Smart Software, Smart Trucks

Safety, efficiency, and availability are the core requirements for commercial vehicles. Technology supplier WABCO has implemented a consistent process to optimize the development of safety-critical, reliable systems. It is based on a comprehensive tool chain in which SystemDesk and TargetLink pave the way to AUTOSAR- and ISO 26262-compliant development.

Efficient processes and methods for developing safety-critical driver assistance systems

Trucks and buses are more efficient and safer when they are in the correct lane at the right speed, have the appropriate tire pressure, and use the smartest collision avoidance systems. Driver assistance systems from WABCO make sure this is the case. The systems are integrated in the complex electrics/electronics (E/E) systems of commercial vehicles from a range of manufacturers. They support the driver by communicating with sensors and actuators in the vehicle. But developing and implementing safety-critical systems involves a number of challenges, which have to be considered when planning tool chain design and the development process. Compliance with important standards, such as ISO 26262 and AUTOSAR, is not the only crucial factor for developers. They also have to optimize development times and costs so that the products are as innovative as they are competitive. The tool chain therefore has to address the following criteria: continuity, traceability, automation, change management, and test front-loading. This is why WABCO uses a process designed like a double V-model (figure 1). It enables developers to quickly perform tests at any time during development.

Developing the AUTOSAR Structure

The development is based on requirements specified in PTC Integrity. Design guidelines ensure that the requirements are sufficiently detailed and formalized to export rudimentary AUTOSAR configuration files (ARXML files) from them with a custom plug-in. The configuration files are imported to the architecture tool dSPACE SystemDesk. This results in a software structure with the names of the structure components. In SystemDesk, the developers add implementation details, data types, and AUTOSAR communication mechanisms to the structure and pass it to the TargetLink Data Dictionary. TargetLink can then be used to generate the frame models for the AUTOSAR software components and the developers can insert function models (figure 2). These processes are directly linked and can be automated by means of a script to ensure more efficiency and prevent errors. The tool coupling makes it possible to trace requirements between requirements management and the development environment. Comments are even passed to the models. >>

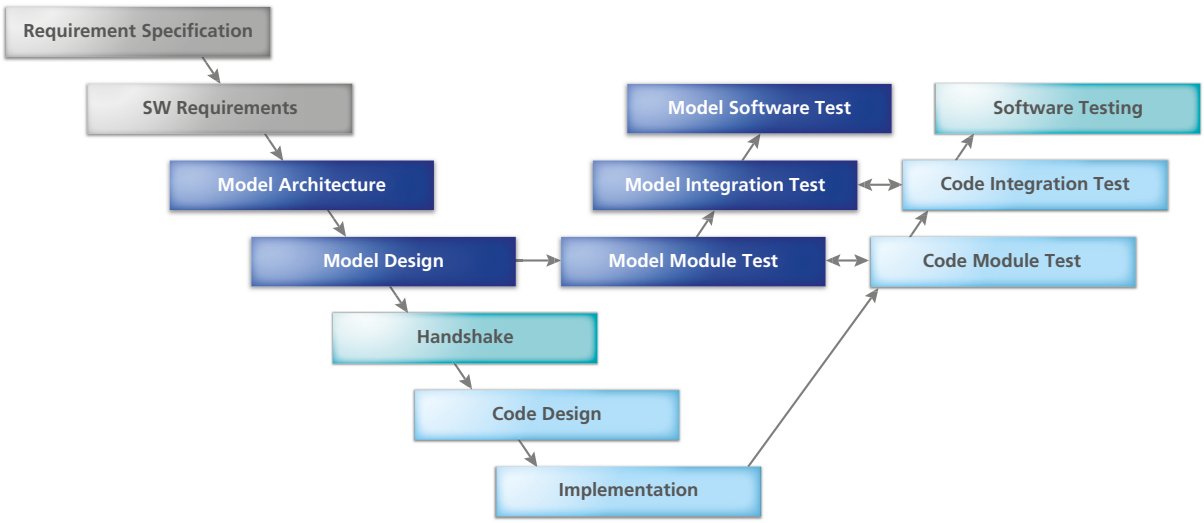


Figure 1: The process established at WABCO is modeled after the V-model, which has been extended to a double-V-model so that software-in-the-loop (SIL) tests can be performed even during the specification and design phase. The aim is a seamless transition between all process steps. This is achieved by means of tool integration.

