

IEEE OTA Software Updates - the Big Picture

> Florian Rohde System Integration and Validation Consultant



Agenda

- Introduction
- Motivation
- High Level Picture
- Dive In
 - Continuous Integration
 - Agile in Automotive
 - Software Branching Strategy
 - Automated Regression Testing
 - Over the Air Software Updates
 - Safety and Security



Introduction





Motivation - SDV and OTA updates

- Continuous improvement of the UX
- Customer interaction after initial sale
- New revenue streams
- Complete feedback loop
- Preventive Maintenance
- Avoid physical recalls



Some Tesla Numbers

Total Software R&D: ~700 engineers, techs, interns Number of customer software releases per year: ~150 Number of vehicle software builds per day: >20 Number of full vehicle regression tests per week: >17



What's needed?



Continuous Integration

Branching Strategy

Automated Regression Testing

Requirements Management

Cl Server Change Over the air updates (OTA)

Change Management

Agile in Automotive

Common Repositories

Configuration Management

MQTT Broker



Continuous Integration





CI Server

- Run static code checks
- Compile source code
- Perform unit tests
- Package software
- Tag builds and packages
- Communicate build information, progress, results, and issues
- Orchestrate build resources
- Archive build details
- Communicate build status and information

Examples:

- CD Jenkins
- Atlassian Bamboo
- Microsoft Azure Pipelines
- Circle Cl



Agile in Automotive - Trains

- Synchronized sprints 2 weeks (2 months for HW)
- Scheduled Release Trains
- Special urgent Release Trains (Hotfix)





Branching Strategy

- Vehicle software packages
- Backbone software integration
- Stable branch for hotfixes
- No new features in validation branch
- Only fully validated merges
- Separate feature branches
- Regression test on all branches





Agile in Automotive - Organization





Agile in Automotive - Organization





Agile Process - Toolchain





Validation





Automated Regression Testing - Goals

- Continuous Integration (CI) needs Continuous Validation (CV) for full power (not Continuous Deployment (CD))
- Test early Fail early Fix Early
- Main issue source in a complex mechatronic product is the integration
- Run vehicle level tests as early and as often as possible
- Allow feature branches in full vehicle tests
- Merge all levels of testing into one complete picture





Automated Regression Testing - Concept





Automated Regression Testing - Toolchain





Over the air updates (OTA)

- Universal Packaging
- Hardware Diversity Layer
- Signed Packages
- Production Fuse
- Gateway Manifest
- Hardware IDs
- Hosted Server Cloud
- WiFi and LTE/5G
- Release Notes
- Binary Diff





Over the air updates (OTA) - Pipeline





Over the air updates (OTA) - Safety and Security



- Process at the Manufacturer
- Unique Identifiers
- Vehicle Software Database
- Vehicle Manifest
- Vehicle Integration
- Vehicle Grouping
- Compatibility Validation
- Change Impact Analysis
- Feature Update Analysis
- Safety Impact Analysis
- User Information
- Update Documentation



Over the air updates (OTA) - Safety and Security



In the European Union UNECE WP.29/R155 will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024



Helping automotive companies deliver better software

Florian Rohde

Founder | System Integration & Validation Consultant florian@iprocess-consulting.com