

ソフトウェア品質管理研究会 特別講義 レポート

作成日: 2023年11月20日

書記氏名: 松波 知典

日時	2023年11月10日(金) 9:50 ~ 12:00
会場	(一財)日本科学技術連盟・東高円寺ビル 地下1階講堂 *ハイブリッド開催
テーマ	自動運転、高度運転支援時代の車載ソフトウェア開発と品質評価
講師名・所属	森崎 修司 氏 (名古屋大学 大学院情報学研究科 准教授)
司会者	岩井 慎一 氏 (株式会社デンソー)
アジェンダ	利用環境や利用範囲をより明確にした上での開発と品質評価 ・Operational Design Domain (ODD: 運行設計領域) ・シナリオベースのシミュレーションテスト より広範囲な要素技術 ・センサ ・アルゴリズム ・車外サービス 新しいタイプの欠陥 ・サイバーフィジカルギャップ ・セキュリティ ソフトウェア開発と品質評価で考慮すべきこと ・継続的开发 ・より精緻な品質評価とその説明 (十分性)
アブストラクト	より高度なセキュリティの実現、自動運転や高度運転支援への対応といった車載ソフトウェアへの要求に対応するため、センサ/カメラやそれらの組合せアルゴリズム、OTA(Over The Air: 無線通信によるソフトウェアの更新、変更)、車外サービス連携、ODD(Operational Design Domain: 運行設計領域)といった要素技術や基盤の整備が進んでいる。車載ソフトウェアの開発や品質保証もそれらに合わせて変えていかなければならない部分がある。本セッションでは、そうした車載ソフトウェアをとりまく新たな環境や要素技術を整理する。その上で、これからの開発や品質保証に求められる変化をソフトウェアエンジニアリングの観点から解説する。また、講演者らの研究グループで検討している研究テーマを紹介する。

第6回の特別講義では、「自動運転、高度運転支援時代の車載ソフトウェア開発と品質評価」と題して、森崎氏よりご講義をいただきました。

◆冒頭、森崎氏より自己紹介が有りました。

- ソフトウェアエンジニアとしてソフトウェア開発 (2001～)
通信事業者でオンラインストレージサービス開発
無線 IC タグの研究開発と国際標準化活動
- 研究者として実証的ソフトウェア工学の研究 (2005～)
58社と機密保持契約ベースの共同研究
ソフトウェア品質シンポジウム 2012～委員長 (現在)
IPA「つながる世界の品質指針検討ワーキンググループ」をはじめ、3ワーキンググループの主査

◆アウトライン

- 自動運転／高度運転支援の分類と大まかな仕組み
自動運転／運転支援の基礎知識
- 利用環境や利用範囲を想定した開発と品質評価の必要性
制約を設けた効果
- 新しいタイプの欠陥
- ソフトウェア開発プロセスと品質評価としてそのほかに考えるべき点
ソフトウェア視点でのこれまでの車載ソフトウェアとの違い
- 私の研究グループでの研究テーマ
説明責任、自動テストの実行効率向上

◆本講演で考えていただきたいこと

- スcopeが広いときに、適切に制約を設けることでスモールスタートできる
「使われ方の前提はこうする」「その前提で設計、評価する」
- 他のシステムでも適切に制約を設けることで開発、評価コストを小さくしたり、システムの品質を向上したりできる
「ユーザーはトレーニングを受けた特定のオペレーターとする」
- 要素技術やトレンドで何かができるような期間は短い
「生成 AI だから」「5G だから」でカバーできることには限界があり、システムの振る舞い等、本質的な理解が必要になる。

◆自動運転／高度運転支援の分類と大まかな仕組み

- 自動運転／高度運転支援のレベル
0～5 (米自動車技術者協会による)
0: 運転支援なし
1, 2: 運転支援 (主体と責任はドライバー)
3, 4, 5: 自動運転 (主体と責任は自動運転システム)
- 大まかな仕組み
センサで周辺環境をデータとしてとらえる
プログラムでデータを解釈する
解釈の結果にもとづいて、アクチュエータ (加減速、操舵) に指示を出す
経路のような長期の計画 (レベル 3, 4, 5 では経路の計画を立てる必要がある)
- 要素技術
センサ
アルゴリズム
車外サービスとの通信