Model-Based Control Design

WABCO uses Simulink/TargetLink for controller development. These model-based tools transform the requirements into a function model. In the first step, the modeled function has to meet all functional requirements, but not yet the restrictions of the target hardware. The functional requirements are checked by means of model-in-the-loop (MIL) simulation in TargetLink. The requirements and the methods called for by ISO 26262 result in test cases for comparative function testing. In the next step, the function and model are optimized for the target hardware before production code generation with TargetLink. The code and model then pass back-to-back tests in BTC EmbeddedTester from BTC Embedded Systems to verify the code.

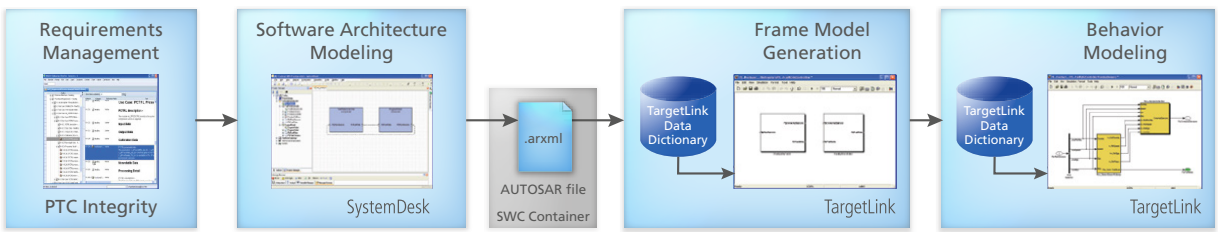
Software Implementation

The AUTOSAR software components that constitute the WABCO software are composed of several modules, which contain the individual functions. Incremental code generation in TargetLink is used to generate code for each model separately. This makes it possible to work in distributed development teams. It also ensures that the tested code of individual modules can be integrated in the AUTOSAR software component (SWC). Incremental code generation is particularly useful for complex SWCs because it is not necessary to generate the module code every time, which significantly reduces code generation times. After the assembled SWC is tested, it is integrated in the overall software for the electronic control unit (ECU).

Efficient Software Verification

A decisive factor for software quality is continuous testing throughout the development process. Early and comprehensive testing means that a high level of maturity is reached faster and more efficiently. WABCO developers use their own tools for consistency and plausibility checks to de-

Figure 2: From requirements to control design. A seamless transition between tools is the basis for the efficient development of complex solutions, such as driver assistance systems.



> "The production code generator TargetLink is particularly valuable because it is certified for software development in line with the safety-relevant standards ISO 26262 and IEC 61508."
>
> *Holger Jakobs, WABCO*

tect and fix design errors right from the start of a project. In the development process, WABCO also uses the following tools from the TargetLink Ecosystem for software validation:

BTC EmbeddedTester: Intelligent test case generation for fully automatic, ISO 26262-certified back-to-back testing.

MES MXAM: Automatic check to determine compliance with relevant guidelines (modeling guidelines, MISRA, TargetLink Modeling Guidelines). The tool is used early in the development process to make sure that even the initial designs are in line with the guidelines. The software is checked before release.

MES M-XRAY: Analysis of model structure and complexity. The tool provides metrics for assessing the complexity and the potential criticality that is relevant for software safety. The tool therefore supports ISO 26262-compliant development.

An in-house reporting tool supports the initiation of tests, summarizes the results, and continuously monitors the project progress.

Results and Outlook

The implemented tool chain made it possible to complete cutting-edge ADAS projects (figure 3). All systems have gone into series production and are used in trucks and buses from various manufacturers. WABCO is planning to use the PC-based simulation platform dSPACE VEOS in addition to the dSPACE Simulator that is currently used for ECU validation to find errors even earlier. ■

Holger Jakobs, WABCO

Figure 3: Examples for successful ADAS projects: The lane keeping assistant OnLane-ASSIST™, the turning assistant OnCity™ Urban Turning Assist, and the autonomous emergency braking system (AEBS) OnGuard-MAX™.

Mission Accomplished: A Seamless Tool Chain

A tool chain becomes seamless through a direct exchange of data between successive development steps and tools. WABCO has achieved this with the following standard tools and its own automation scripts:

- Requirements management: PTC Integrity™
- Architecture design: dSPACE SystemDesk
- Control design: Simulink®/dSPACE TargetLink
- Code implementation: TargetLink
- Software verification: BTC EmbeddedTester, MES MXAM, MES MXRAY, own custom tools

Holger Jakobs
Holger Jakobs is an expert for model-based software development with Simulink and TargetLink in the competence center for application software at WABCO in Hanover, Germany.