RTOSハイパーバイザーとオープンソースによるドメインコントローラの機能安全

OSAKA NDS Embedded Linux Cross Online Forum #11

2020, July 10

BlackBerry Japan

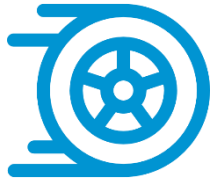
Kazunori Inami

BlackBerry | QNX

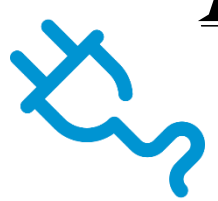
自動車業界のトレンド

コネクテドカー
（コネクティビイティ）

自動運転
（レベル 2-5）



自動車モビリティ
（ライドシェアなど）

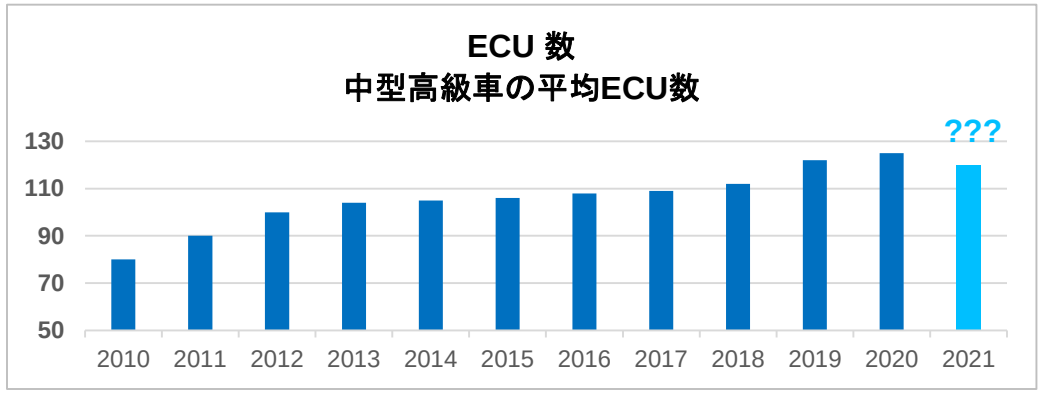


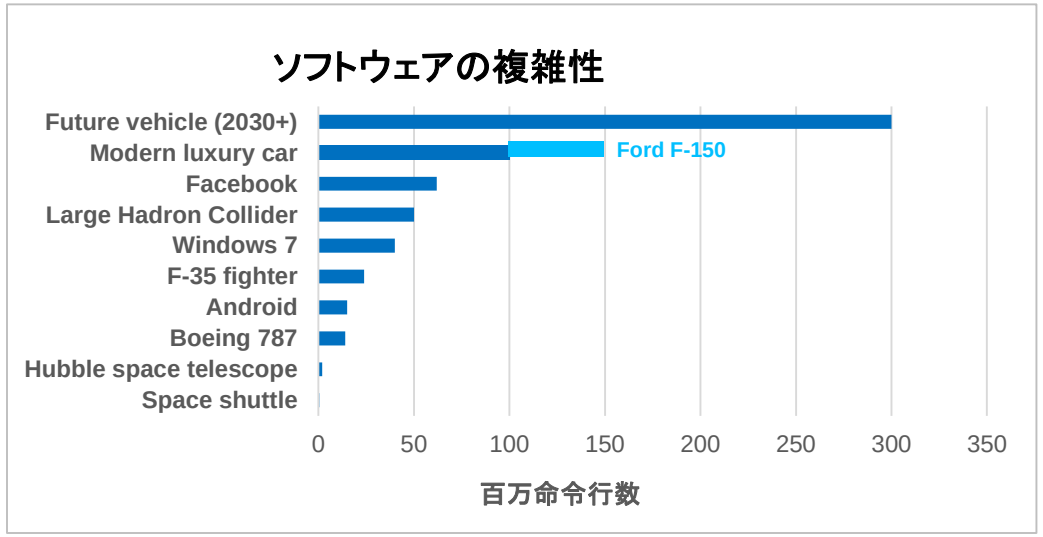
電動化
（電気自動車）

- 自動車の電子アーキテクチャの変化
- 全体的に増大する複雑度
- サイバーセキュリティ

- ハードウェアのコモディティ化、重要な差別化要素としてのソフトウェアの重要性が増加
- 電子装置 + SW = 2030年までに自動車BoMの50%

ドメインコントローラへの遷移





現在

- 60～100個以上のECU
- 6～8個のOS
- 各々が単独で動作
- コストと複雑性が増大
- 最低レベルのアップグレード機能

将来

- 6～10個の高性能コンピューター (HPC)プラットフォームへ移行
- 統合されたソフトウェアシステム
- 協調分散処理
- 重量、コスト、複雑性の低減
- OTAアップグレード機能による将来機能の保証