- ・大まかな仕組み (レベル4)
高精度地図を使って、おおまかな進路を決める
センサ (LiDAR、カメラ等) で周辺の物体を認識して、回避、追従する
- ・地図上での自己位置推定とルート決定
高精度地図 (車線レベルの詳細が記載)
GPS、GNSS、センサからの情報等で地図と現在地を対応づけて、自車位置を確定して今後のルートを決める
- ◆利用環境や利用範囲を想定した開発と品質評価の必要性
 - ・シナリオを使ったシミュレーションテスト
シナリオにより実世界をシミュレーションし、シミュレーション結果を開発するプログラムに与える。
期待通り動作するか確かめる
 - ・PEGASUS の階層別の環境想定
シナリオを書いそうか、階層ごとに組み合わせをシミュレーションして、テストする
 - ・環境想定：シナリオを元にした品質保証
シナリオからテストを生成し、各種シミュレータで実行したり実車で確認したりする
 - ・ISO/PAS 21448 SOTIF (Safety Of The Intended Functionality)
自動車の安全性のための国際標準
シナリオを使った安全性分析
開発の進行とともに既知の安全シナリオを増やす
- ◆新しいタイプの欠陥
 - ・サイバーフィジカルギャップ
コンピュータ上の現実世界のモデルと現実世界の間には差ができる欠陥
現実世界のモデルはセンサや他の情報から作る
コンピュータ上に現実世界をモデル化する
 - ・複雑になるフィードバックループ
カルマンフィルタをはじめとして誤差やノイズに強いフィードバックループにおいて測定対象や制御対象が複雑になると想定しづらいレアケースが増える
多くのレアケースでは問題が起きないが、特定の条件下では安全を脅かすようなリスクとなる場合がある
 - ・セキュリティ
安全性の検討と似ているが、新しい手口が発見されたり、攻撃者の実行が契機となったりする。
次々と新しい手口が発見され、製品の脆弱性となる。
攻撃対象によっても攻撃者の実施の動機が変化し、リスクが変化する
- ◆ソフトウェア開発プロセスと品質評価としてそのほかに考えるべき点
 - ・継続的改善の必要性和可能性
継続的に開発、品質保証を続け、製品 (ソフトウェア) に問題が無い状態を維持する必要がある
→セキュリティアップデート
新たな脆弱性への対応と OTA (Over the air) による反映
→シナリオデータベース更新への追従
問題が有る場合には、シナリオへのプログラム/システムの対策
→シミュレーションテストの自動化
 - ・継続的に開発することで、新たな価値提供の可能性もある
購入後の追加機能の購入 (Feature on Demand)
購入後の機能更新の購入 (制御プログラムの最適化)
段階的ロールアウト (リリース) において更新を早く受け取る権利の購入
 - ・継続的改善のために必要な点
継続的改善のための開発体制

- 開発者の確保
- 新製品の開発と改善を同時に進められることが望ましい
- 製品群の定義による共通化 (プロダクトラインエンジニアリング)
- 車両のプラットフォーム/アーキテクチャ/シャーシの共通化と同様
- より精緻な品質保証と開発の仕組み
- これまでは製品⇔品質保証⇔法規、基準
- これまでは製品⇔品質保証⇔法規、基準・実行環境

◆私の研究グループでの研究テーマ

- テーマ1: V&V 戦略
- 個別のサービス、リファレンスモデルにおいて問題を早期に検出するための仕組みを検討している
- 地図やコース上でもMRC (Minimum Risk Condition) が偏在している等の「そもそも」難しいという見立て
- この車両の仕様や運行速度ではリスクが大きいという見立て
- テーマ2: 継続的インテグレーションでの Defect-prone テストの識別
- 継続的インテグレーション
- コード変更後にテストを実行し、問題が起きていないかを確認する
- 変更するとすぐにテスト結果がフィードバックされ、デグレード等に気づきやすくなる
- コード変更で新たなバグを混入した場合に見つかりやすくなるので、積極的にコード変更できる
- 継続的インテグレーションの課題
- テストが増えるとテストの実行時間が長くなる
- バグが出やすいテストから実行していく

(講義の感想)

今回の講義は車載ソフトウェアに関する開発手法について、詳しく解説いただきました。個人的にはこれまでにあまり聴講したことが無い講義内容だったので、理解が進むか不安でしたが、使用している用語や例え話は日常生活に基づいた内容で、ユーモアを交えて話していただいたので、とても分かりやすく興味深い話でした。

特に最後にお話しいただいた研究テーマでは、継続的インテグレーションにおいて、バグが出やすいテストを先行して実施していく、という研究内容でしたが、広くソフトウェア開発者の興味をそそる内容だったと思います。

今後の研究内容とその展開についても、勉強させて頂きたいと思いました。

大変有意義な講義、ありがとうございました。

以上