複雑化する車載制御ソフトウェア開発を支える最新電子プラットフォーム技術

Advanced Electronic Platform Technologies Supporting Development of Complicated Vehicle Control Software

深野 善信 Fukano Yoshinobu
後藤 広生 Goto Kosei
松原 正裕 Matsubara Masahiro
勝 康夫 Sugure Yasuo
宮崎 義弘 Miyazaki Yoshihiro

車載制御ソフトウェアは，電動化や予防安全など自動車の高機能化により，プログラムの大規模化・複雑化が進んでいる。さらに，2011年に発行された自動車の機能安全国際規格（ISO26262）に基づいて，安全性・信頼性の高いソフトウェアを高効率に開発する技術が求められている。これらの課題に対して日立グループは，機能安全対応基盤ソフトウェア技術および高度ソフトウェア検証技術の開発に取り組んできた。

1. はじめに

自動車への組み込みシステムの搭載は，排出ガス規制や交通安全対策などの社会的な要請に応える形で，1970年代から始まった。現在は，自動車の基本機能である「走る」，「曲がる」，「止まる」という動作の統合的な制御を実現するため，エンジン，パワートレイン系，シャシー系などのさまざまな部品に車載制御ソフトウェアが実装されている。車載制御ソフトウェアに要求される機能は，年々，高度化する一方で，車載制御ソフトウェアの大規模化と複雑化は，今もなお進展している[1)]。

ここでは，このような大規模かつ複雑な車載制御ソフトウェアの開発に対応するための最新技術について述べる。

2. 車載制御ソフトウェア開発の動向

自動車に搭載されているソフトウェアの規模は，2005年の時点で，コード行数が約200万行に達している。最近では，ハイブリッド自動車や電気自動車に見られる電動化への対応などの要因により，車載制御ソフトウェアの開発規模と複雑度は増加の一途をたどっており，2015年には，コード行数が1億行に到達すると予想されている。

次世代車両に実装される車載制御ソフトウェアは，エンジンやパワートレインの制御，ブレーキ，パワーステアリング，サスペンションなどのシャシー制御に加えて，予防安全制御やエネルギーマネジメント制御が加わり，制御・組み込みソフトウェア開発力の強化が必要になっている[2)]（図1参照）。

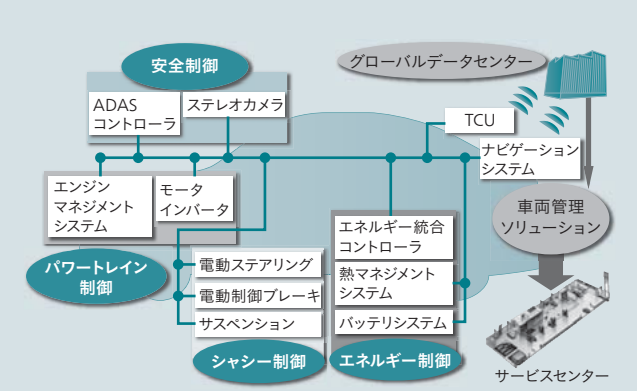


図1｜次世代車両における車載制御ソフトウェアの全体構成
エンジン，パワートレイン，シャシー系に加えて，予防安全，エネルギー制御，外部ネットワークとの連携などを統合的に管理する必要がある。

車載制御ソフトウェアの大規模化と機能の高度化が進む一方で，ソフトウェアの品質を維持しつつ，開発期間の短縮が求められている。さらに，自動車用機能安全規格（ISO26262）の要求に対応した安全設計・検証を実施する必要がある。日立グループは，これらの要求に対応する基盤ソフトウェア技術，高度検証技術（形式検証と仮想マイコン応用シミュレーション）を開発してきた。これらの技術について次に述べる。

3. 機能安全対応基盤ソフトウェア技術

日立オートモティブシステムズは，車載用組み込みソフトウェア開発における開発期間の大幅短縮，低コスト化，および高信頼化のために，ソフトウェアの標準プラットフォーム化に取り組んでいる。機能安全規格や業界標準化

［AUTOSAR（Automotive Open System Architecture）など］に対応した日立の標準基盤ソフトウェア（**図2**参照）は，主にエンジンやインバータなどのパワートレイン系と，ブレーキなどのシャシー系のマイコンに対応している。