資料: 戦略分析、informationisbeautiful.net

二つの重要なチャレンジ

サイバーセキュリティー

車はサイバーセキュリティ攻撃の大きなターゲット

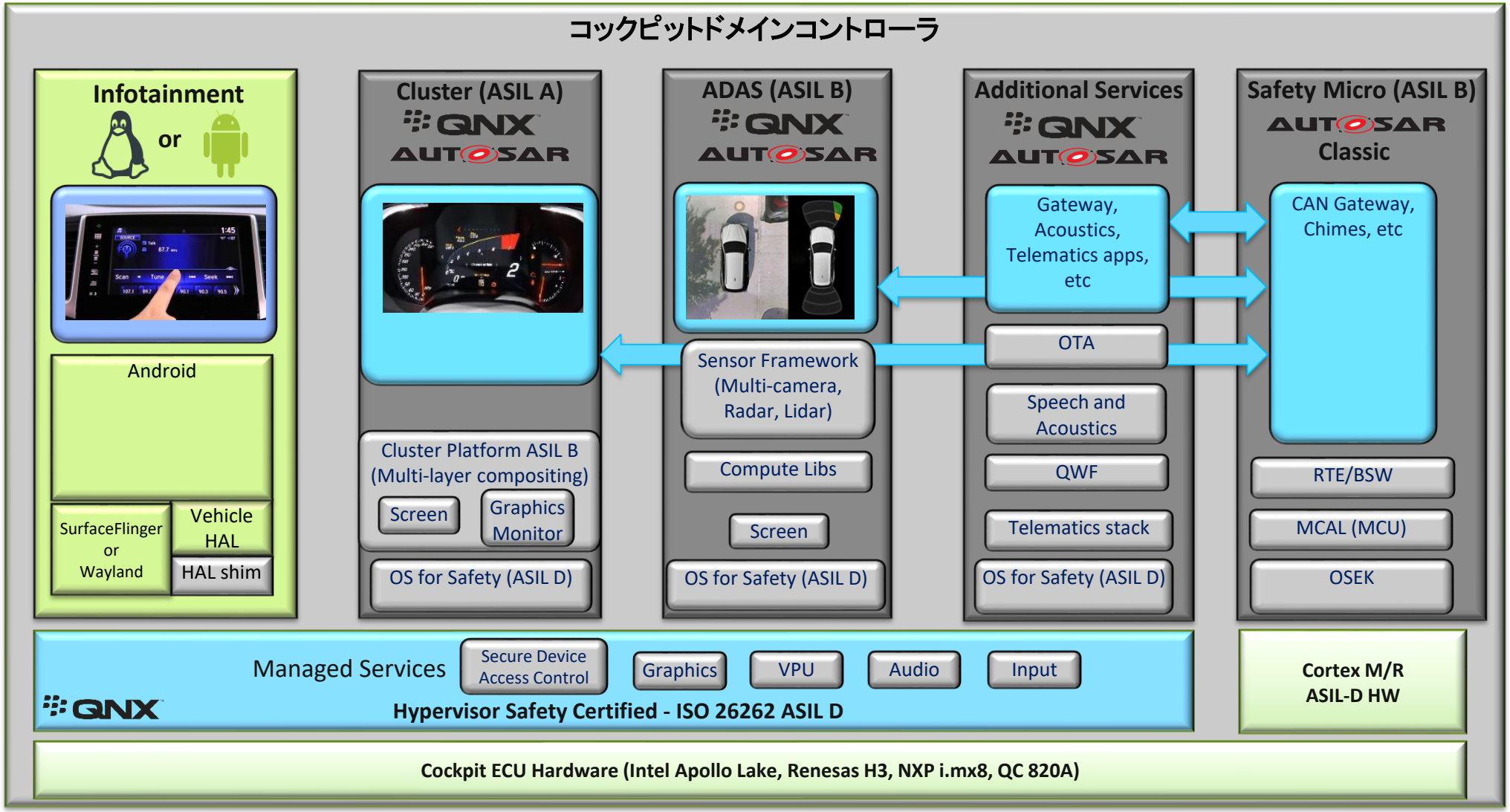
- ソフトウェアが如何に安全かを確認できるか？

ソフトウェアの複雑性の増大

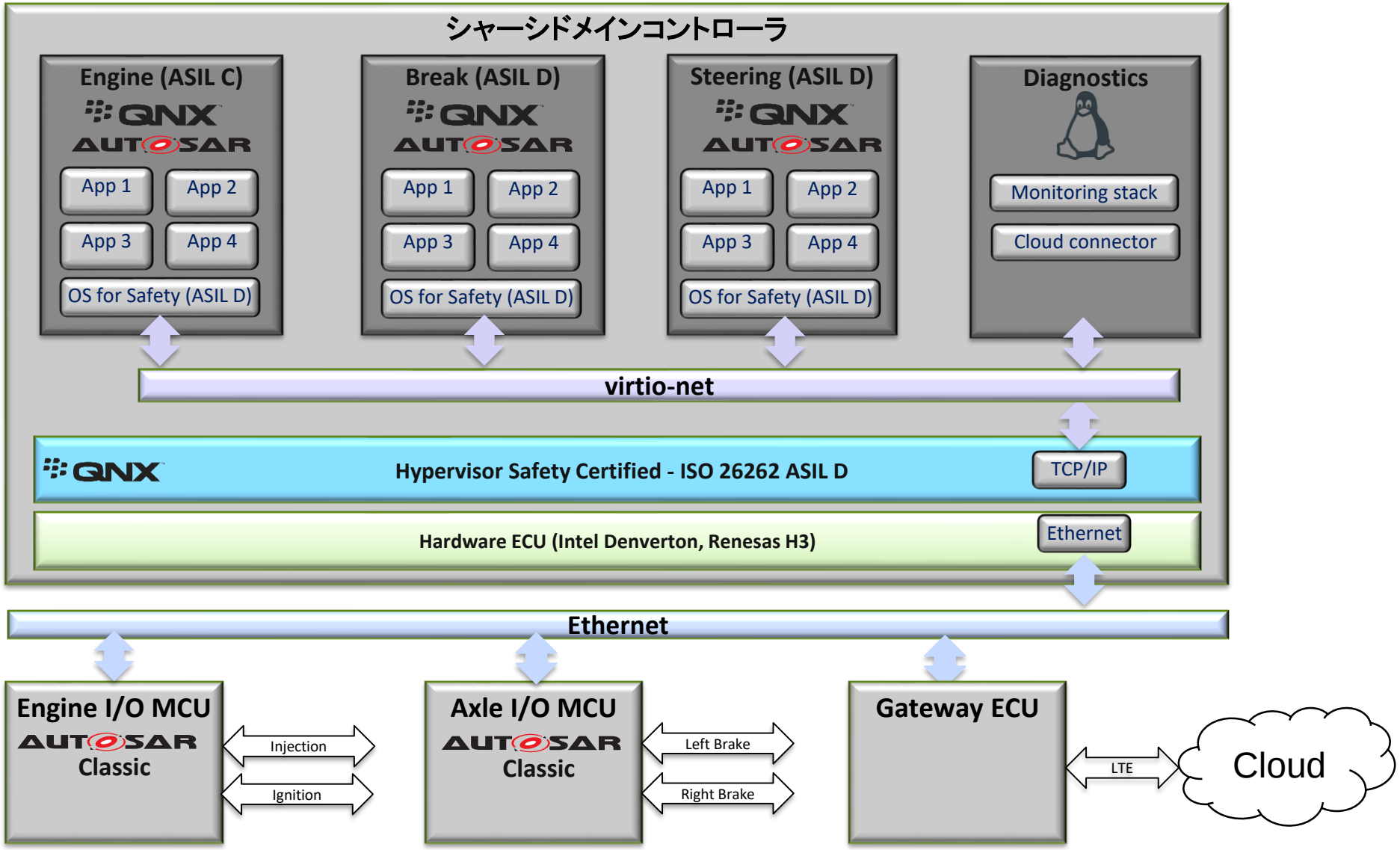
ソフトウェアは、車のクリティカルなドライブシステムを制御している

