カーエレクトロニクスにおけるディペンダブルシステム構築について

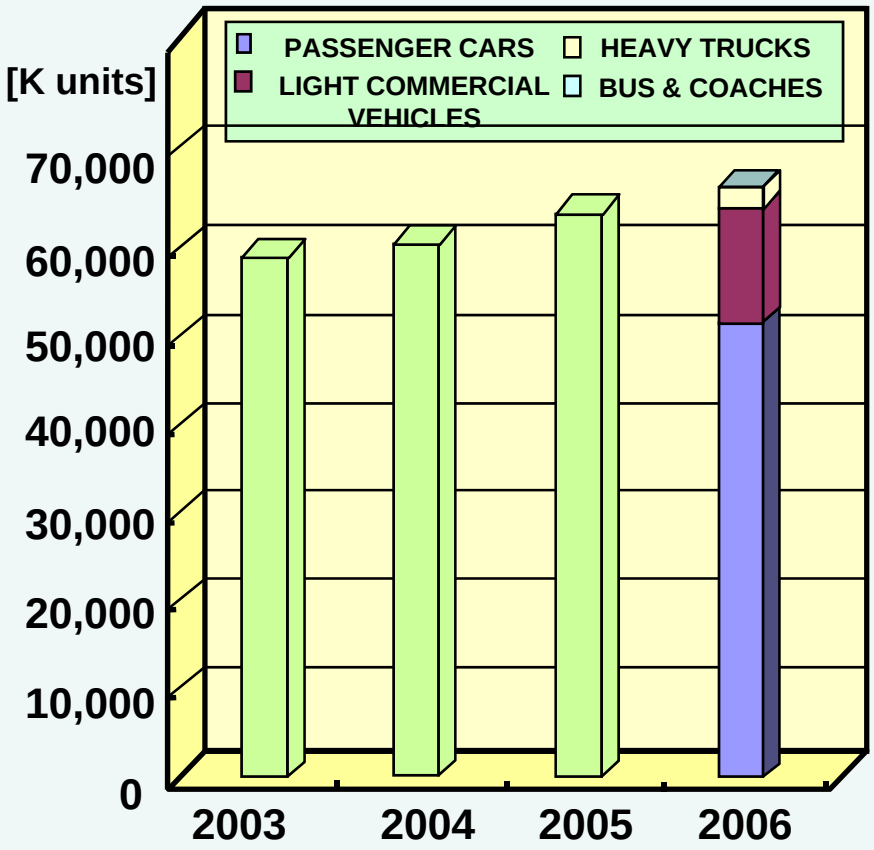
トヨタ自動車株式会社
BR制御ソフトウエア開発室
服部雅之

本日の報告内容

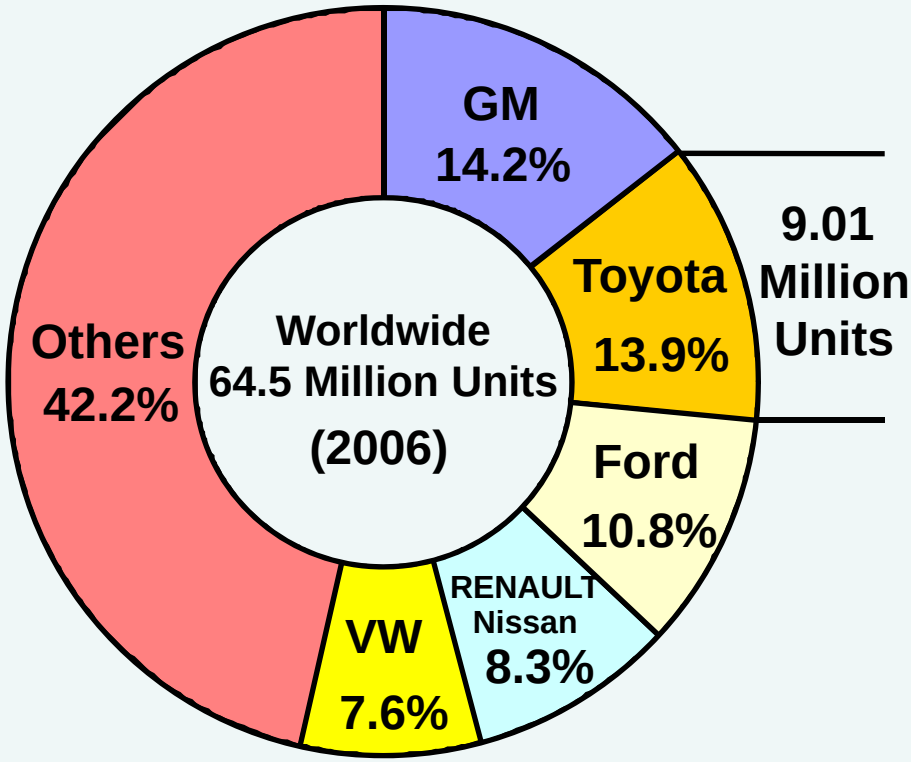
１．自動車市場/車両電子部品の現状
２．組込みシステムの将来と課題
３．自動車における統合制御技術とインフラ協調
４．自動車におけるディペンダブル設計
５．組込みシステムソフト設計について
６．まとめ