この標準基盤ソフトウェアは，業界標準のAUTOSAR仕様（ICC1）に基づいた構成となっており，顧客や日立の各製品設計部門が開発するアプリケーション層のソフトウェアは，RTE（Runtime Environment）を介して基盤ソフトウェアと接続される。したがって，アプリケーション層のソフトウェアは，RTEのインタフェース仕様に従うことで，マイコンや，制御ユニットの回路構成など，ハードウェアの相違による影響を最小限に抑えることが可能となる。

また，基盤ソフトウェア自体も階層構造にすることにより，マイコンやハードウェアの相違を，下層部のMCAL（Microcontroller Abstraction Layer）で吸収し，汎用性を持たせる仕組みになっている。

基盤ソフトウェアの機能安全規格への対応については，どの安全度レベルの製品にも適用できるように，ISO26262で要求されるASIL（Automotive Safety Integration Level）-Dの開発プロセスを実施している。

機能安全規格の対応で，重要な技術となるのが，無干渉（Freedom From Interference）機能（以下，FFI機能と記す。）の実現である。FFI機能とは，異なる安全度レベル（以下，ASILと記す。）のソフトウェアが1つのマイコンに混在する場合，低いASIL領域から高いASIL領域への従属故障を防ぐための機能である。

日立グループが開発する基盤ソフトウェアは最もレベルの高いASIL-Dであるが，自動車に組み込まれるアプリケーションソフトウェアには，ASIL-AやB，もしくは機能安全対象外のQM（Quality Management）などさまざまなケースがある。

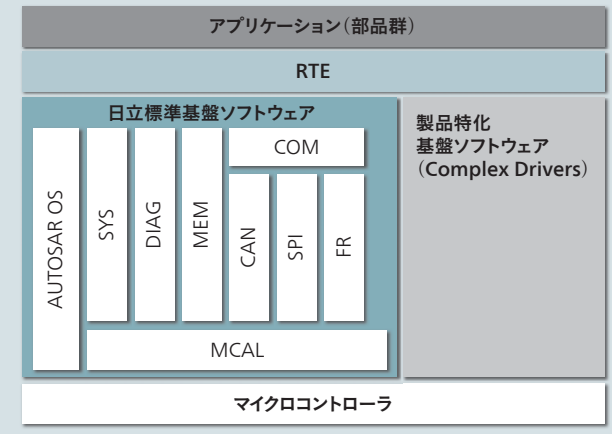
そこで，基盤ソフトウェアとして，以下の保護機能を実現させて，ASIL-D以外の領域からの従属故障を防ぐ仕組みを構築している。

（1）時間保護

主にAUTOSAR OS（Operating System）の機能を使って，タスクや割込みのタイミングを監視する。さらに，保護機能を強化するため，日立グループで開発した機能を追加搭載することとした。

（2）メモリ保護（メモリパーティショニング）

AUTOSAR OSと，マイコンのメモリ保護機能を使って，ASIL-D領域のメモリを保護する。ASIL-D領域とそれ以外の領域の間でのプログラム動作モードを切り替える際（コンテキストスイッチ）のオーバーヘッドを最小限に抑えた，高速メモリパーティショニング技術を開発した。



注：略語説明　RTE（Run Time Environment），
AUTOSAR（Automotive Open System Architecture），
OS（Operating System），MCAL（Microcontroller Abstraction Layer），
CAN（Control Area Network），SYS（System），DIAG（Diagnosis），
MEM（Memory），COM（Communication），SPI（Serial Peripheral Interface），
FR（FlexRay）

図2｜日立標準基盤ソフトウェアの概略構成
RTEを境界として，上部が製品仕様のアプリケーション層，下部が基盤ソフトウェア層（標準ソフトウェアプラットフォーム）である。

4. 形式検証

機能安全国際規格ISO26262では，特に安全性が求められるASIL-C/Dのシステムに対して形式検証の適用が推奨されている。日立グループは，形式検証の1つであるモデル検査を製品に適用し，大規模化・複雑化を続ける車載ソフトウェアの信頼性維持･向上を図っている。この動機は，入力に対する出力を期待値と比較する従来のテスト手法に加えて，ソースコード上のすべてのテストパスを網羅的に検証することにより，ソフトウェアの不具合の発生をゼロに近づけることにある。