- 正しいソフトウェアをどのように選択するか？
- ハードウェアとソフトウェアの統合化をどのように実現するか？

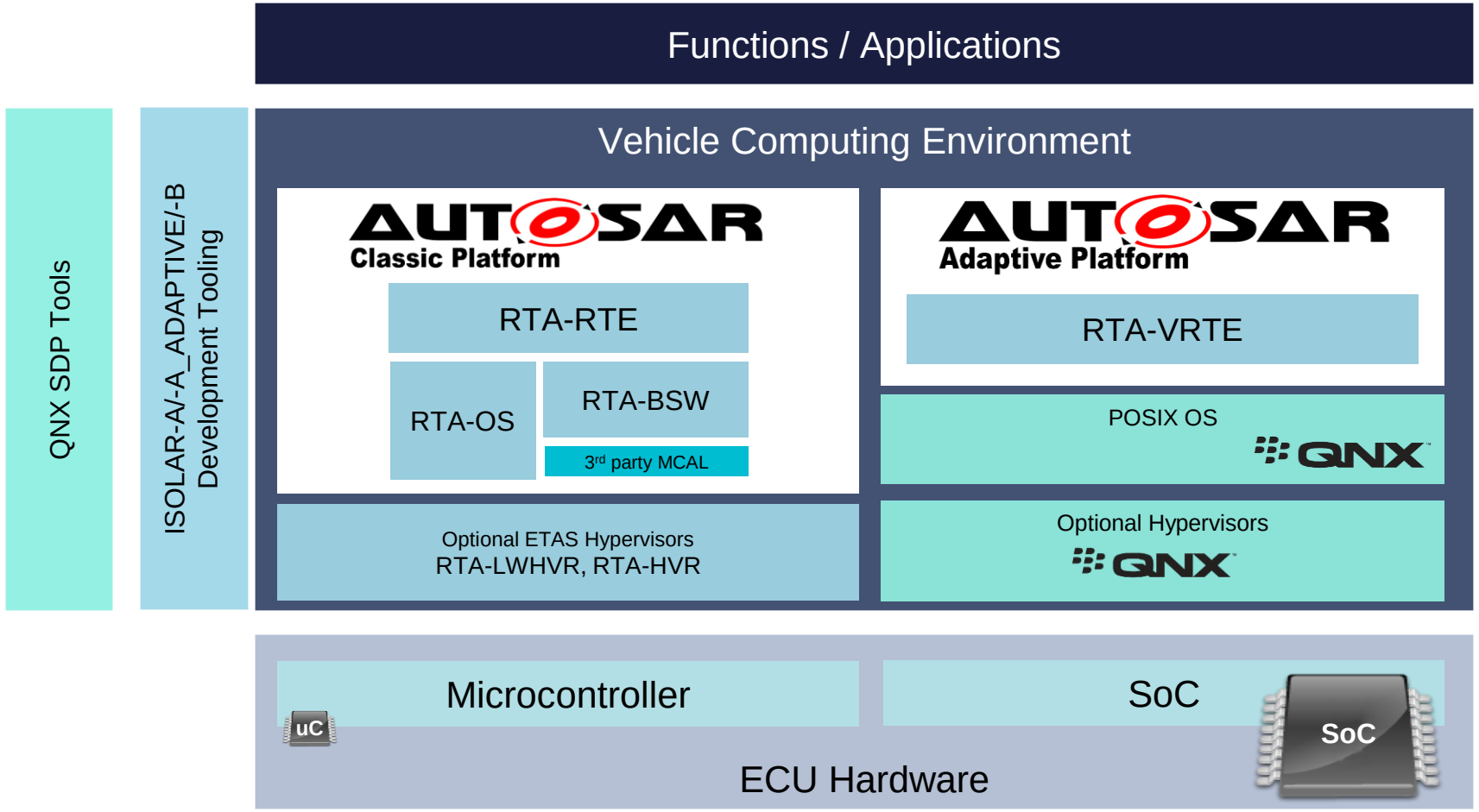
集約化の例 1



集約化の例 2



Combined Portfolio of Products



Safety Case

Evidence of the ASIL-D compliant process

Certified QNX OS