世界自動車生産実績

Worldwide Vehicle Sale

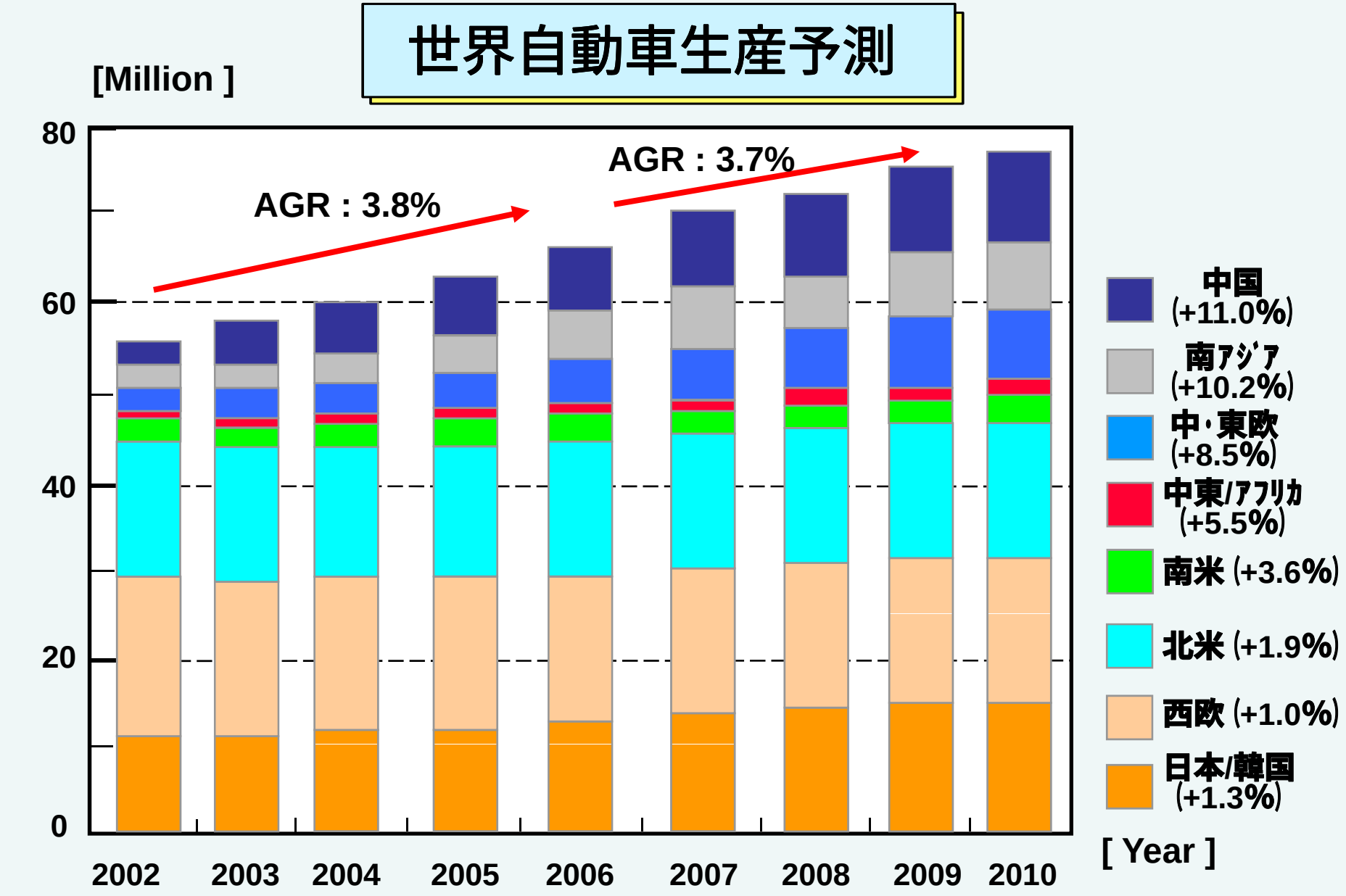


Worldwide Vehicle Sale by Manufacturer



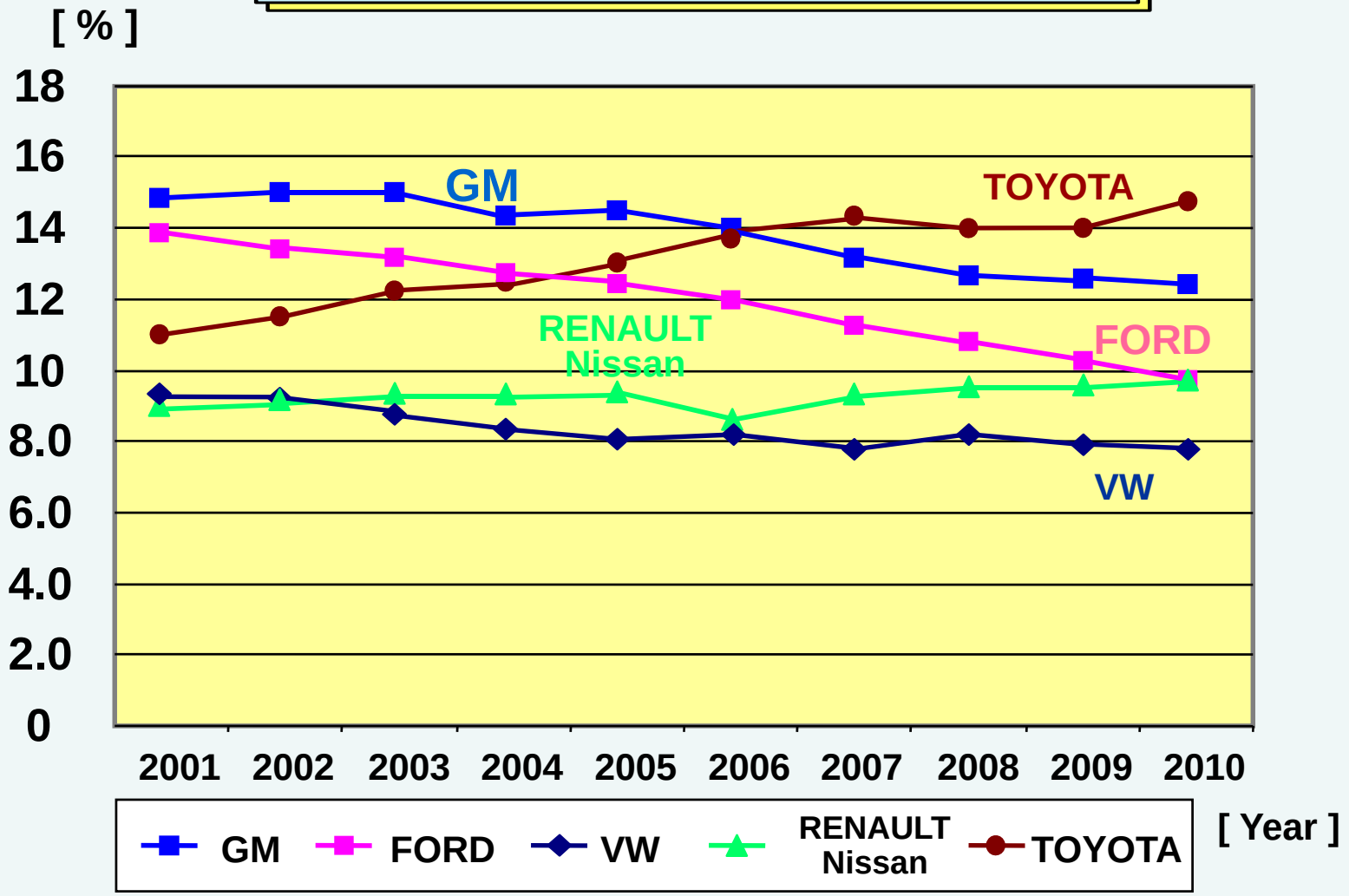
Source: FOURIN Special Reports

世界自動車生産予測



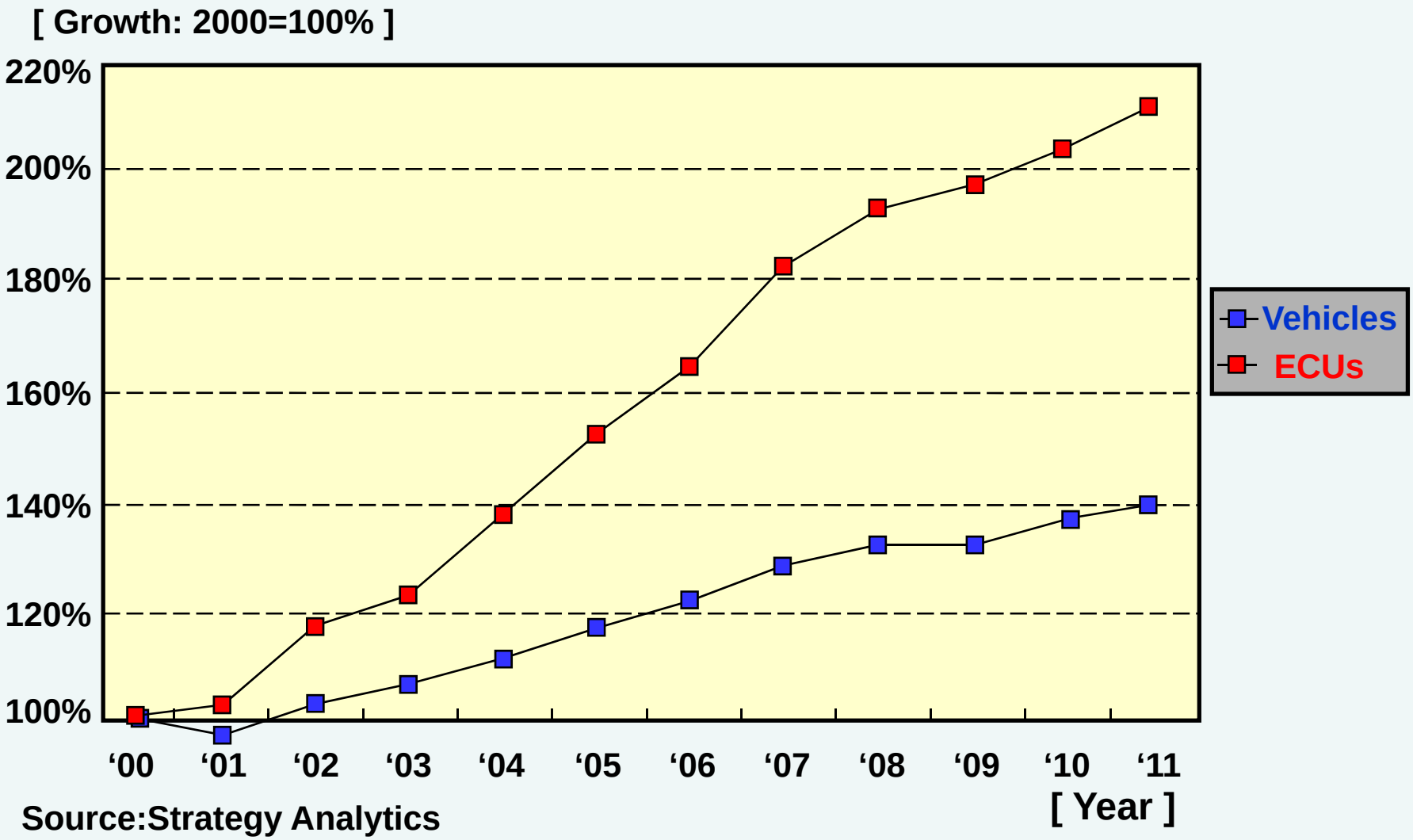
(Source: CSM World)

自動車メーカ別シェア推移



(Source: CSM World)