形式検証は，要求仕様とこれに基づく設計とを厳密に意味づけられた言語を用いて記述するものであり，両者の一致性を数学的理論によって厳密に検査することができる。さらにモデル検査では，この検査が自動化される。モデル検査の仕組みは，ソフトウェアの設計に関するモデルから，ソフトウェアの動作時に取りうる状態を，計算機が網羅的に調べ上げることで，仕様にない動作，つまり，設計時には予期されていない動作の発生の有無が判定される。しかし，ソフトウェアの状態数が膨大になると，計算機のリソースが不足して検査しきれないという課題があった。計算機性能の進展があったものの，モデル検査の適用対象は限定され，量産製品規模のソフトウェアを扱うのは長年困難であった。

日立グループは形式検証（モデル検査）を実用化するため，ソースコードに現れる変数間の関連性（依存関係）を解析し，検査項目の変数に関連するコードだけを抽出して

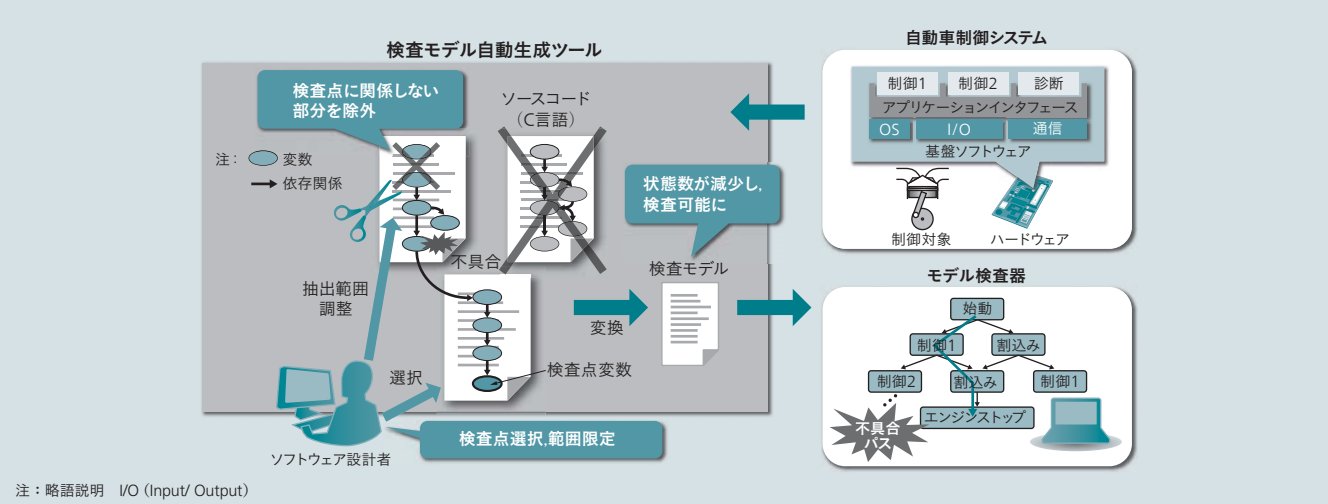


図3｜ソースコードからの検査モデル自動生成技術

検査点変数は，不具合の影響が出現しうる変数である。この変数に対する他変数のつながり（依存関係）が自動的に解析され，関連するコードが高精度に抽出される。さらにソフトウェア設計者は，設計知識を用いてモデル化するソースコードの範囲を限定できる。これにより検証可能なモデルを得る。

から検査モデルに変換することで，検査モデルの状態数を大幅に削減する技術を開発した（**図3**参照）。これにより，ソフトウェア規模が数十万行に達するものでも，電子制御ユニットのソフトウェア全体をモデル検査の対象とすることに成功した[3]。検査対象の規模は，これまでに論文などで報告されているデータと比較して約10倍である。検査対象を拡大できた理由は，高精度かつ高速（汎用PCを用いて約10万行に対し数分以内）な解析手法，およびソフトウェア開発者が設計知識を活用して検査点の選定や抽出範囲の調整を行える仕組みを用意した点にある。変数の関連性はグラフ化され，ソフトウェア開発者はモデル化する範囲の調整を視覚的に実施することができる。

また，この技術を用いて，ソフトウェアのソースコードから検査モデルを自動生成する検査支援ツールを製作し，検証作業を効率化した[4]。これによりASIL-C/Dの製品開発に対して形式手法（モデル検査）を適用する環境を整え，順次適用を進めている。

