Abstract: Qualification challenges in next generation automotive performance ECUs

Dr. Moritz Neukirchner
Elektrobit Automotive GmbH
Braunschweig, Germany
moritz.neukirchner@elektrobit.com

***Abstract* — The specification of the AUTOSAR Adaptive Platform introduces the capability to dynamically load individual software applications that are automatically configured and started through the platform on the basis of manifest files. Communication among these applications is established at runtime via a service-oriented communication middleware that is agnostic of the underlying communication mechanism. Despite such dynamics of the platform, automotive applications still demand guarantees on real-time, safety and security. This presentation outlines the scope, architecture and capabilities of the AUTOSAR Adaptive Platform and the verification challenges that arise from state of the art performance ECUs.**

I. Introduction

The software of automotive ECUs is currently undergoing great changes in terms of architecture, communication paradigm and lifecycle. The main drivers for these changes are applications for highly automated driving (HAD) and connectivity solutions. While the former largely depend on feature rich operating systems and standard libraries such as OpenCL and require high processing power, the latter require to establish short software lifecycles in order to provide frequent updates of individual software components. Both sets of requirements are hard to accomplish with current automotive platforms, as e.g. the AUTOSAR Classic Platform.

Until now the software of automotive ECUs is typically integrated and qualified completely before deployment into the field. This means that all functionality including the operating system and basic software is previously available and configured, and a single binary is flashed onto the target device. In case updates are required later in the field (e.g. as part of a recall) the complete ECU is re-flashed with a new software version. Runtime dynamics e.g. with respect to resource allocation is not permitted. The AUTOSAR Adaptive Platform [1] changes this paradigm in order to support the above use-cases.

II. ADAPTIVE AUTOSAR

The AUTOSAR Adaptive Platform introduces a new development workflow as shown in Figure 1. It is separated into an offboard part (top) and an onboard part (bottom). In the offboard part software and platform properties and configuration parameters are described through a service interface description and manifest files. When an application is deployed on the target ECU, the software package contains not only the binary code, but also a description of the application in the form of a manifest. On the target the manifest SW Package is checked by SW Configuration Management for integrity and compatibility with the platform before it is configured and started through Execution Management based on the information contained in the Manifest file.

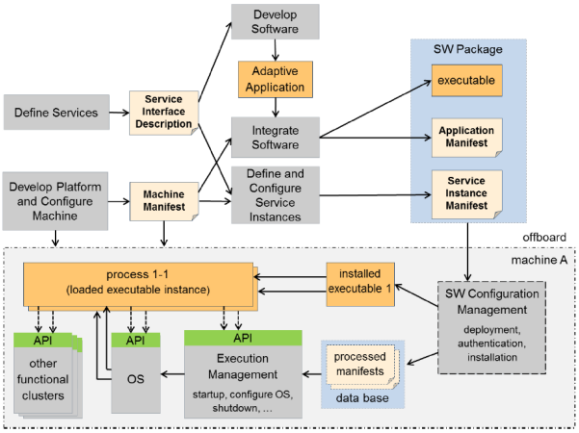

Figure 1: Development Workflow [2]

III. VERIFICATION CHALLANGES

This development process, as introduced in Adaptive AUTOSAR poses new challenges to the verification of an ECU. At the point in time, at which the ECU is initially deployed not all software functionality and their requirements are known. Conversely, an application developer may not be fully aware of the configuration of the ECU onto which the software is deployed. As a result, the design time verification of properties is becoming increasingly complex. Possible remedies to this are e.g. i) on-board verification of requirements, ii) runtime mechanisms for isolation and monitoring of requirements, and iii) runtime supervision through external watchdog functionality.

References

[1] AUTOSAR Adaptive Platform, https://www.autosar.org/standards/adaptive-platform/
"Explanations of Adaptive Platform Design", AUTOSAR, Release 17-03