Safety Certificates

Certificates for RTA and QNX Tools

Safety Manuals

Guideline on using our products in an ASIL-X environment

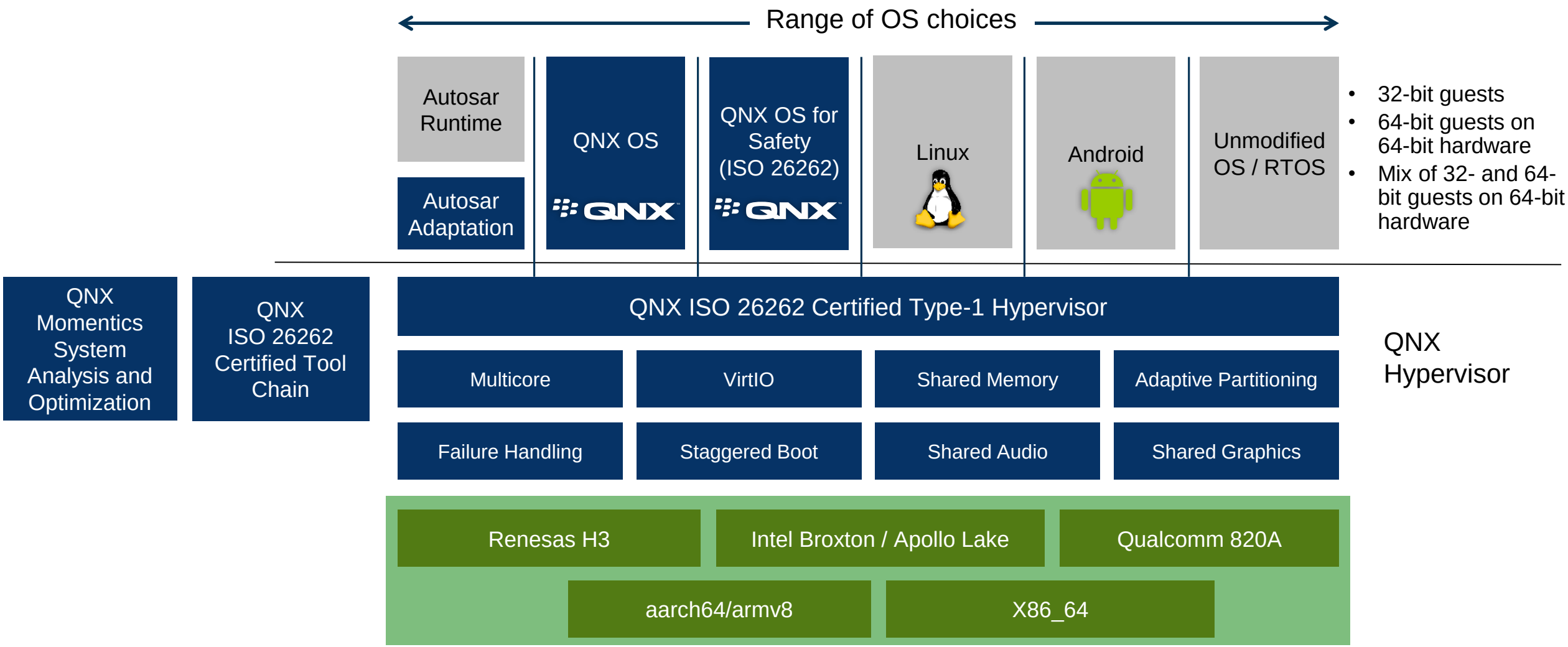
ETAS AUTOSAR Products / Solutions

QNX

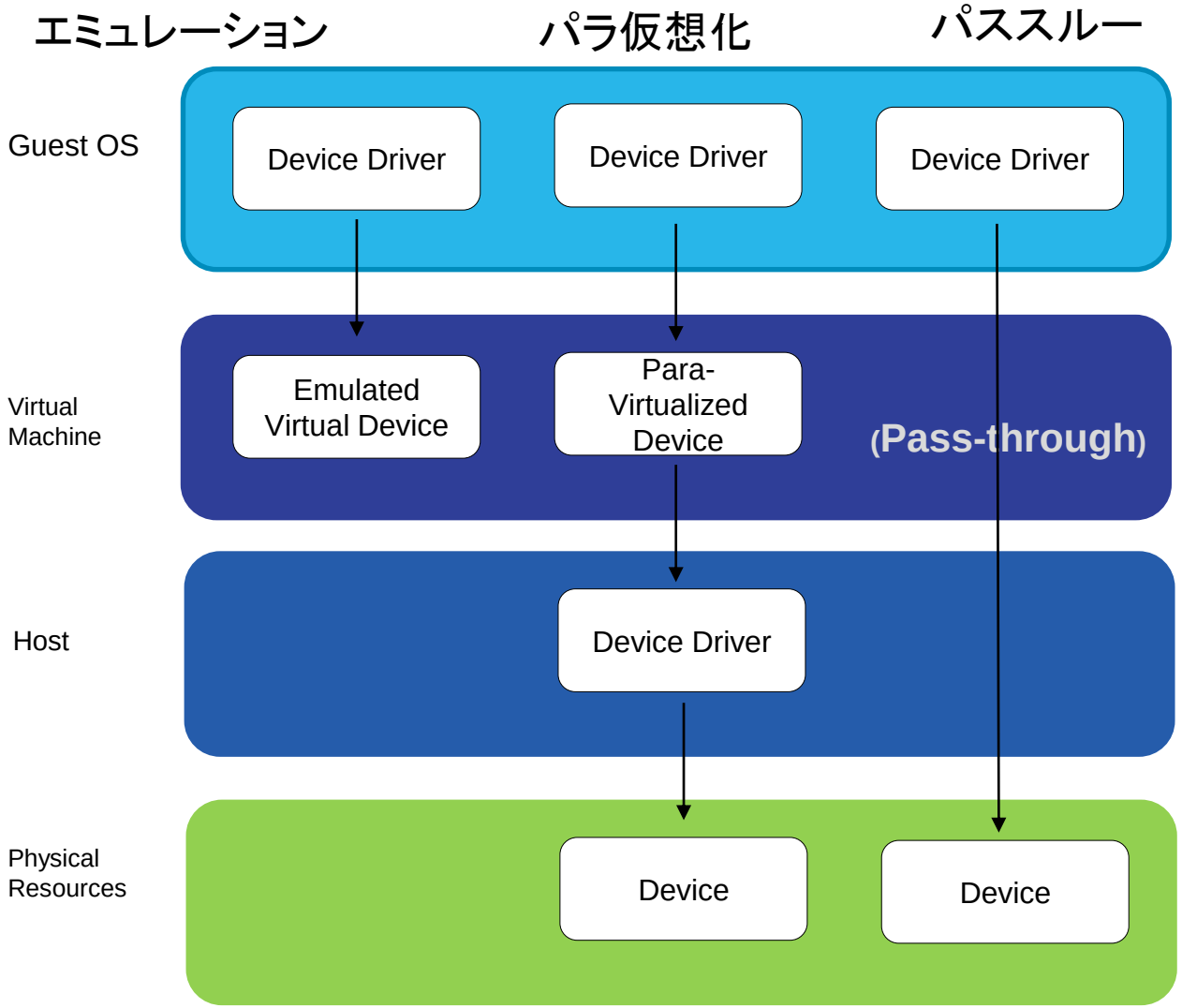
ドメインコントローラ実現に必要な技術

- Hypervisor の機能安全 ISO26262 ASIL D対応
- OSの高度なセキュリティー機能
- サイバーセキュリティーへの対応
- libC++の機能安全対応 (Adaptive AUTOSAR)
- libmの機能安全対応 (自動運転アルゴリズム）
- Adaptive AUTOSAR, Classic AUTOSARの対応
- AUTOSARベンダーとの密な関係による最適化