5. 仮想マイコン応用シミュレーション技術

ここでは，仮想マイコン応用シミュレーション技術による自動車制御ソフトウェアの実機レス検証環境に関して述べる。

従来，量産コードレベルでの制御ソフトウェアの検証手法として，実機ハードウェアでのマイコンと，制御対象の挙動を模擬するシミュレータを接続したHILS（Hardware in the Loop Simulation）が用いられてきた。しかし，実機ハードウェアを使用するため，運用上の制約があった。そこで，日立グループは，仮想マイコンと制御対象モデルとの協調シミュレーションによる，制御ソフトウェアの実機レス検証環境vHILS（virtual HILS）を開発した[5), 6), 7)]。

vHILSにより，量産コードレベルでの制御ソフトの検証が実行可能となる。その主な効果として，(1) マイコンを含む実機がない時期や場所でもソフトウェア検証が可能となる点，(2) 検証環境の一時的な複製が容易となり，大量の検証項目を同時に並列実行することで，検証を短期化できる点の2つがある。

vHILSを，車間距離制御（ACC：Adaptive Cruise Control）システムに適用した（**図4**参照）。ACCシステムは，外界認識センサーによって先行車との距離と相対速度を計測し，エンジン，ブレーキなどを制御して，先行車に追従する機能を有する。自動車エンジン，ブレーキなどの各ECU（Electronic Control Unit）およびその制御対象に関しては，HILSで使用していたMATLAB※)/Simulink※)モデルを流用した。一方，ACC ECUに搭載されているメインマイコン，サブマイコン，メモリと，ACC ECUと他ECUを接続するCAN（Control Area Network）通信については，新たにモデル化をした。特にCAN通信の模擬に関しては，制御ソフトウェアの動作検証に最小限必要なメッセージレベルの通信を模擬することで，精度を保ちつつシミュレーション実行の高速化を可能にした。

vHILS上で，従来のHILSによる検証時と同じテストケースを実行させ，シミュレーションの精度，実行速度を評価した。その結果，**図4**に示すとおり，自動車エンジン回転数の値や変化タイミングなどの論理的動作が一致していることを確認した。従来のHILSと比較して，同等の精度でありながら，シミュレーション実行速度は34％であった。これにより，複数検証項目を並列実行させることで，3台のノードで実機と同等であることを確認した。さらに，

※）MATLAB，Simulinkは，米国The MathWorks, Inc.の登録商標である。

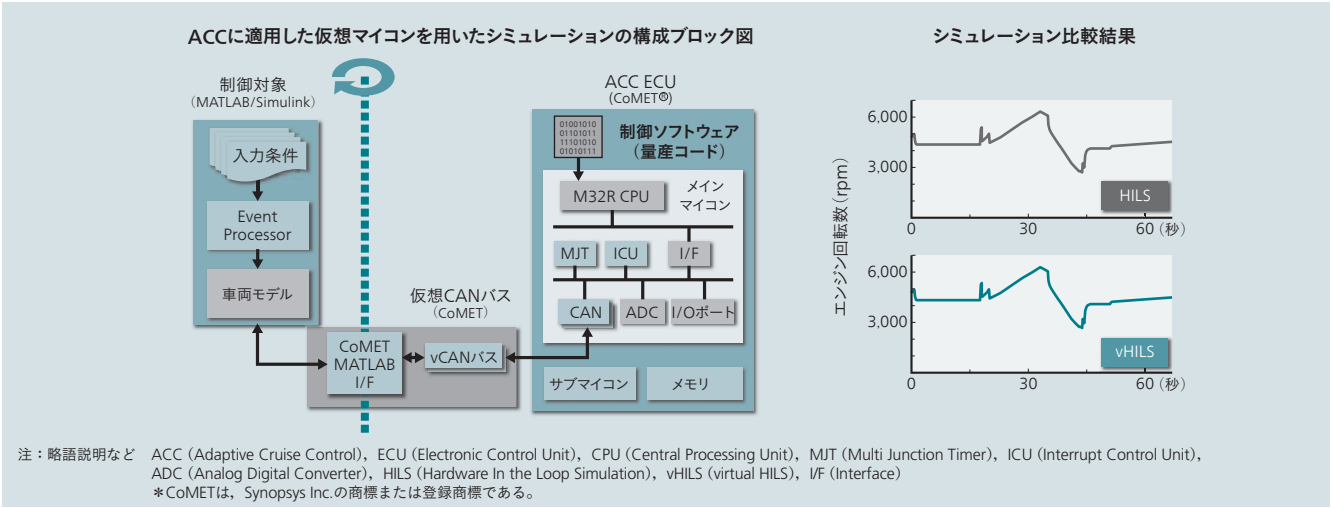


図4｜仮想マイコンを用いたシミュレーションのACCシステムへの適用
制御対象のMATLAB/Simulinkモデルとマイコンを含むECUとCAN通信のCoMETモデルとの協調シミュレーションを行うことで，実機を用いることなく，量産コードレベルでの制御ソフトウェアの検証が可能である。