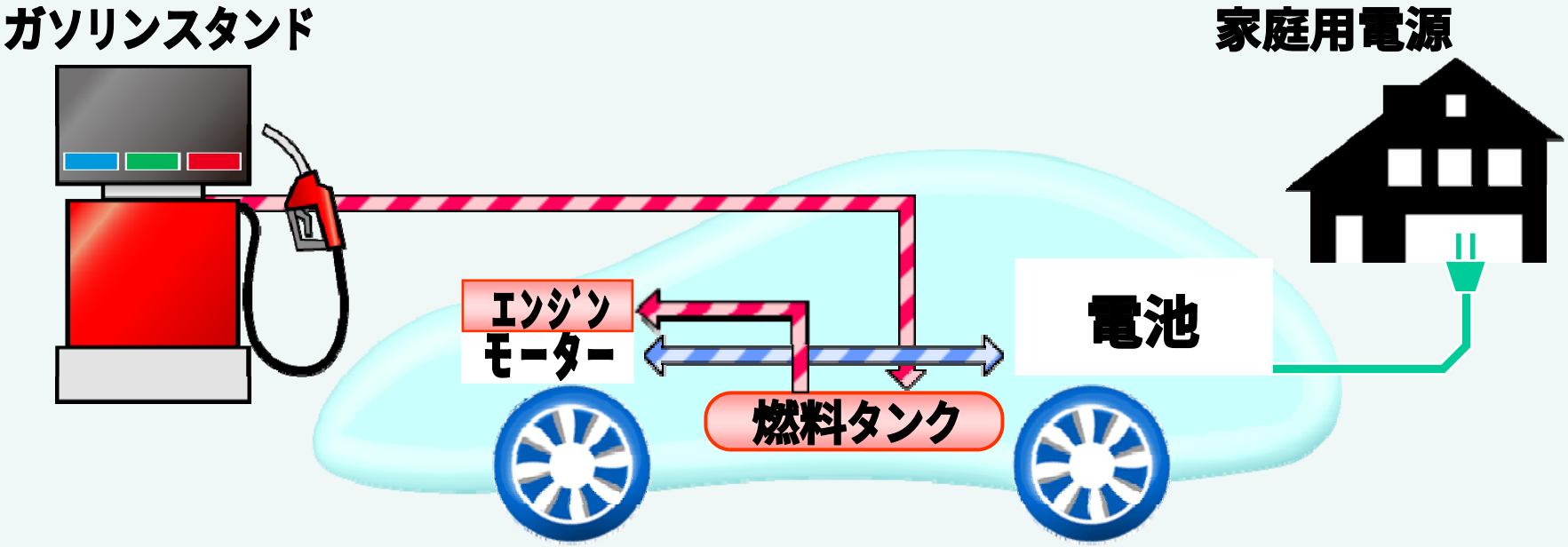
車両電子部品の成長



プラグインハイブリッド

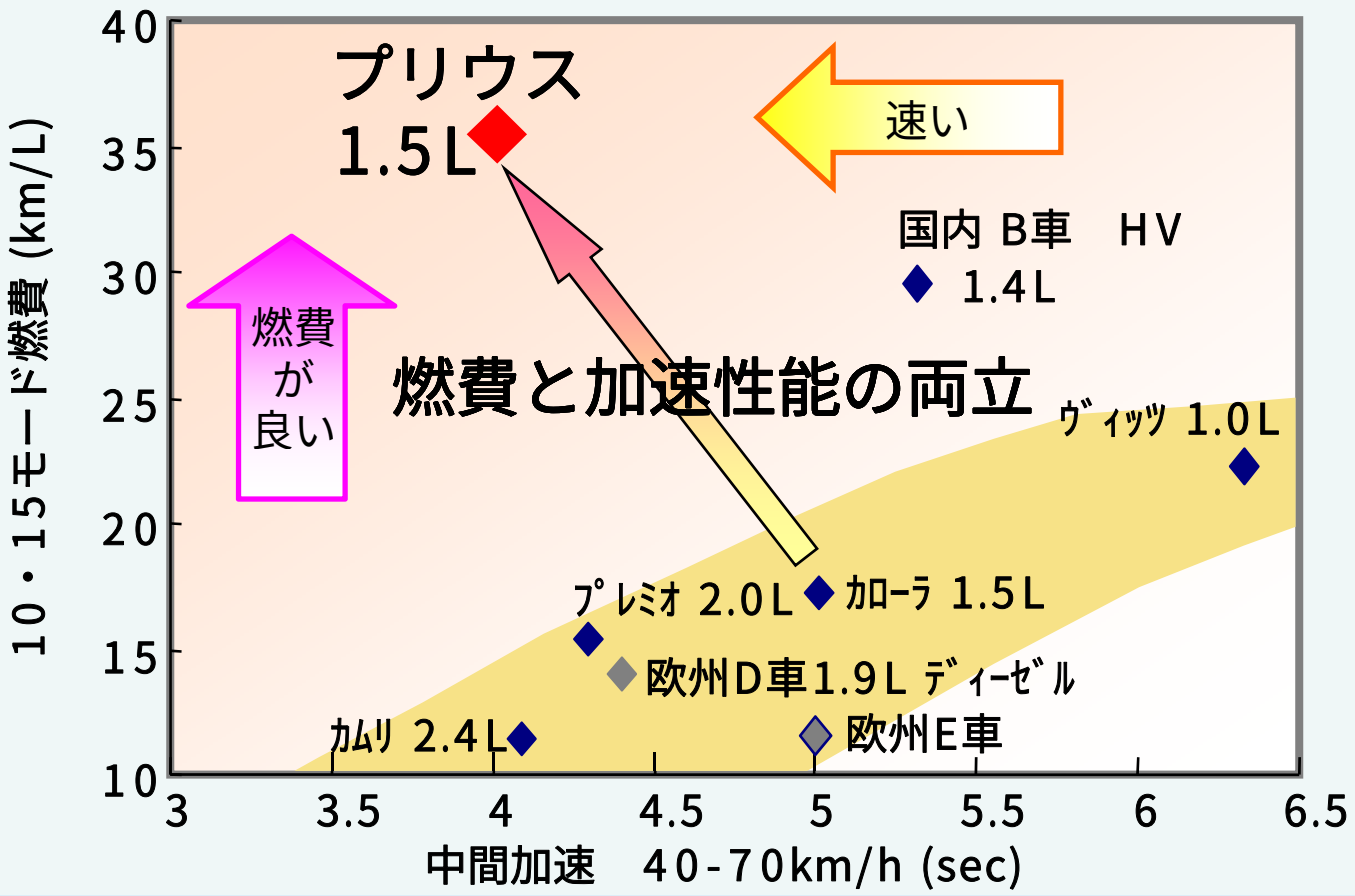
電池を外部電力で充電し、モーターによるＥＶ走行レンジを拡大

- ショートトリップは充電電力でのモーターによるEV走行
- 長距離、高速、登坂はエンジンとモーターによる走行



電気利用車両の現実的な在り方として期待

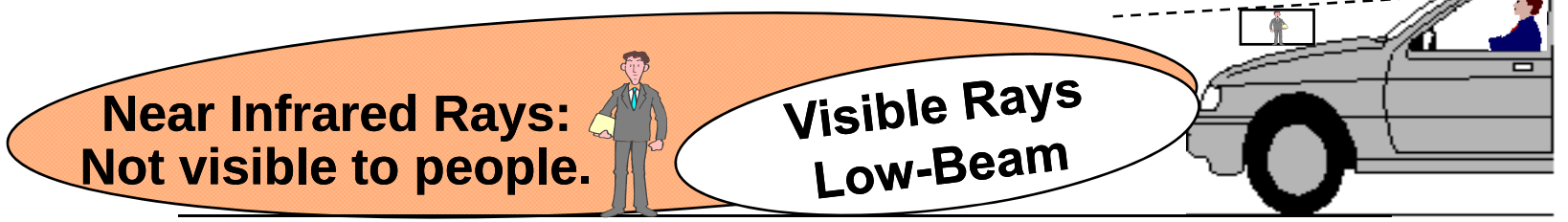
ＨＶの燃料効率と加速性能



ＨＶは燃費向上において加速性能を犠牲にしない

Night View System

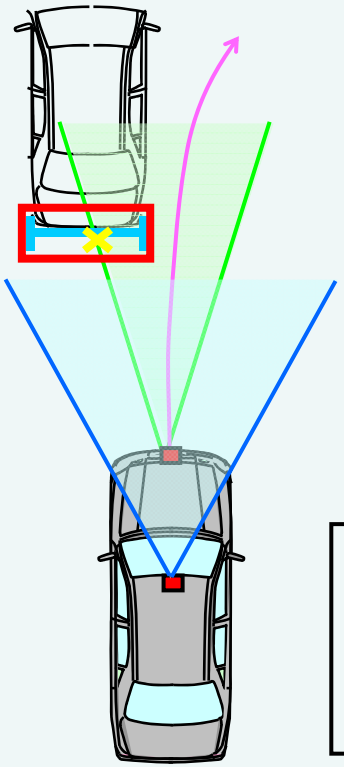
Concept

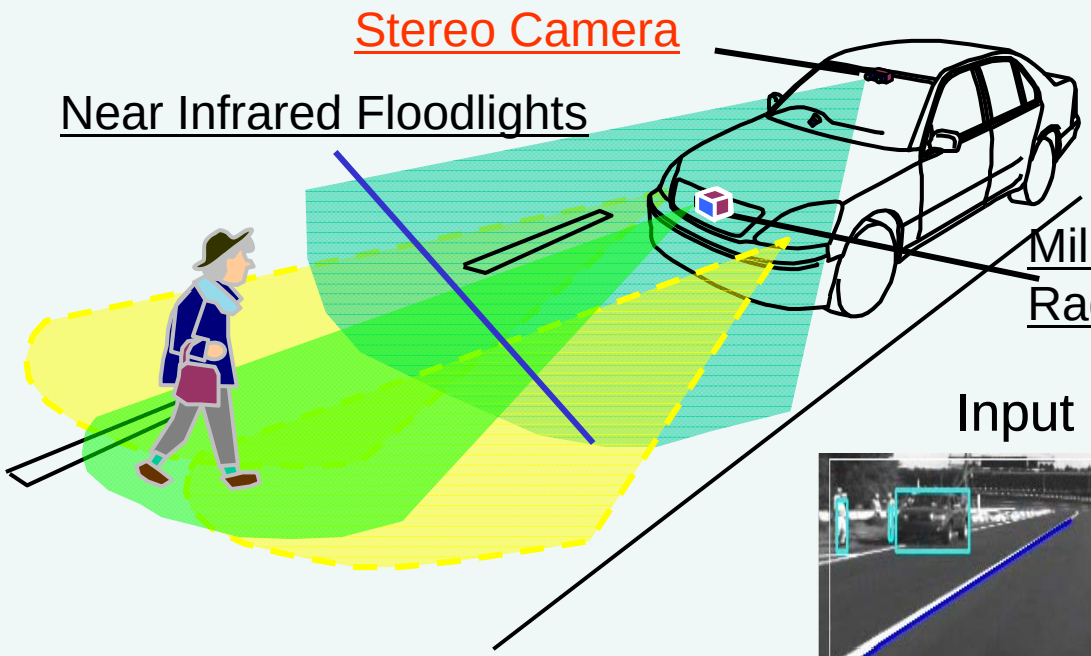


Real View

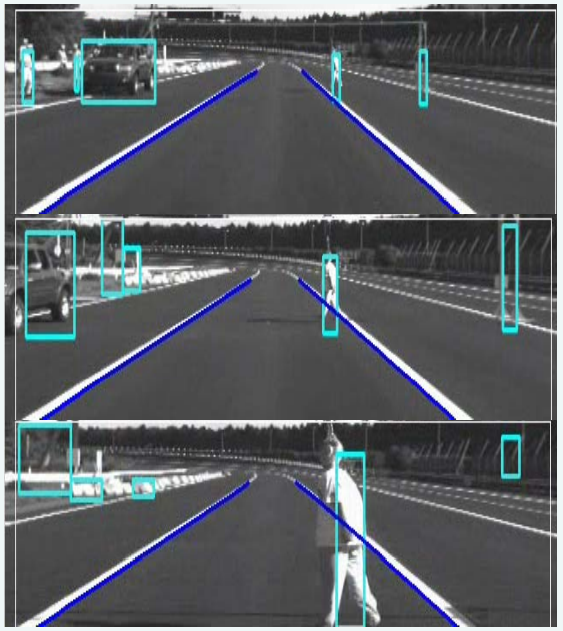
Night View System

障害物検知方式





Input image



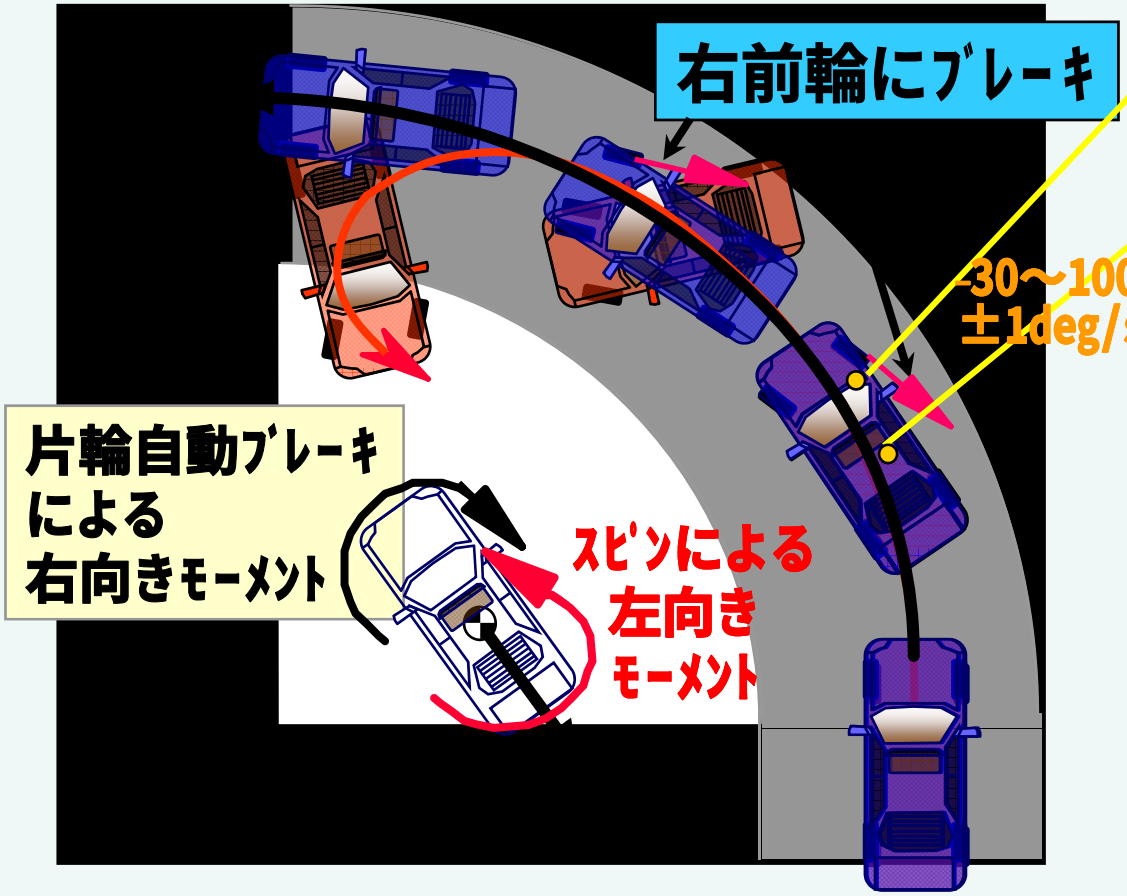
Camera info.
Radar info.
Fusion result

Effect of sensor fusion

VDIM System

進化

VSC ⇒ VDIM



-30～100℃
±1deg/sec

ｽﾃｱﾘﾝｸﾞ角度ｾﾝｻ

比較

ﾖｰﾚｰﾄｾﾝｻ

車両状態量推定

フィードバック

スピン判定

ﾄﾞﾘﾌﾄｱｳﾄ判定

ブレーキ,エンジン制御

サスペンション,ステア制御

マルチメディアシステム

いざというときの心強いサポート

ドライブサポート

目的地設定
施設情報案内
交通情報案内
駐車場案内
ニュース配信
天気予報

セキュリティサービス

まさか・・・

クルマが急に心配に・・

車が盗難にあってないか心配に！

携帯で調べよっ

良かった！車の位置は変わってないわ！

マイカーサーチ　始動時通報

盗難ｱﾗｰﾑ連動・対処員派遣

盗難発生

位置追跡

警備員派遣

ｴﾏｰｼﾞｪﾝｼｰｻｰﾋﾞｽ

うっかり・・・

よく知らない場所で脱輪！

あっ！

お願い助けて！

助かりました

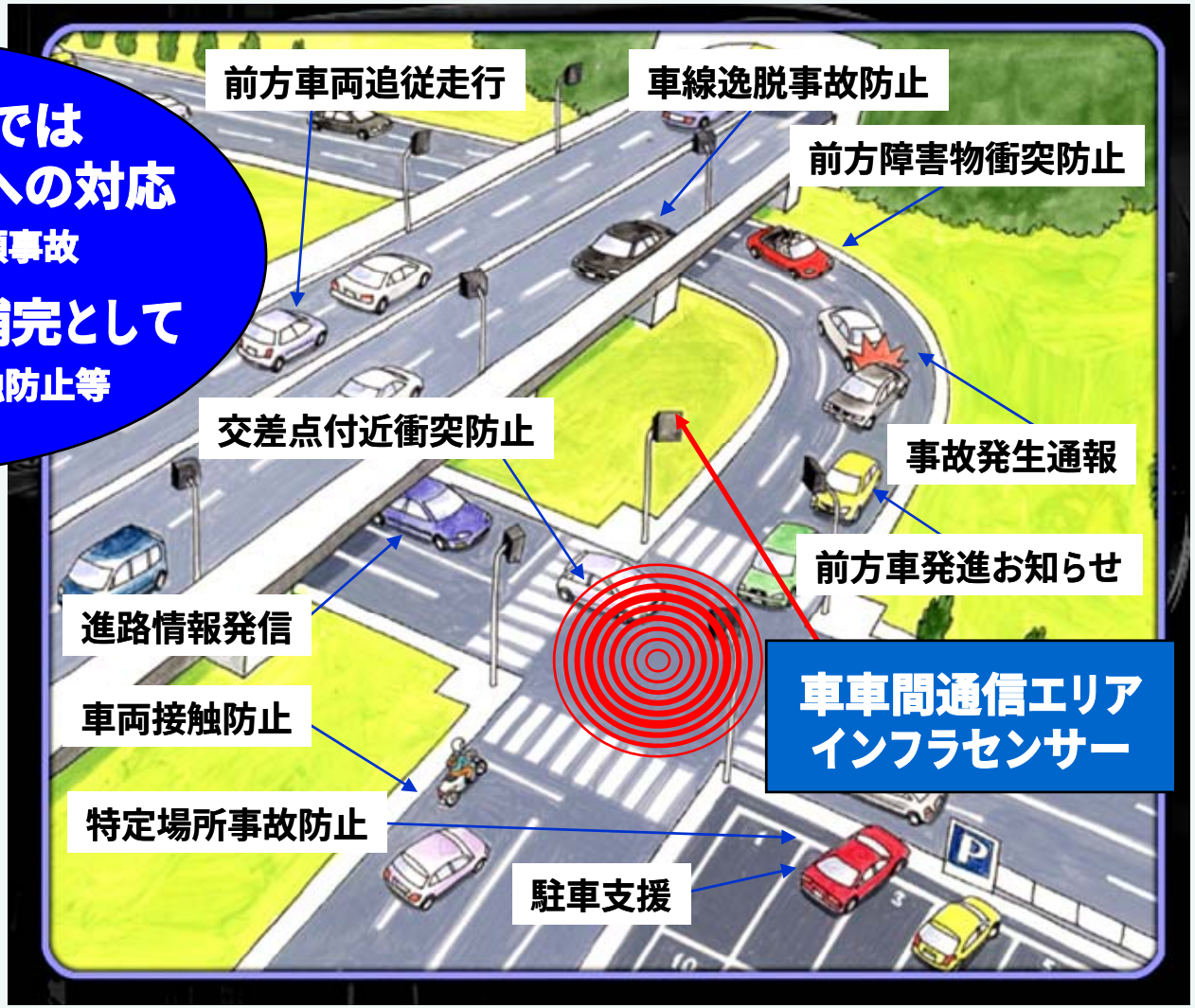
場所がわかってるから早いんだ

ロードサポート２４

インフラ協調システム

自律機能だけでは
実現できないものへの対応
交差点での出合い頭事故

自律システムの補完として
車線変更による接触防止等



車載電子システムの特徴（１）

必要要件

１）*リアルタイム制御*

２）*安全性・信頼性*

３）法規対応

４）低コスト

５）利便性・快適性

６）厳しい使用環境

具体的事例

・エンジン高速回転時
６気筒ｴﾝｼﾞﾝ@５０００rpm回転時、
点火・噴射演算は4msec毎に実行

・急ブレーキ、タイヤスリップ時
ｽﾘｯﾌﾟ状態を判定し、制御目標ﾀｲﾔﾛｯｸ率
