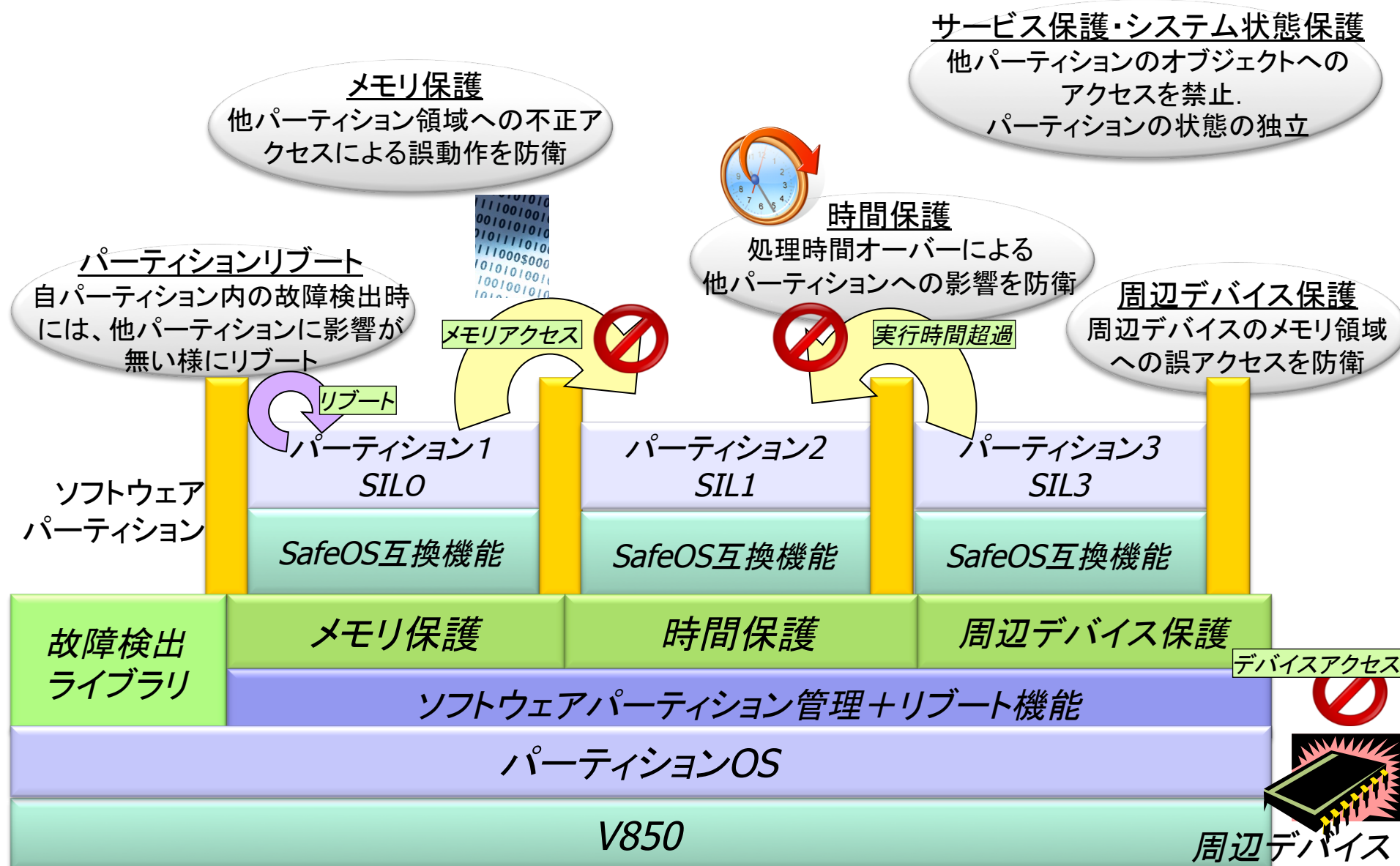
- 機能安全規格 (IEC61508 SIL4 / ISO26262 ASIL-D) 適応によるシステム構造の複雑化、検証コストの増大
- ECU統合時における高レベルでのSIL/ASIL適応による開発コストの増大