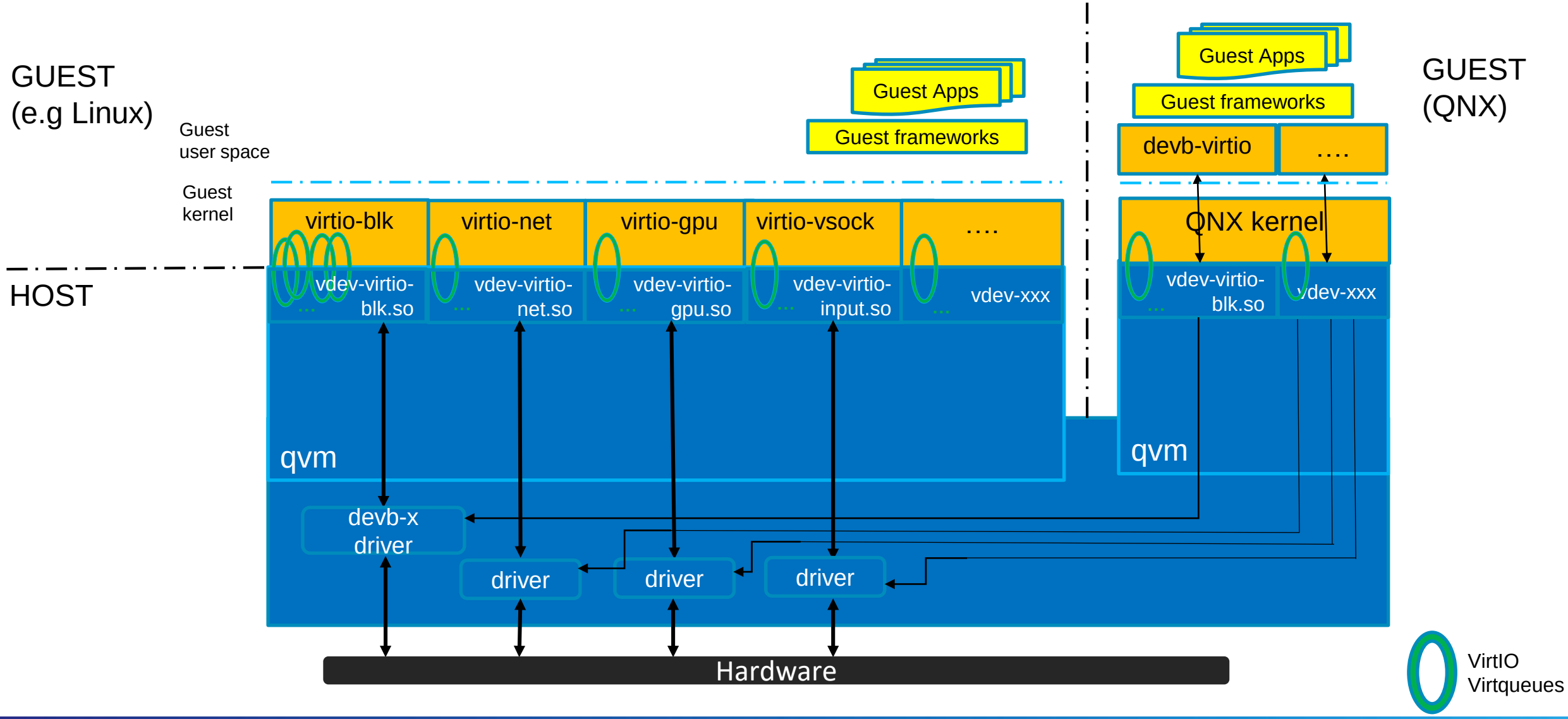
QNX ハイパーバイザープラットフォーム



ハイパーバイザーのデバイス共有

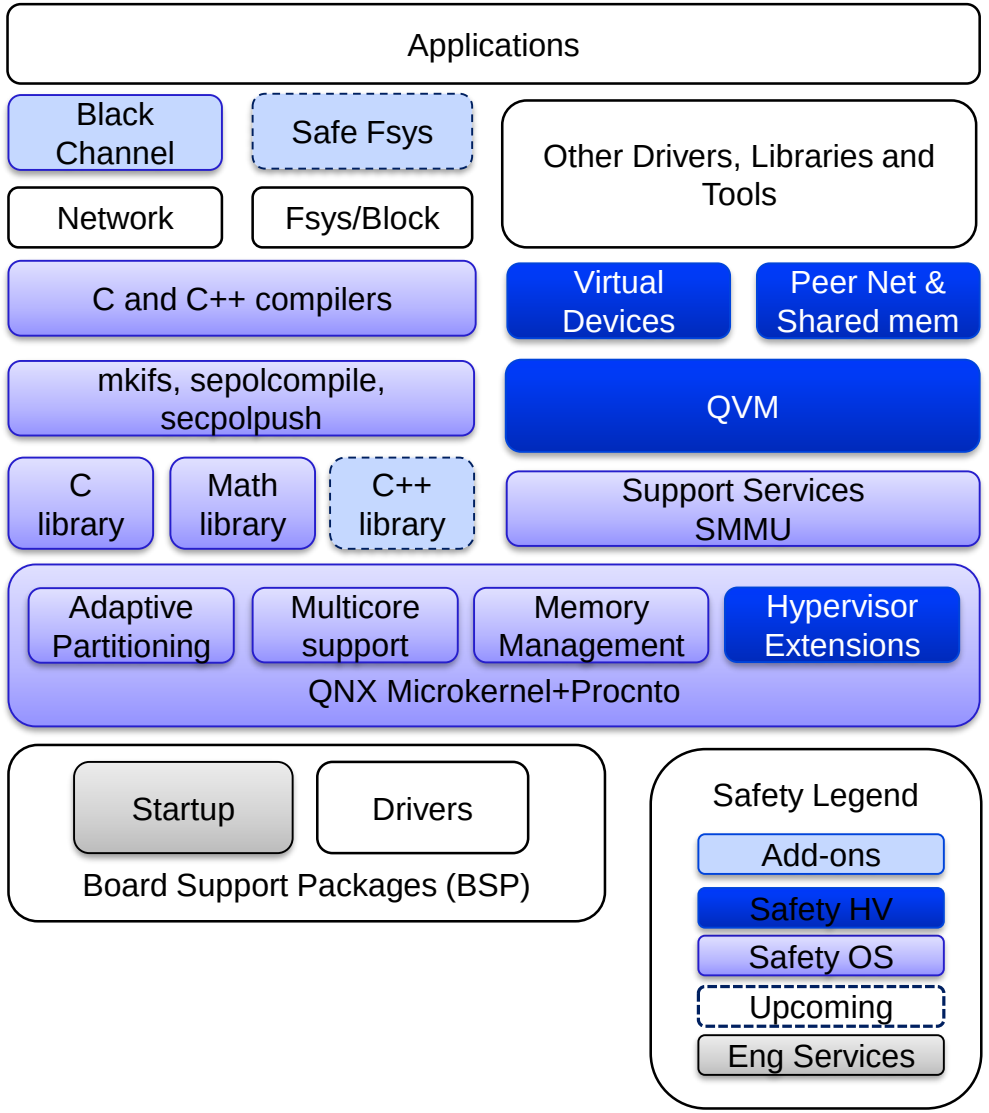


Virtual IO on QNX



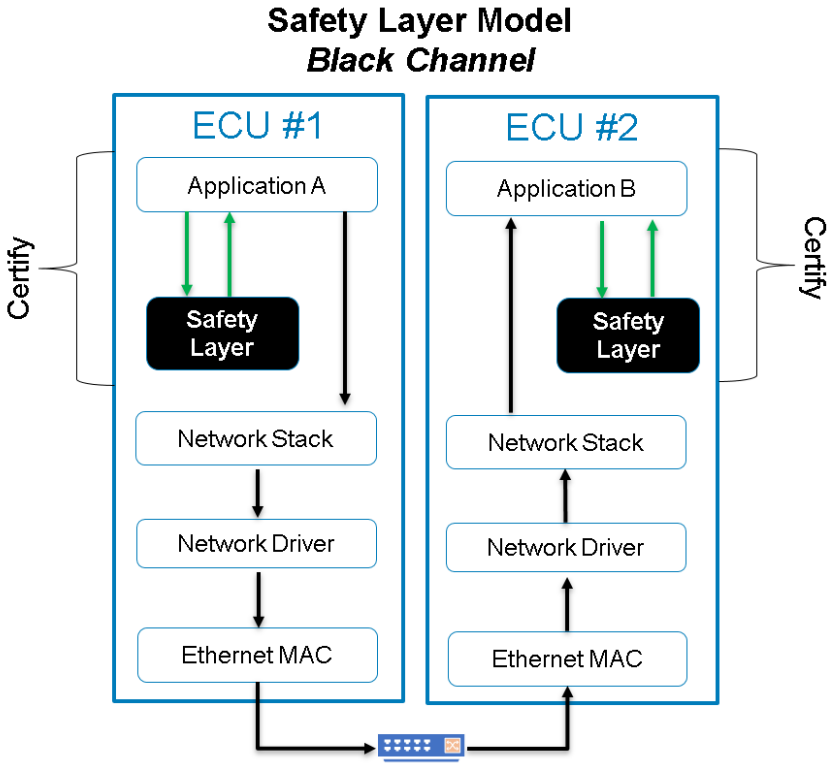
Safety Products

- **QNX OS for Safety (QOS)**
  - ARM, x86 64ビットハードウェアプラットフォームのQNX SDPにコンパチブル
  - マイクロカーネルとプロセスマネージャー、マルチコアサポート、アダプティブパーティショニングスケジューラー
  - システムライブラリー: C, Math, C++ ライブラリーの認証
  - 認証を受けたQNXユーティリティー
  - ツール: C、C++ コンパイラー, リンカー, アセンブラーTCL3
- **QNX Hypervisor for Safety (QHS)**
  - QNXマイクロカーネルへのハイパーバイザー拡張
  - QVM ゲスト管理システム
  - パラ仮想化のサポート (VirtIO)
  - ピアネットワーク
  - ゲスト / ホストシェアードメモリー
- **Safety Certified Add-on Products**
  - QNXブラックチャンネルコミュニケーション; QNX Black Channel Communications Technology (QBCCT)
  - 認証済みの C++ システムライブラリー
  - QNX セーフファイルシステム (レビュー中)