を瞬時に判定しﾌｨｰﾄﾞﾊﾞｯｸ制御

・車両衝突時
衝突か否かを瞬時に判定し、複数のｴｱﾊﾞｯｸﾞ
を衝突形態に合わせて順次起爆

特徴

① 複数の仕事が割り込みにより集中
② 規定以上の遅れは許されない
③ 誤動作は命取り

車載電子システムの特徴（2）

必要要件

1）リアルタイム制御

2）安全性・信頼性

3）法規対応

4）低コスト

5）利便性・快適性

6）厳しい使用環境

特徴

・使われ方、法規は各国様々
世界各国で特殊な使われ方・法規が存在
>>安全性、大気汚染、電波、灯火
近い将来、排気ｶﾞｽは大気よりｸﾘｰﾝになる

・法規は常に変化する
政治（保護貿易）の道具にされることも
法規は社会・文化・経済を反映して変化

・法規対応費用はコスト削減で吸収
法規対応はﾒｰｶの責任

参考
・セキュリティシステムは泥棒との競争
・排気ガス規制は各国で異なる
⇒東京都ディーゼル規制・・・
等々

車載電子システムの特徴（３）

必要要件

１）リアルタイム制御

２）安全性・信頼性

３）法規対応

４）低コスト

５）利便性・快適性

６）厳しい使用環境

特徴

・過酷な世界競争
自動車は高額耐久消費財、政治/経済と密接
市場の成熟により各国の競争激化
莫大な研究開発費、設備投資が必要

・車載半導体は特別製
汎用の素子は使えない（温度・信頼性等）
１０年以上の信頼性が必要
１０年以上の継続生産が必須（補給対応等）
家電並みのｺｽﾄを要求（ｵｰﾃﾞｨｵ等）
カスタム指向の半導体開発
ﾊﾞﾘｴｰｼｮﾝの多さ、少量多品種生産

高機能/高信頼性の割にはコスト高

車載電子システムの特徴（４）

必要要件

１）リアルタイム制御

２）安全性・信頼性

３）法規対応

４）低コスト

５）利便性・快適性

６）厳しい使用環境

特徴

・走行中でも使い易い機能
瞬時の操作が要求される
衝突時は部品が凶器になる怖れも配慮

・車と家電のギャップ
お客様は常に最新の機能を要求
一方、車は簡単に買い替えてもらえない
⇒時代を先読みした装備が必要

・お客様は神様
使い勝手・快適性は千差万別
（ﾏﾆｭｱﾙや注意事項は守ってもらえない）
木目細かくご要求に応えることが肝心

カーエレクトロニクスのフレキシビリティは商品性向上のために必要

車載電子システムの特徴（５）

必要要件

１）リアルタイム制御

２）安全性・信頼性

３）法規対応

４）低コスト

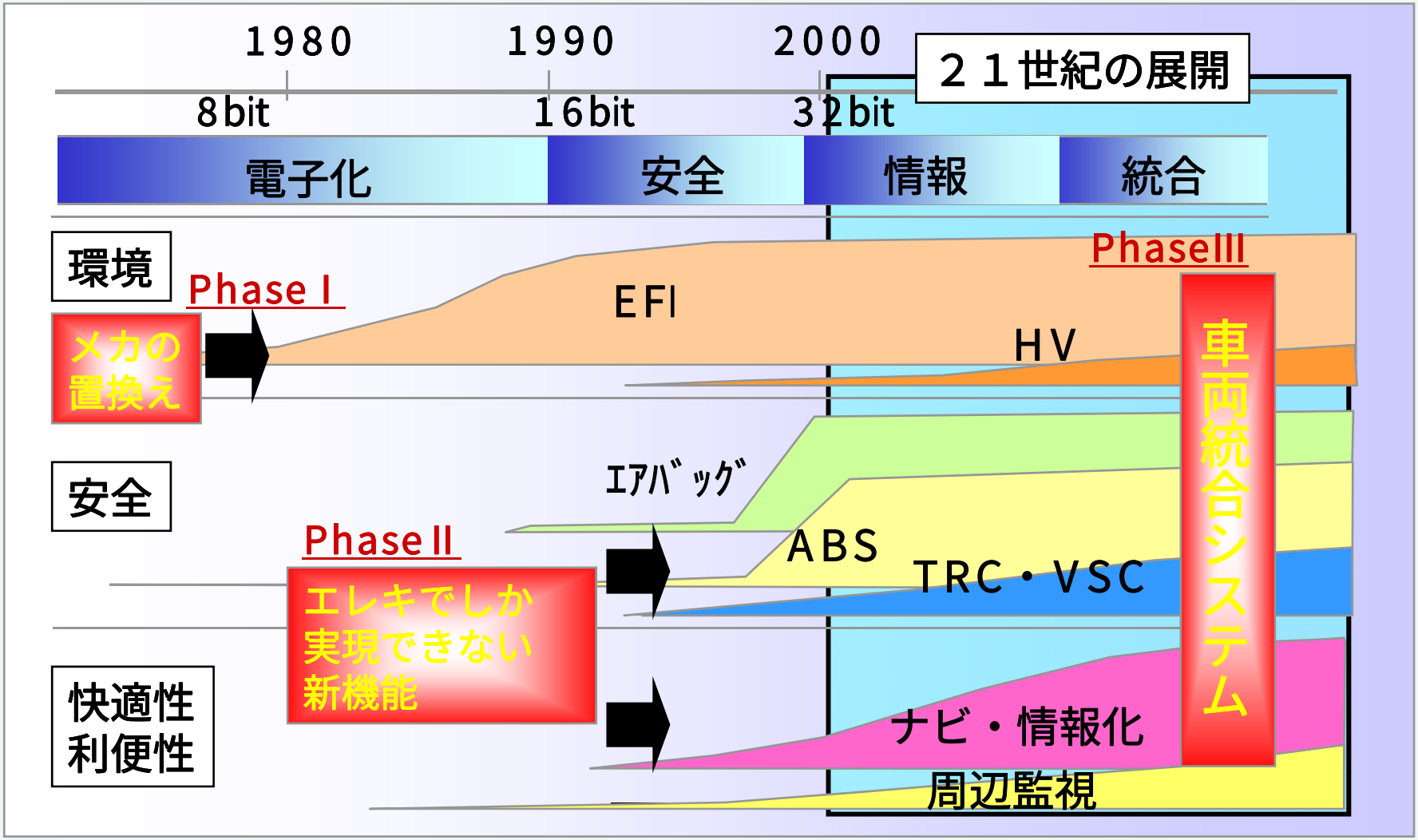
５）利便性・快適性

６）厳しい使用環境

特徴
・車の使われ方は様々
　シベリアからアフリカまで世界各地で使用
　お客様の使われ方、感性は千差万別
・半導体には厳しい使用環境
　PC、携帯等に比べて過酷な温度・振動環境
　１０年以上の信頼性はあたりまえ

参考
・道路公団の車はバックで数キロ走行
・タクシーの走行距離は十万キロ以上
・東南アジアでは室内も洗車（家畜並扱い）
・VIPの車は毎日アイドルで数時間待機
・高出力放送用アンテナの直下でも動作
・エンジンルームは１００℃以上
・真夏の車内は５０℃、インパネは１００℃以上
等々