計算ノードを増やすことで，HILS以上の検証処理性能を達成することを確認した。また，クラウド上でソフトウェア検証を自動実行する仕組みを構築し，出荷前確認テストの作業時間を，従来のHILSに比べて、$\frac{1}{20}$〜$\frac{1}{400}$に短縮できる実証結果を得た[7)]。

上述したvHILS技術を普及させるために，vHILS技術に関わる業界（自動車メーカー，自動車部品メーカー，シミュレーションツールベンダー，半導体メーカー，研究機関）を縦断した協調活動として，仮想マイコン応用推進協議会/vECU-MBD（Virtual ECU Model-Based Development）ワーキンググループを推進している[8)]。

6. おわりに

ここでは，次世代車載制御ソフトウェア開発に対応した，基盤ソフト開発技術および高度検証技術について述べた。

日立オートモティブシステムズでは，日立グループ内の研究部門との連携により，これらの技術以外にも，車載制御ソフトウェア開発の基盤技術を開発中である。今後，ここに述べた技術の統合により，高度な次世代車載制御ソフトウェア開発プロセスが構築できる。

参考文献など

1) 川名：車載ソフト開発の現状（特集 組み込みソフトウェア開発技術），情報処理，45巻，7号，713〜715 (2004.7)
2) 車載ソフト開発で適用範囲拡大するシミュレーション技術，日経Automotive Technology (27)，68〜73 (2011.11)
3) 日立ニュースリリース，形式手法を用いた自動車制御ソフトウェアの高信頼検査技術を開発 (2013.4)，
http://www.hitachi.co.jp/New/cnews/month/2013/04/0416a.html
4) M. Matsubara, et al. : “Application of Model Checking to Automotive Control Software with Slicing Technique”, SAE 2013 World Congress (2013-01-0436), April 2013.
5) Y. Ito, et al. : VIRTUAL HILS : A Model-Based Control Software Validation Method, SAE 2011 World Congress (2011-01-1018), Int. J. Passeng. Cars - Electron. Electr. Syst. 4 (1) :142-149 (2011.4)
6) Y. Sugure, et al. :“Failure Mode and Effects Analysis Using Virtual Prototyping System with Microcontroller Model for Automotive Control System”, 7th IFAC Symposium on Advances in Automotive Control, September 2013.
7) 日立ニュースリリース，実機を用いずに鉄道や自動車の組み込みソフトを開発する完全仮想化シミュレーション技術を開発 (2010.10)，
http://www.hitachi.co.jp/New/cnews/month/2010/10/1028.html
8) vECU-MBDワーキンググループ，http://www.vecu-mbd.org/

執筆者紹介


深野 善信
1995年日立製作所入社，日立オートモティブシステムズ株式会社 技術開発本部システム開発技術部 所属
現在，モデルベース開発手法による車載制御ソフト開発の推進に従事
博士（理学）
ACM会員，自動車技術会会員


後藤 広生
1999年日立製作所入社，日立オートモティブシステムズ株式会社 技術開発本部 電子プラットフォーム開発部 所属
現在，標準基盤ソフトウェアの開発に従事


松原 正裕
2001年日立製作所入社，日立研究所 グリーンモビリティ研究部 所属
現在，車載制御ソフトウェアの検証技術開発に従事
情報処理学会会員


勝 康夫
1999年日立製作所入社，中央研究所 プラットフォームシステム研究部 所属
現在，自動車向け仮想マイコン応用モデルベース開発に従事
博士（工学）
SAE会員，電子情報通信学会会員


宮崎 義弘
1977年日立製作所入社，日立オートモティブシステムズ株式会社 技術開発本部 所属
現在，車載制御システムの電子プラットフォーム技術開発に従事
電気学会会員，情報処理学会会員，自動車技術会会員