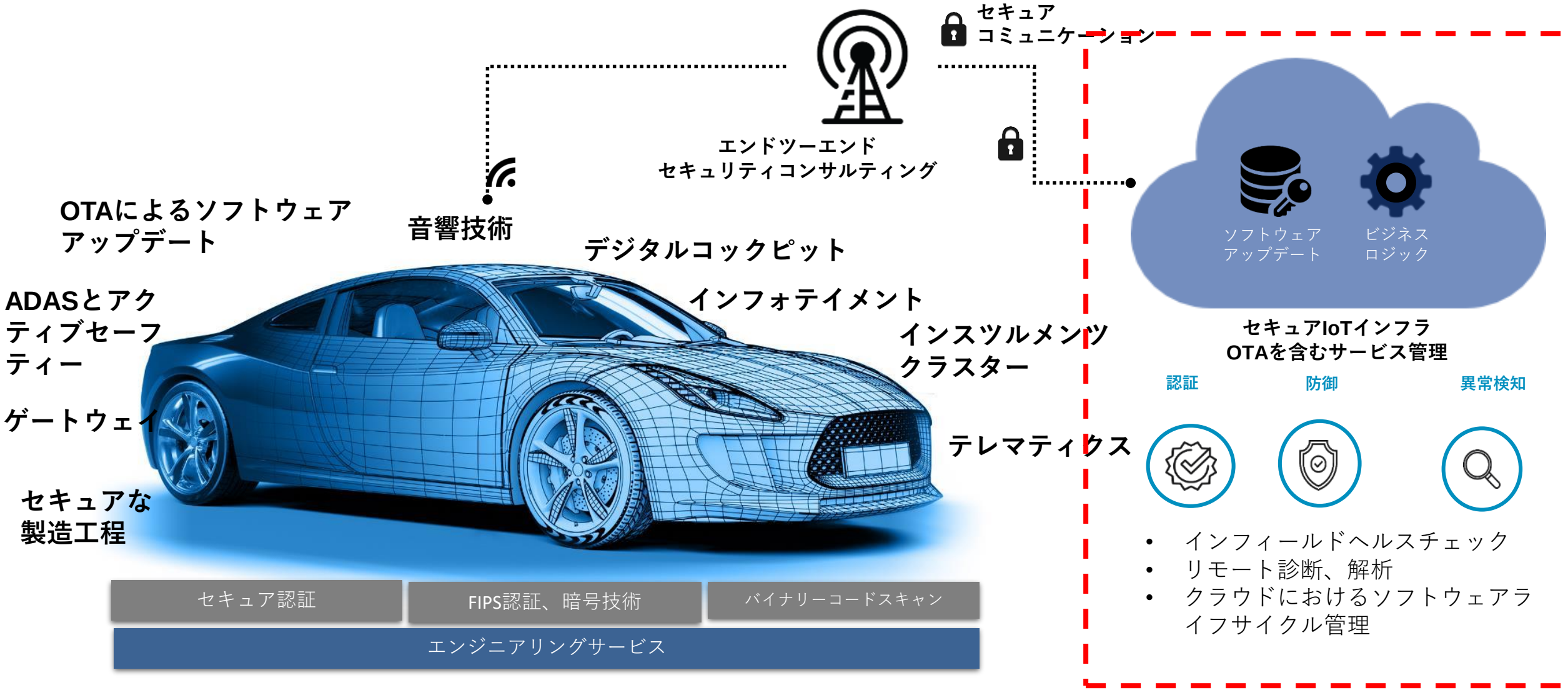


QNX Black Channel Communications Technology 1.0

- ISO 26262 ASIL D認証済みのセーフコミュニケーション
- ハードウェア、通信ソフトウェアを利用し、ポイントツーポイントでやり取りされるデータを保護
- 完全性（改ざんがないこと）のチェック、認証、データ損失の検出ならびに他の方法を提供するセーフティーレーヤーを提供 (IEC 61784-3、AUTOSARで定義されている)
- 標準的なシステム、ならびに機能安全標準に準じて認証を受けるシステムに利用可能
- システムのセーフティーケースを実現する場合、通信コンポーネントを組み込む際、コストを低減することが可能.
- QNXと非QNXシステム (Linux, SafeRTOS) 両方で利用可能



BlackBerry QNXのカバーする範囲



車載標準化の拡大

サイバーセキュリティー

- **ISO/SAE 21434**
- J3061の継承
- 安全性、財務性、運用性、プライバシーの問題を発生するE/Eコンポーネントへの悪意のある攻撃に対するセキュリティー （ネットワーク、クラウドは対象外）

機能安全

- **ISO 26262**
- E/Eコンポーネントにおける故障イベントに対する安全性の確保

意図した機能への安全性 (SOTIF)

- **ISO/PAS 21448**
- 故障がない場合でも、意図した機能への安全性の確保

ソフトウェアアップデート

- **ISO 24089**
- 車載における有線、無線で提供される安全でセキュアなアップデート
- ISO 26262, ISO/PAS 21448, ISO/SAE 21434の参照面
  - Some content originally a part of ISO/SAE 21434
- 2022年に発行の予定

Thank You!