自動車用電子システムの推移



➢ 対象システムの急拡大と機能の統合による新規性向上

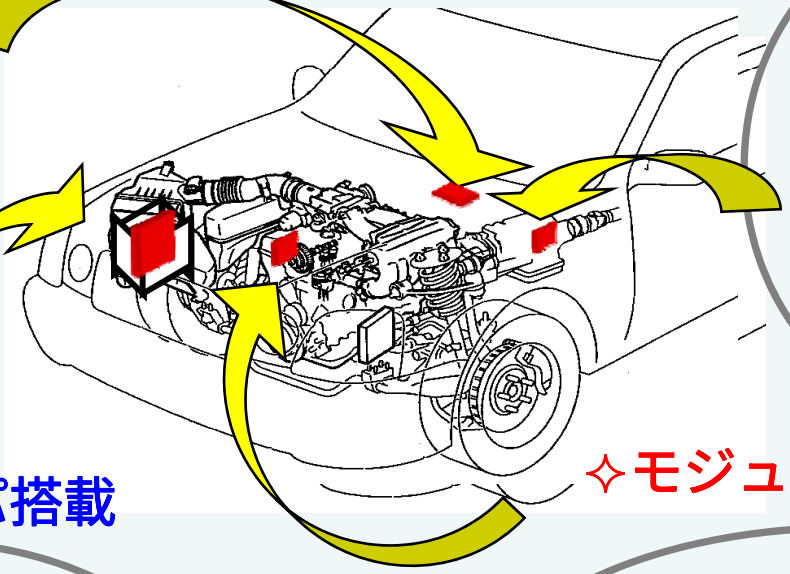
必要な演算性能

車両電子部品の技術動向（１）

高温対応・小型化技術開発が必須

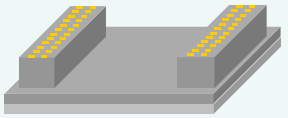
これまでの搭載 ➡ 今後の搭載

✧車室内



✧直載ＥＣＵ

側面搭載



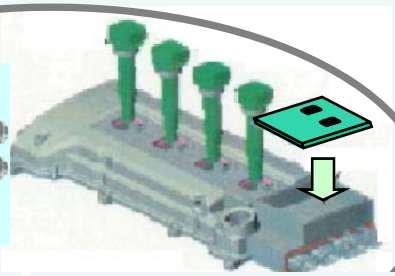
直載小型ＥＣＵ

✧モジュール直載ＥＣＵ

✧エンコパ搭載

E-BOX収納ﾀｲﾌﾟ

ﾊﾞﾙﾌﾞﾓｼﾞｭｰﾙ内蔵



ﾓｼﾞｭｰﾙ一体ＥＣＵ

車両電子部品の技術動向（２）

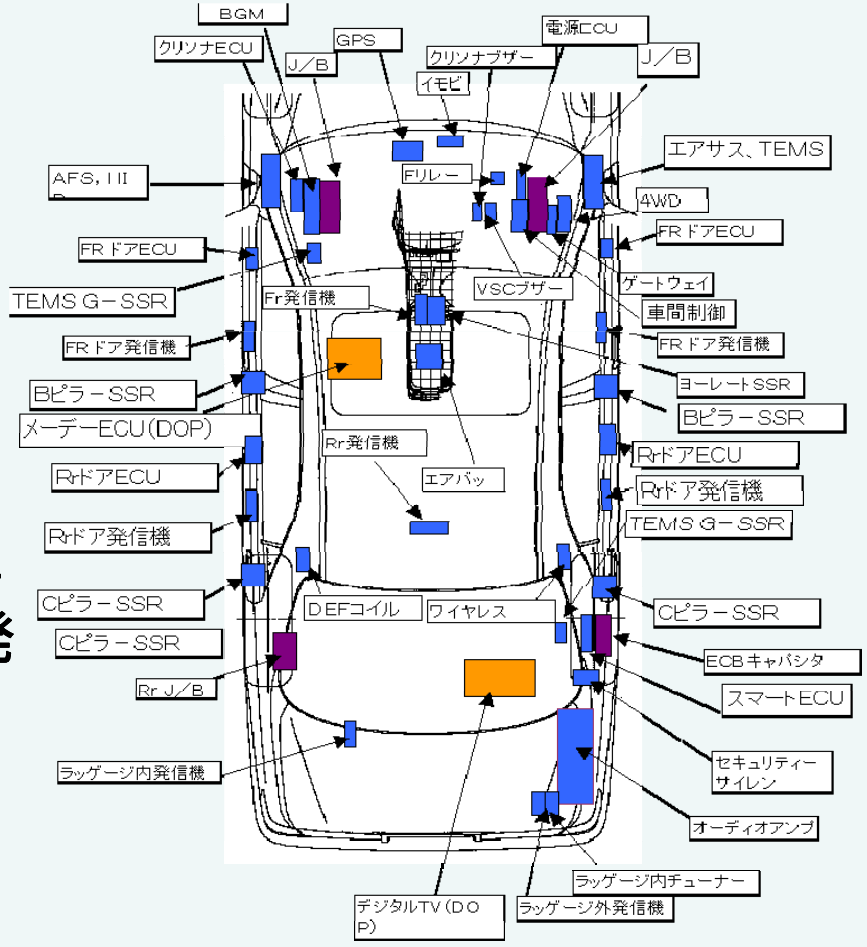
車両電子ｼｽﾃﾑの増大に伴い、ＥＣＵ搭載ｽﾍﾟｰｽが厳しくなっており、
次世代車両成立に向け、ＥＣＵの小型化・標準化が必須な状況

クラウン クラス

ＥＣＵ計６０個以上

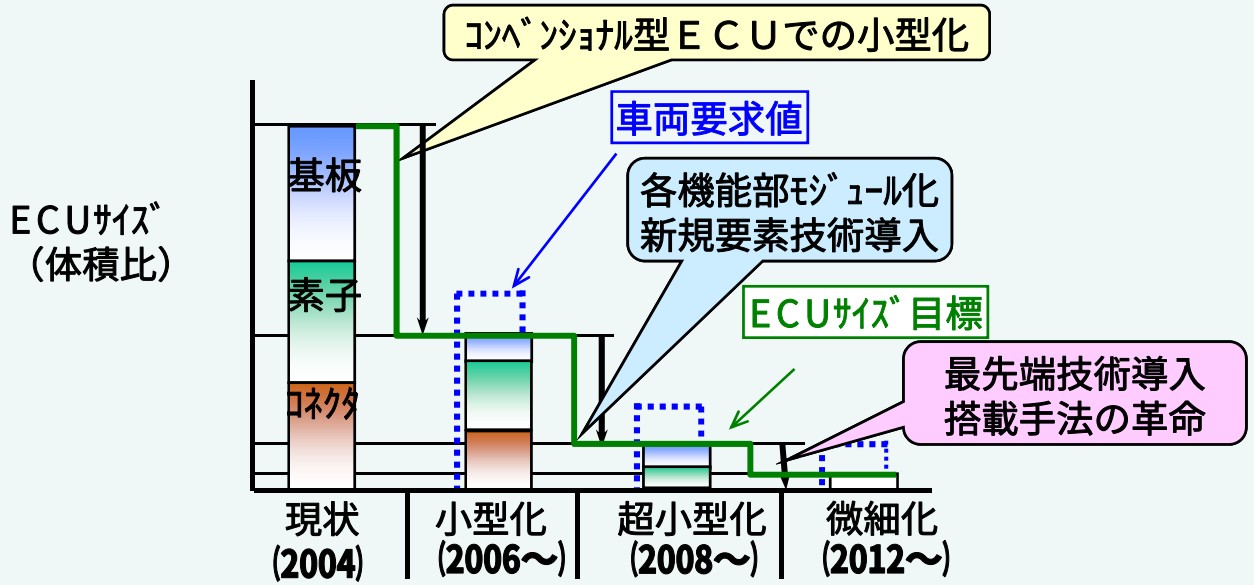
(‘０６年車種では、７０～８０個)

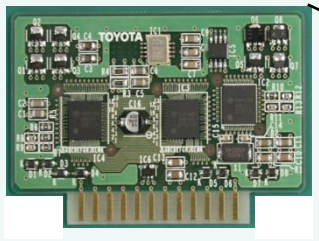
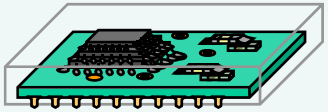
- 単独配置検討は限界
- 統一した設計思想による効率化
  ⇒設計・素子の標準化
- ＥＣＵｻｲｽﾞの小型・標準化が必要
  ⇒小型ICﾊﾟｯｹｰｼﾞ・実装技術開発
- 民生を超えた先端技術が必要



車両電子部品の技術動向（３）

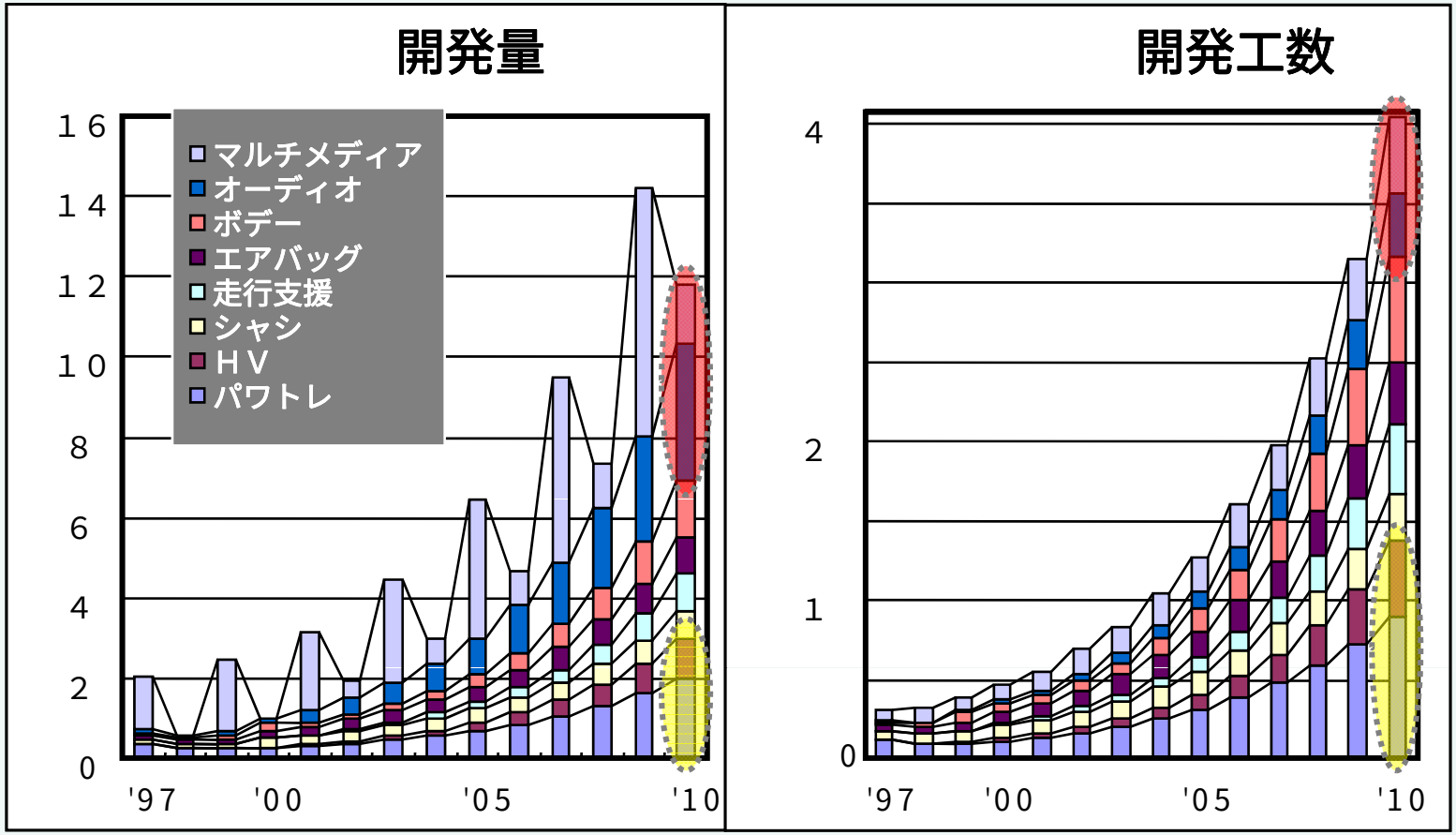
ＥＣＵ小型化が待ったなしの状況：高集積化/高密度実装



2008　超小型化	2010　～微細化
 ベアチップ実装 超高密度実装 体積１/Ｎ (面積１／Ｌ×高さ１／Ｈ) 耐熱１２５℃	SiP化  体積１/Ｍ (面積１／Ｋ×高さ１／Ｈ) 耐熱１２５℃
モジュール化	ワンチップＥＣＵ

車両電子部品の技術動向（４）

Increase of Software Development Volume



信頼性技術

Location	Max Temp.	Vibration Level	Fluid Exposure
On Engine On Transmission	>140℃	30G	Harsh
At the Engine (Intake Manifold)	125℃	20 - 30G	Harsh
Under hood Near Engine	120℃	10G	Harsh
Under hood Remote Location	110℃	10G	Harsh
E-Box	105℃	3 - 5G	Benign
Passenger Compartment	85℃	3 - 5G	Benign