→機能安全対応範囲をコンパクトにするべき

問題への解決策として

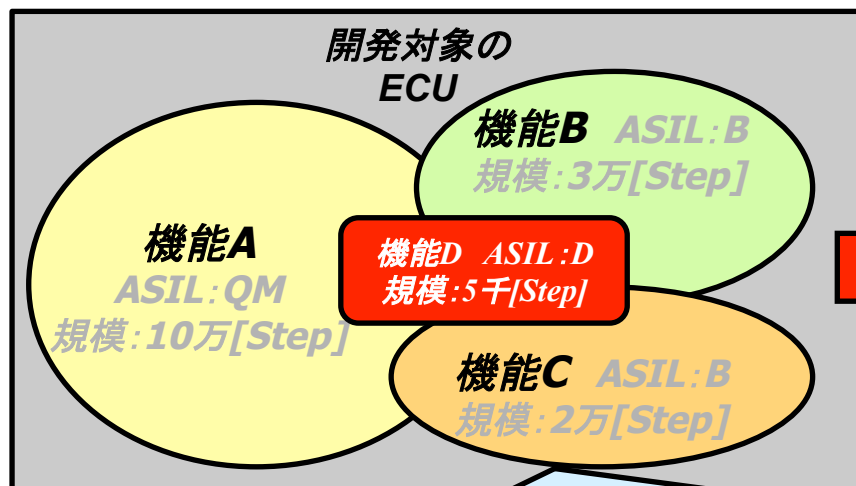
- 高いレベルのSIL/ASILをコンパクトにするためには、対象機能が「他の機能から悪影響を受けない」よう、独立性を高くする必要がある。
 - 独立性を保つためには...
 - もっとも簡単な対策はマルチマイコン化すること
⇒ しかし、この対応を行うとHWコストが増加する...
 - パーティショニングOSを使うことでマイコンを増やさずに「高いレベルのSIL/ASIL機能の独立性を保つこと」が可能！
- ※ISO26262におけるASILデコンポジションを適用する際に、
パーティショニングOSは非常に有効。

パーティションOSの全容(機能)



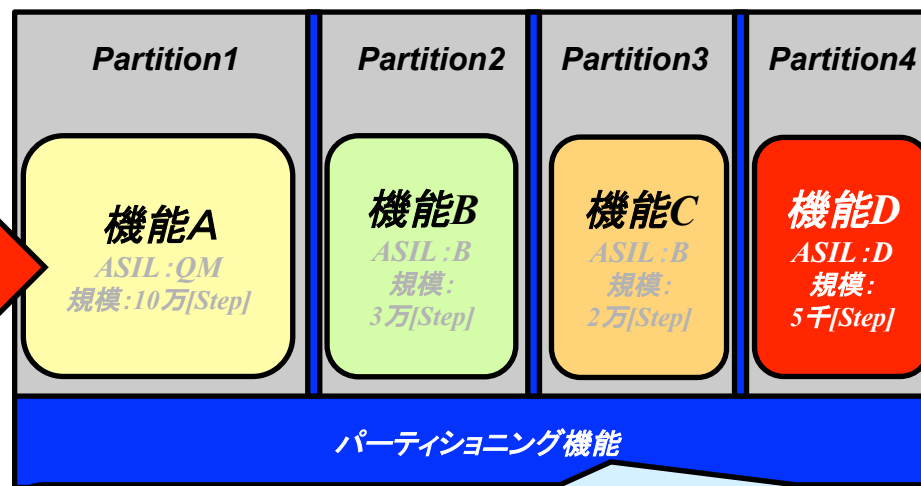
開発コスト削減効果(試算)

■ パーティショニング機能なし



機能間に従属関係があると、故障が伝搬する恐れがあるため、ASIL-Dが証明できないため、ECU全体に最も高い「ASIL-D」対応が必要となる。

■ パーティショニング機能あり



パーティショニング機能を利用して機能間の独立性を保証できれば、ASIL-Dで開発する範囲を小さくできる！
⇒開発コストの増加を抑えることができる

※開発規模(Step数)とヴィッツの実績から試算

パーティショニング機能なし
約1240[人月]

開発コスト
4倍！！

従来開発の場合…
約310[人月]