車両電子部品技術動向まとめ

１）自動車電子部品

- 自動車に使われる半導体はパソコンの１０台分
- ＥＣＵ　６０～７０個/台　@高級車クラス
- 電子部品の伸びはメカ部品の伸び率の３倍
- 電子部品コスト比率は約５０％　@ＨＶ車

２）自動車電子化トレンド

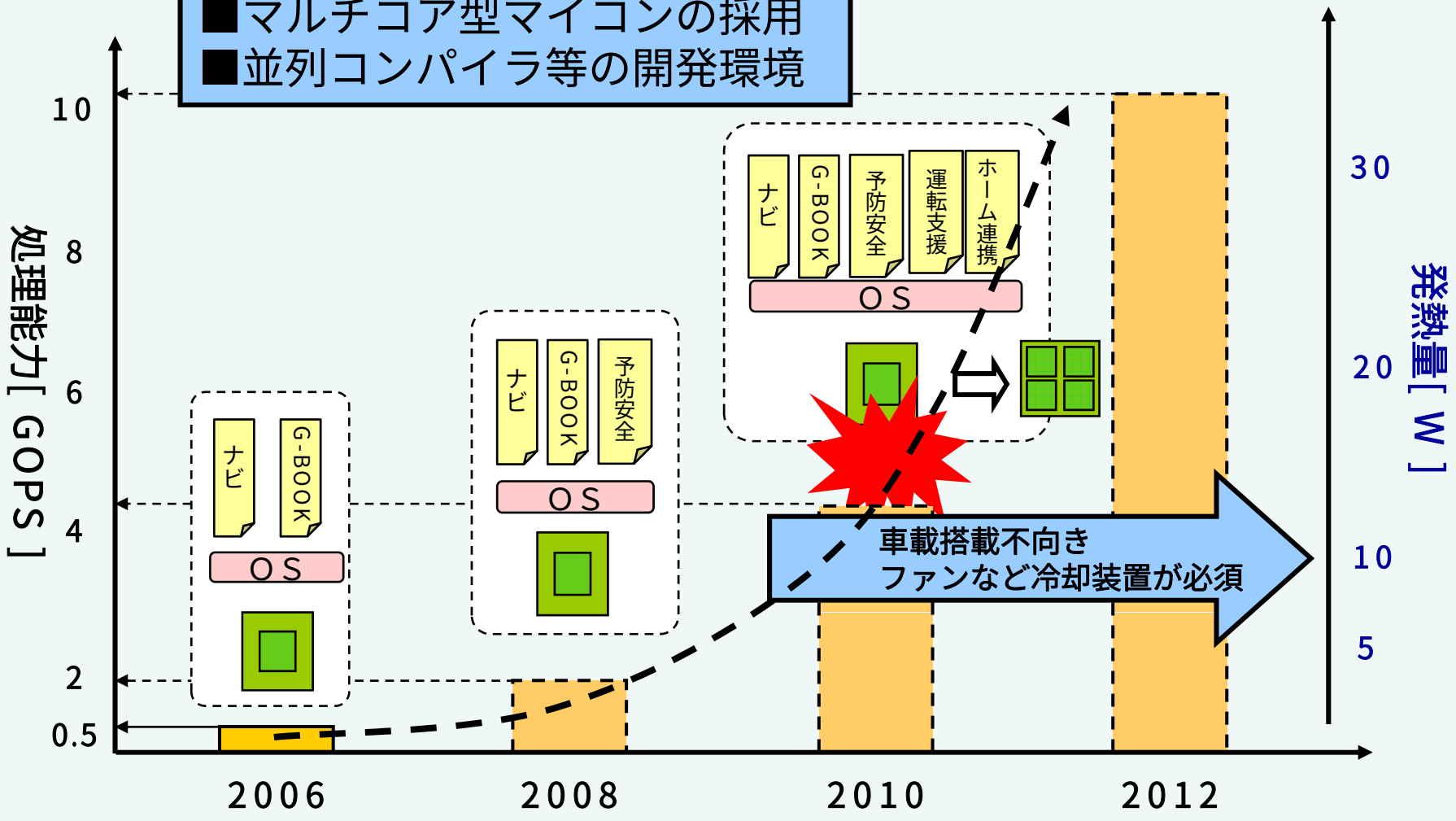
- 「快適」「情報通信」「安全の更なる向上のため統合化が進む
- センサーの数も増加し、ＭＥＭＳ等の開発が促進される
- 電子部品の品質、コストで車の性能が決定

⇒ **生体系構造が電子システムの目指す姿**
（機能毎に独立した電気・電子的構造）

- 電子部品の小型、高温、高密度化
- 従来技術を超えた発想の部品開発（ソフト/ハード最適）
- 部品同士を繋ぐコネクト技術が重要

新技術の導入

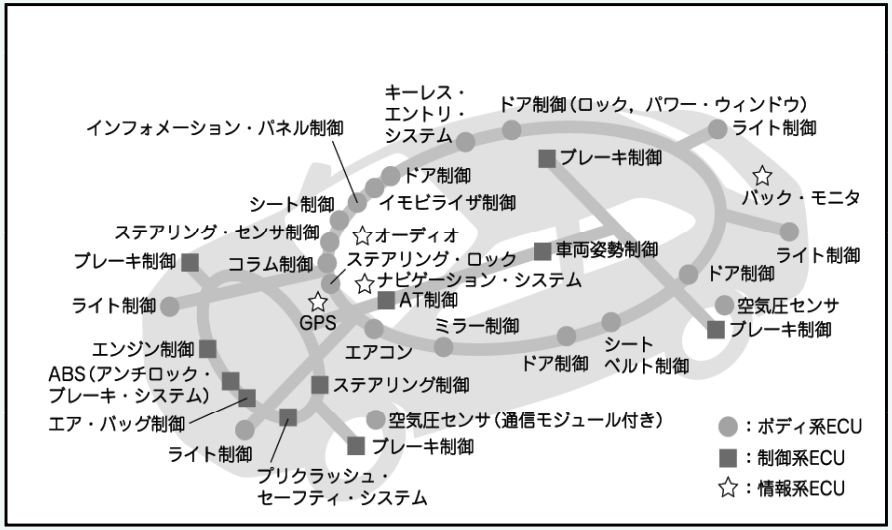
新たな技術導入が必須
■マルチコア型マイコンの採用
■並列コンパイラ等の開発環境



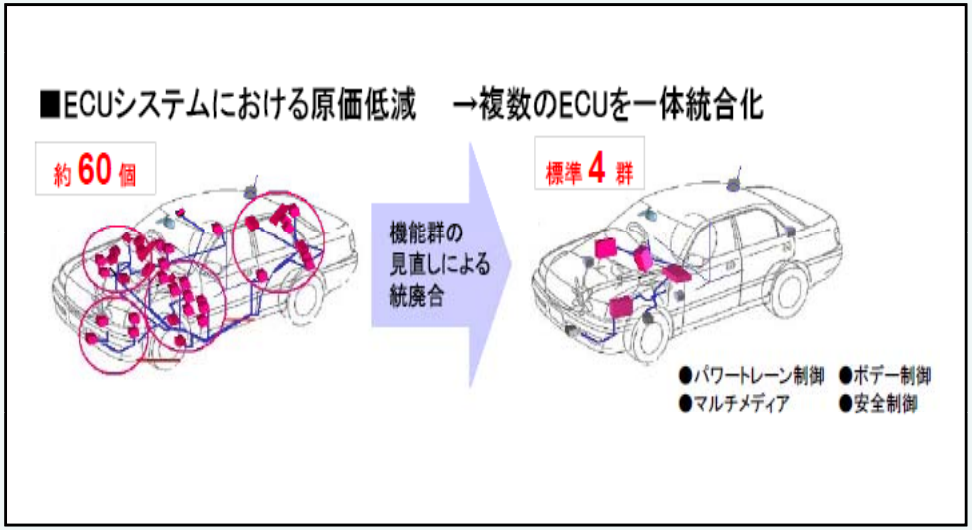
車載部品のディペンダビリティ

車載エレクトロニクス部品の統合化の進展により、システムレベルのディペンダビリティが部品に必要

車両に搭載されているECU



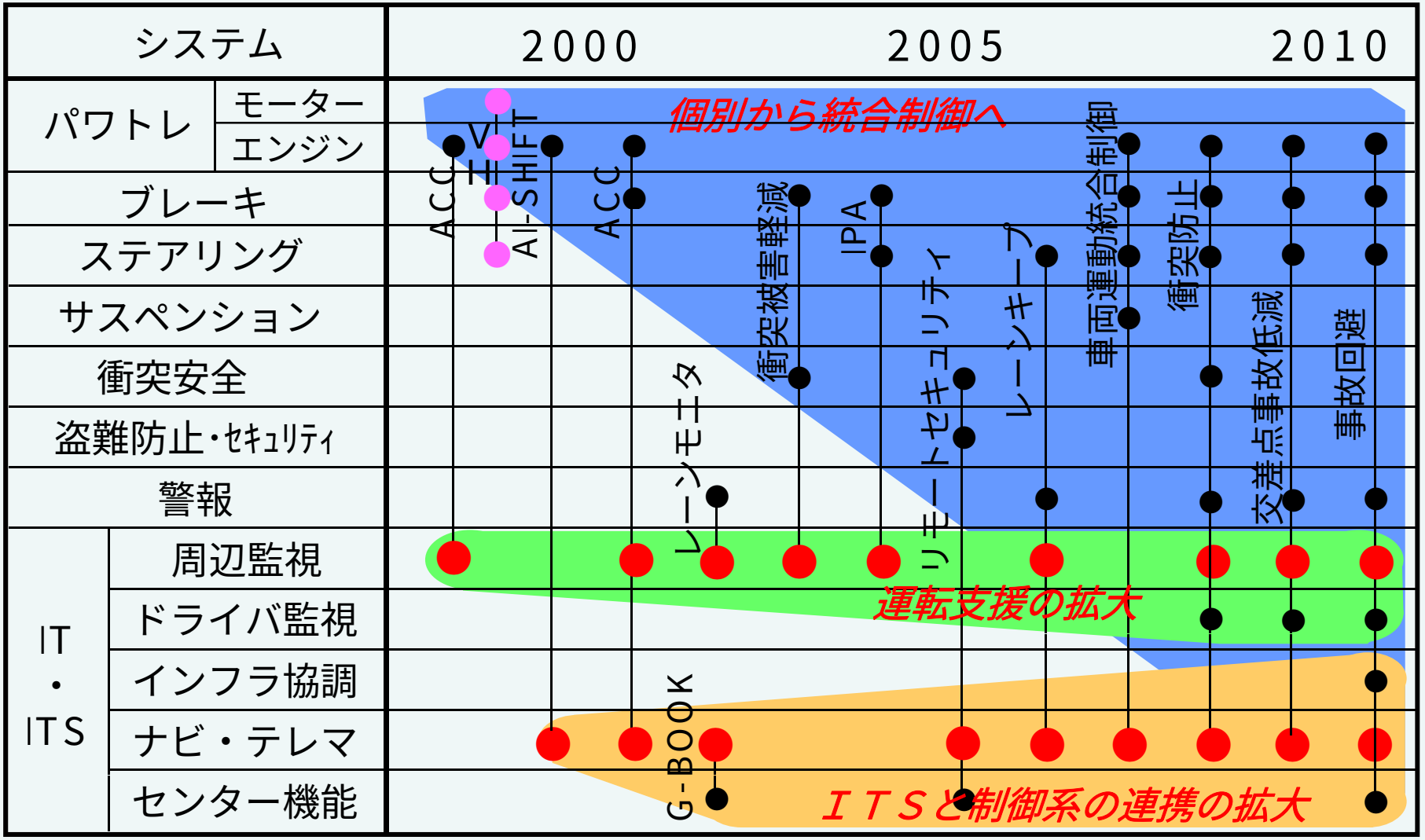
車載ECUの統合化



http://www.kumikomi.net/article/explanation/2005/03osek/01.htmlより引用

車載部品のディペンダビリティ

個別制御から統合制御への流れが加速



自動車の機能安全

IEC61508
(Functional safety of electrical/electronic/ programmable electronic safety – related systems

IEC61508 – 1: General requirement
– 2: System requirement
– 3: Software requirement
– 4: Definition
– 5: Example for SIL Determination
– 6: Guideline for Part 2,3
– 7: Techniques Examples

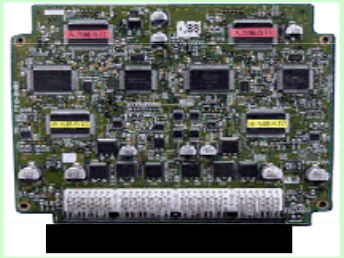
プロセス産業	：IEC61511	医療器械	：IEC62304
原子力	：IEC61513	鉄道	：IEC62278
産業機械	：IEC62061	航空機	：JAR/FAR 25 1309
電子制御モータ	：IEC61800	防衛	：Defense Standard 00-56
ロボット	：ISO10218	自動車	：ISO26262（'08末 ISO化）

自動車の機能安全

	IEC61508	ISO26262
対象領域	全産業	自動車
安全システム搭載	外付け監視可能	車載に限定
系統エラー	SILレベルに応じた 遵守プロセス差別化	差別化困難
SILレベル	SIL 1-4	ASIL A-D
使用実績	認証時に加味	証明で説明回避
SILレベル 目標故障率	最少10^{-9}回/Hr	数値目標議論中

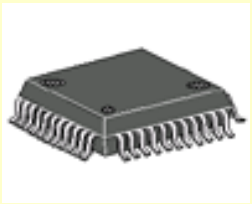
自動車の機能安全

従来



システムレベルで
半導体部品の検証
が容易

SOC化



1チップ化の進展により
システムレベルで半導体
部品の検証が不可能

1）自動車業界において、部品レベル（マイコン、統合IC）
レベルのテスト環境の仕様化が必要
2）半導体業界においては部品レベルでの検証能力の把握と、
新し い検証技術の開発を望まれる

機能安全規格　ISO26262 Road Vehicle – Functional Safety を制定中

半導体における機能安全

従来方式

- ｲﾘｰｶﾞﾙｱﾄﾞﾚｽ
- ｲﾘｰｶﾞﾙｲﾝｽﾄﾗｸｼｮﾝ
- ＥＣＣ
- ｳｵｯﾁﾄﾞｯｸﾞ
- 冗長周辺回路
- ｽｰﾊﾟｰﾕｰｻﾞｰﾓｰﾄﾞ
- ｸﾛｯｸ/電圧監視
- ｻﾌﾞﾏｲｺﾝ監視
- ﾌｪｲﾙｾｰﾌ監視ﾓｰﾄﾞ