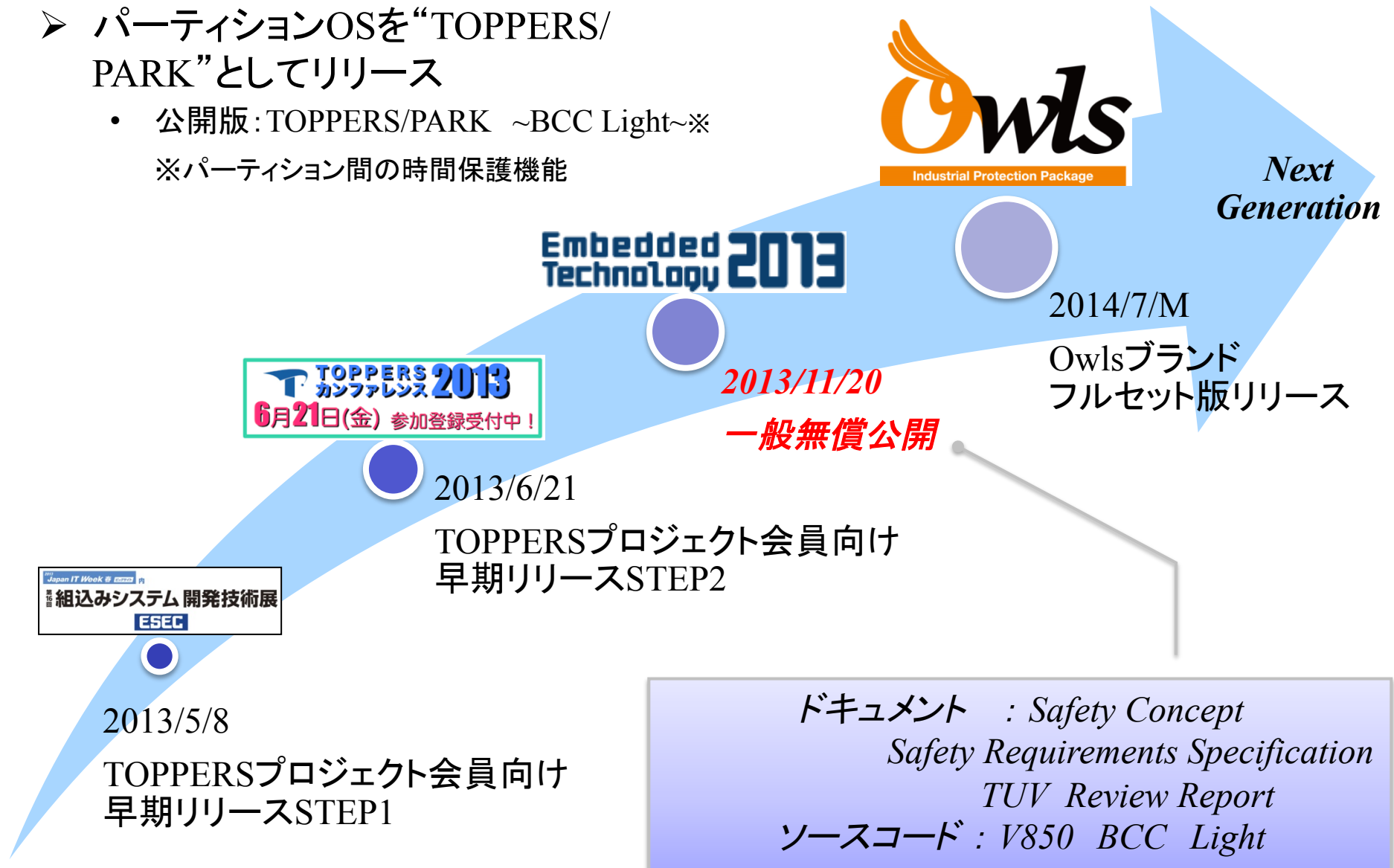
開発コスト
1.6倍！！

パーティショニング機能あり
約490[人月]