最近の取り組み

- ＣＰＵｾﾙﾌﾁｪｯｸ
- ﾋﾞﾙﾄｲﾝｾﾙﾌﾃｽﾄ
- ｵﾝﾗｲﾝ周辺回路ﾁｪｯｸ

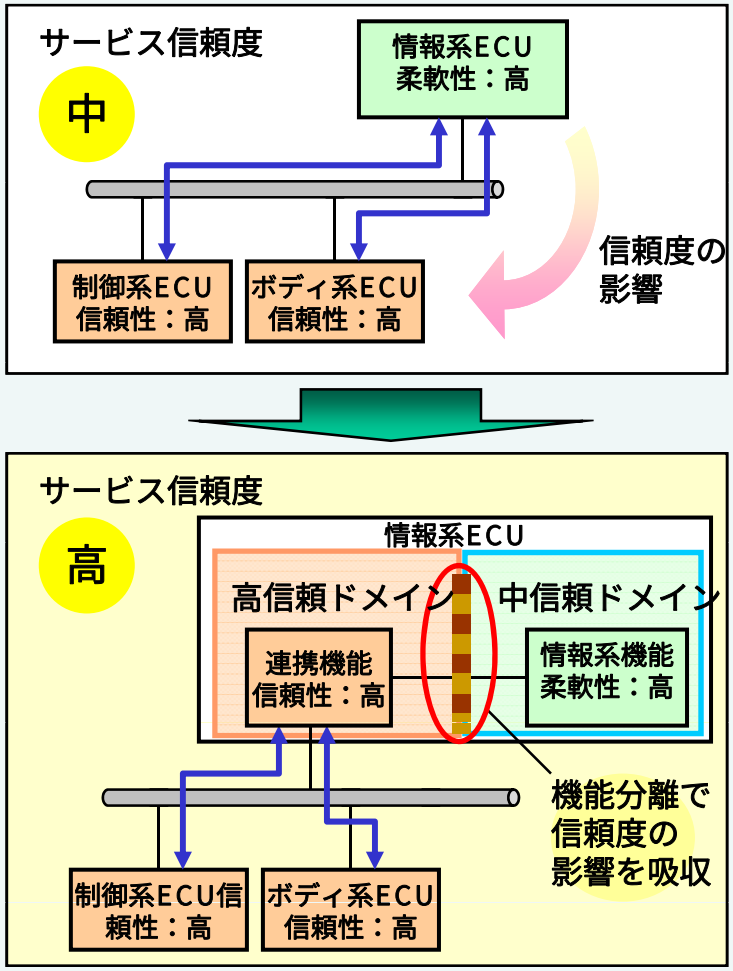
将来技術

- ﾏﾙﾁｺｱ相互監視
- ﾄﾗｽﾄｿﾞｰﾝ
- ﾌｫﾙﾄ ﾄﾚﾗﾝﾄ ﾃﾞﾊﾞｲｽ

～2005年 ⇒ 2006 - 2010年 ⇒ 2010年～

ディペンダビリティの考え方（例）

各ドメインの必要信頼度を定義し、システム構造に織り込む



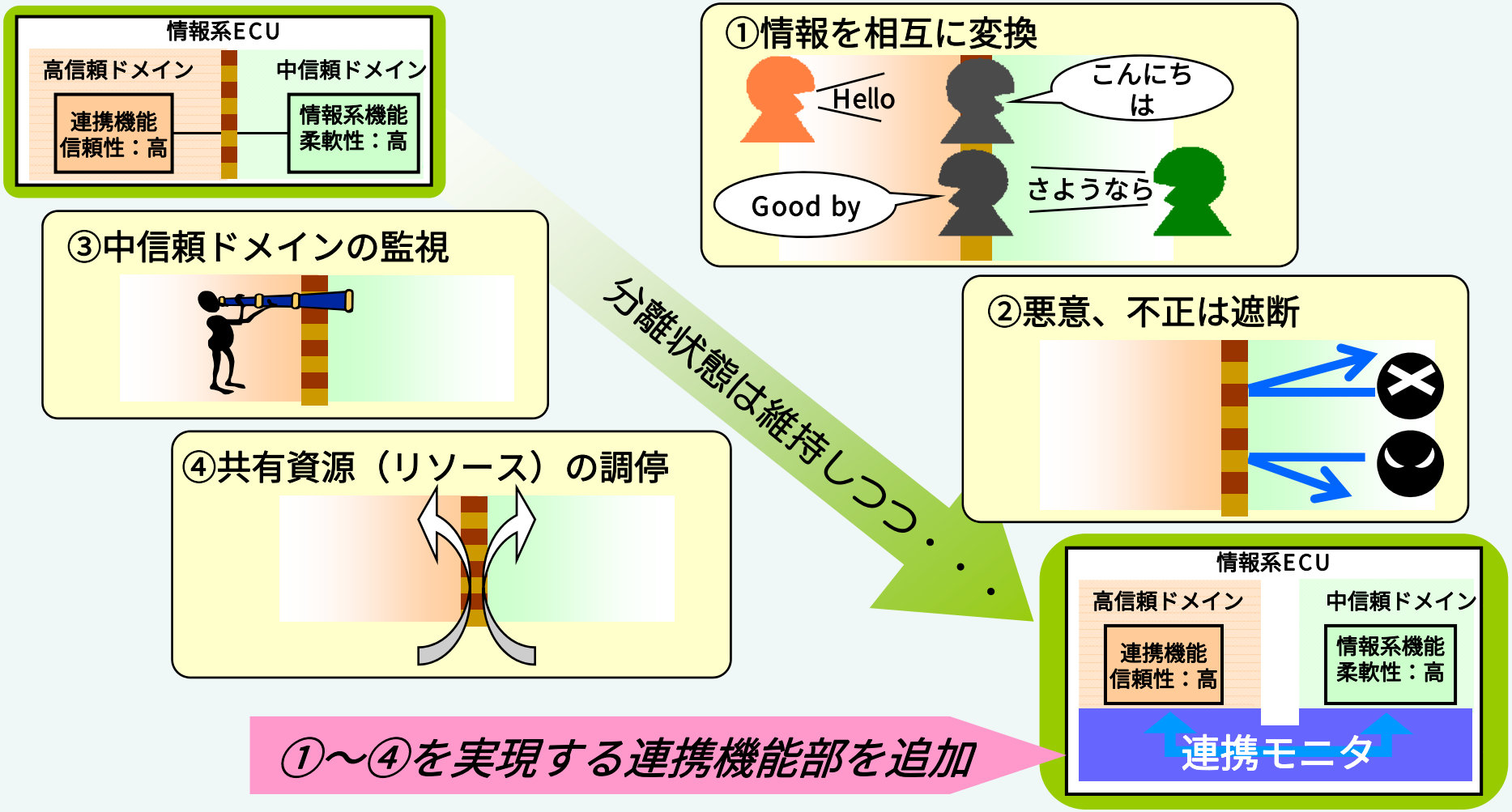
信頼度の異なるシステム間接続は、全体の信頼度は低い側となる

⇨ このままでは高信頼なシステムを構築できない

情報系ECUの内部に制御系・ボディ系ECUと同等の高信頼な連携機能と中信頼な領域（ドメイン）に分離

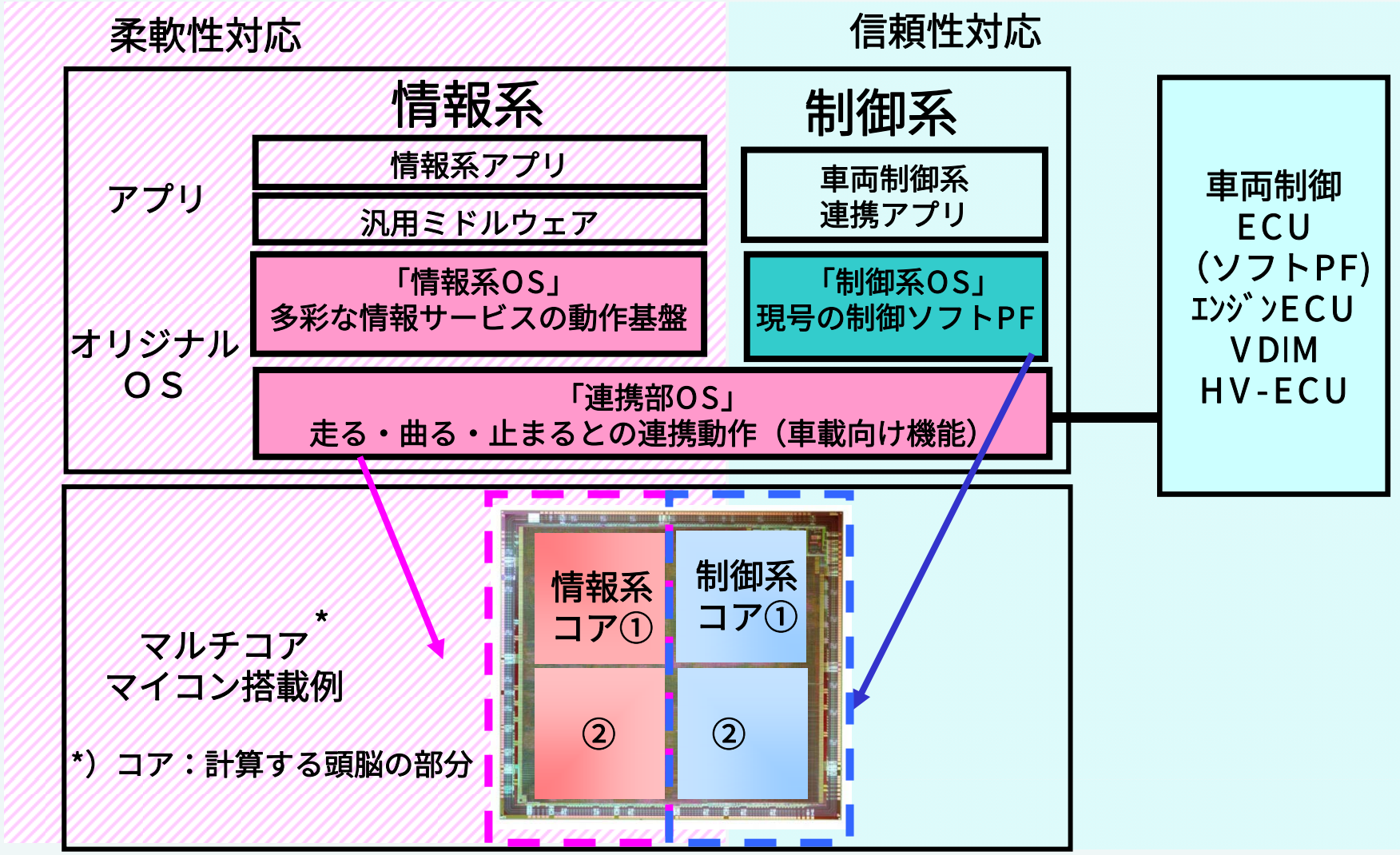
⇨ 制御系・ボデー系との接続は高信頼ドメインに限定することで、信頼性を確保

マルチコアマイコン、デュアルOSを用いて２つのドメインを安全に接続し、必要な監視・調停の実現

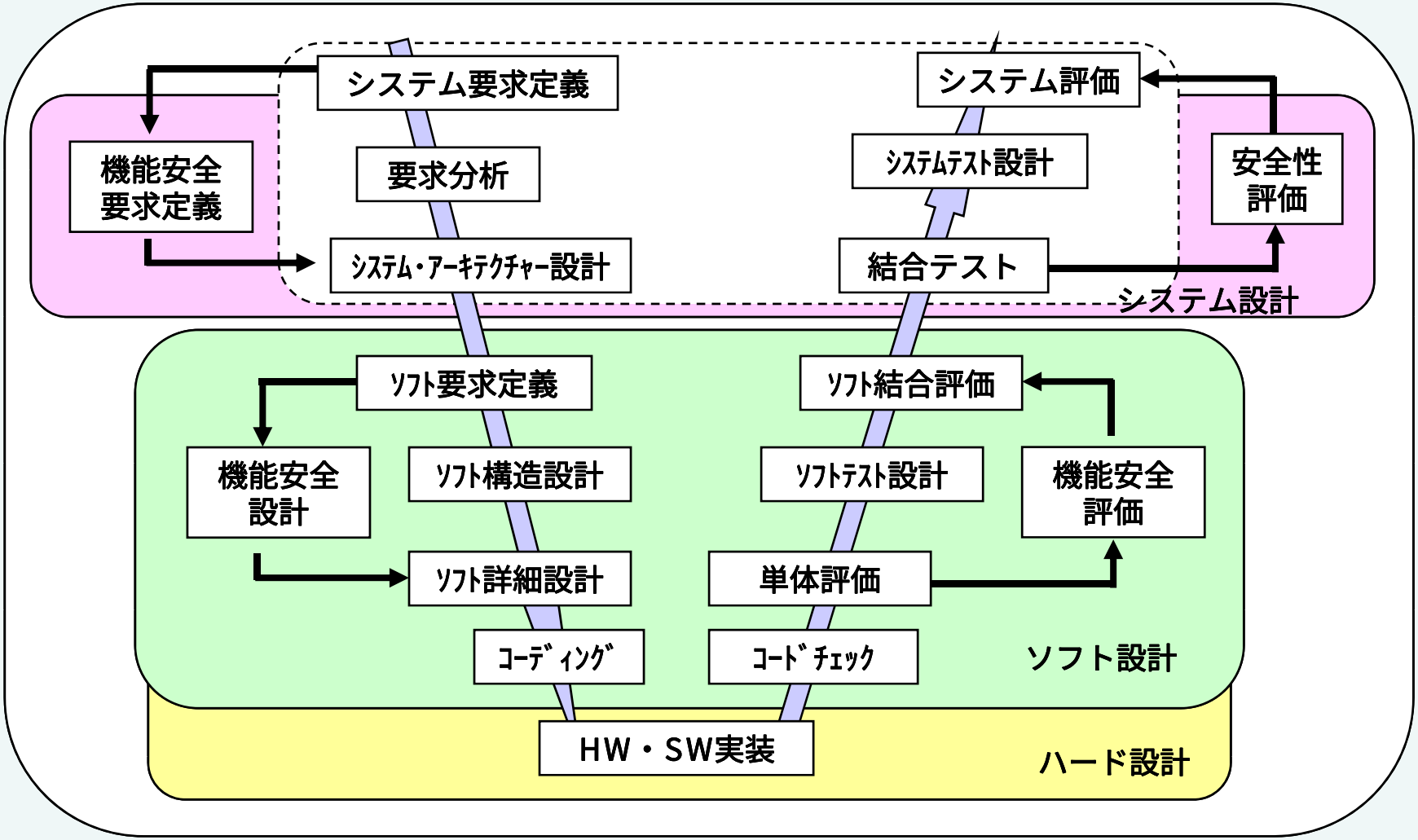


マルチコア技術

情報系柔軟性と車両制御信頼性の２律背反を確保



電子システム開発モデル



1）機能安全の法規化に伴いアーキ設計がより重要に
2）安全性向上にはハード設計と密接なソフト設計が必須

ソフト構造化アーキテクチャー

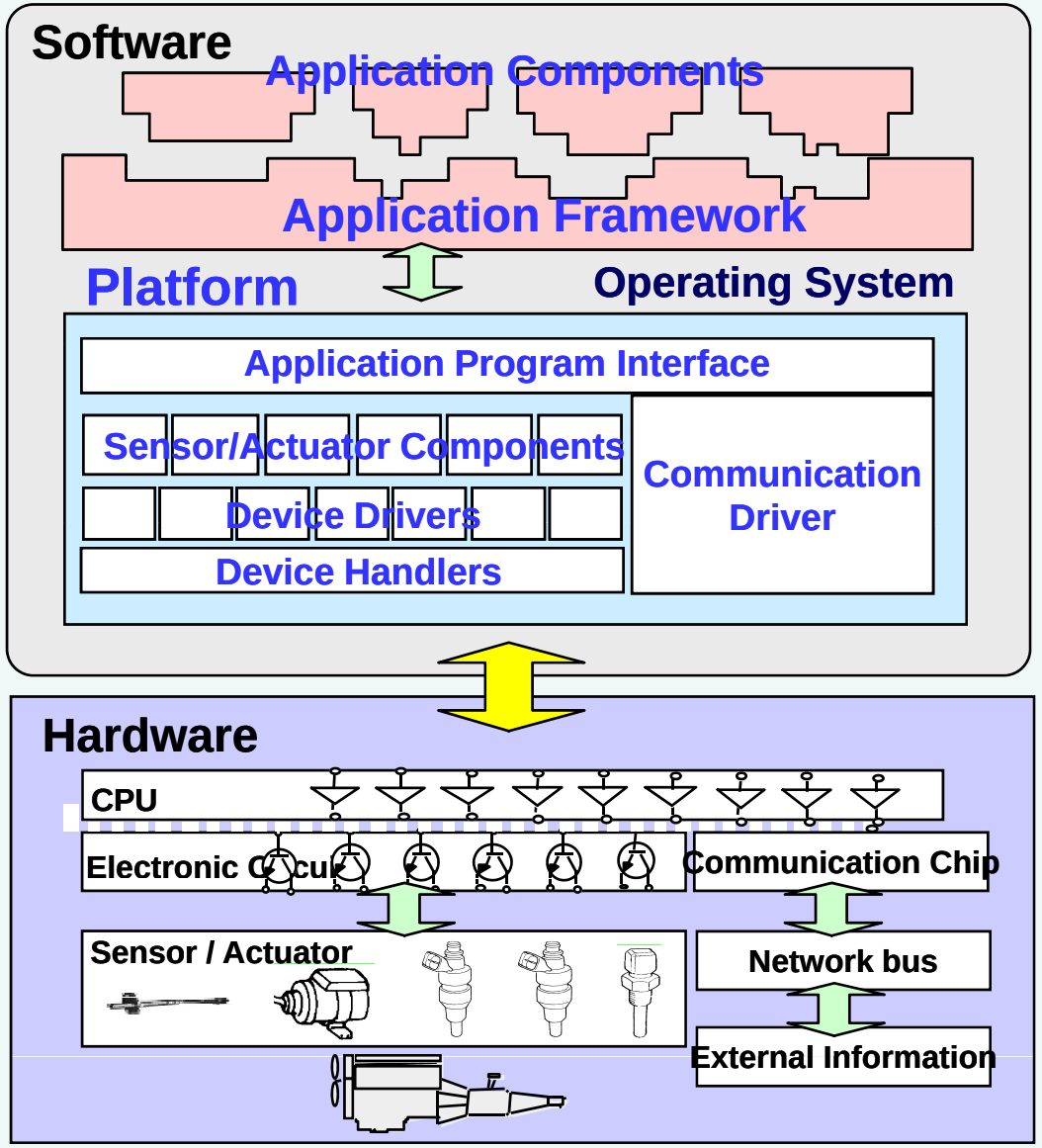
従来:ソフトが機能単位

大規模化

仕様変更が
ソフト全体に波及

再利用単位での
階層化・部品化

モジュール化技術の
適用



まとめ

１．自動車用電子制御システム開発の動向

◆電子ｼｽﾃﾑ肥大化、個別→ｼｽﾃﾑ統合で複雑化

◆車両機種展開を「電子ＰＦ」ﾍﾞｰｽでの開発手法に転換

２．自動車用ソフトウェア開発の動向

◆個別ｼｽﾃﾑｿﾌﾄ開発は効率化・信頼性向上で一服感

◆ｼｽﾃﾑの統合化でｿﾌﾄ開発量は急増、抜本的改革が必要

◆ＯＥＭ各社の危機感一致、非競争領域の技術は国際協調に移行

３．自動車の性能はエレクトロニクスが決める様になる

◆ディペンダビリティの良し悪しが自動車の品質/安全性を決定

◆エレクトロニクス化が進むとシステムの脆弱性も高まる

４．システムから部品開発までスルーで実現出来る設計環境がディペンダビリティには必要

◆最適なハード/ソフトの機能分担、設計ツールのチェーン化

◆高精度/高速動作モデル：メカとエレキの境界検討

◆部品レベルの完璧なディペンダビリティ実現をシステム側は期待