・ パーティショニング機能を導入する効果は大きい！

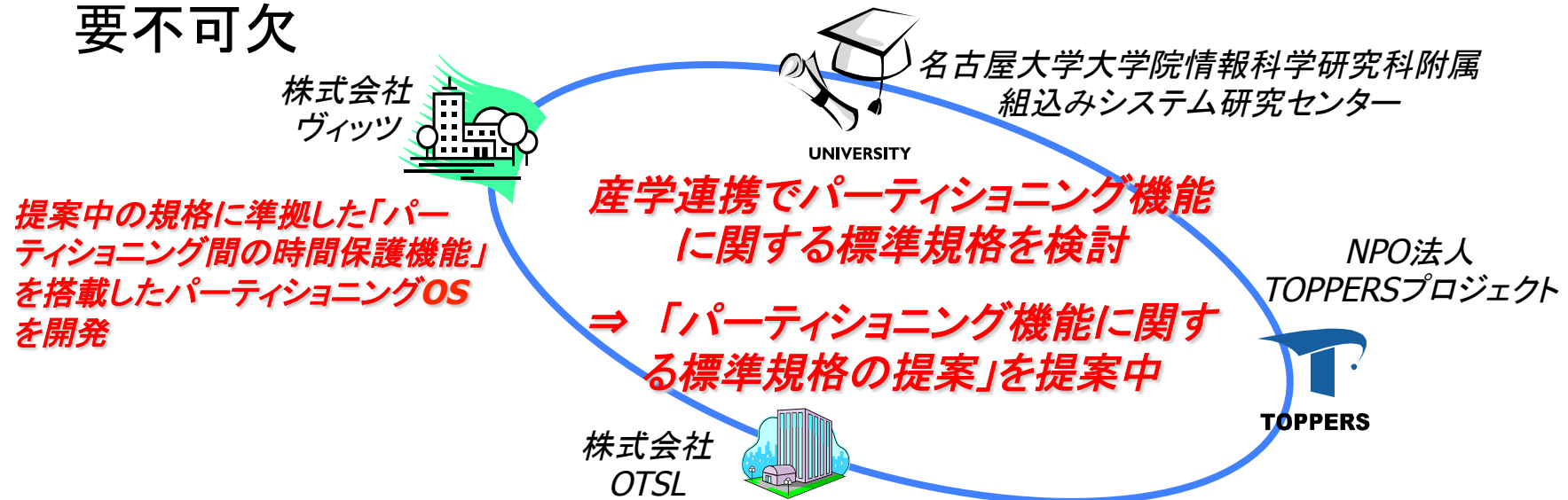
パーティションOSの公開スケジュール 株式会社 ヴィッツ

- パーティションOSを“TOPPERS/PARK”としてリリース
 - 公開版: TOPPERS/PARK ~BCC Light~※
- ※パーティション間の時間保護機能



組込みソフトウェア業界発展に向けて 株式会社 ヴィッツ

- 機能安全規格への対応が求められる中で、ソフトウェアの開発/検証コストを最適化するために、パーティショニング機能は必要不可欠



- パーティションOSをTOPPERSプロジェクトより一般公開することで、提案中の「パーティション間の時間保護機能」を多くの方に実際に使用して頂き、**パーティショニング機能の機能性や有用性を検証**
⇒パーティショニング技術が広く活用され、組込みソフトウェア業界の発展につながることを期待

謝辞

本認証取得に際し、経済産業省・(独)中小企業基盤整備機構の戦略的基盤技術高度化支援事業の採択テーマとして実施した「故障未然防衛機能を有した高信頼性ソフトウェアプラットフォームの開発」の成果を活用しました。

研究実施プロジェクトのメンバならびにアドバイザー各位

メンバ組織

(株)ヴィッツ、名古屋大学(NCES)、産業技術総合研究所(CVS)

アドバイザー組織

トヨタ自動車(株)、アイシン精機(株)、(株)東海理化、オークマ(株)、
(株)デジタル

本発表への問い合わせ先

一般公開物および製品等のより詳しい内容は、
ET2013展示場内 E-20 ヴィッツブースまでお越しください

総合問い合わせ先

株式会社ヴィッツ

総務部：安場、佐藤 (052) 220-1218

技術的問い合わせ先

株式会社ヴィッツ

技術本部： 片岡(kata@witz-inc.co.jp)

杉山(ayumus@witz-inc.co.jp)

(052) 220-1218

ご静聴ありがとうございました

本内容についてのご質問は下記にお願いします

株式会社ヴィッツ

Tel: 052-220-1218

片岡 歩

kata@witz-inc.co.jp