

TargetLink for Safety-Critical Systems

- **ATENA Engineering uses automatic production code generation**
- **Standards for software in safety-critical systems**
- **TargetLink embedded in a company-specific tool chain**

The vehicles of the future will contain more and more safety-critical electronics. Developing them will be a major challenge to the industry. ATENA Engineering is already in a position to offer automotive manufacturers and suppliers comprehensive expertise in developing safety-critical systems. The development process used for such systems at ATENA Engineering is based on the experience and standards in the aviation industry and uses dSPACE TargetLink for automatic production code generation.

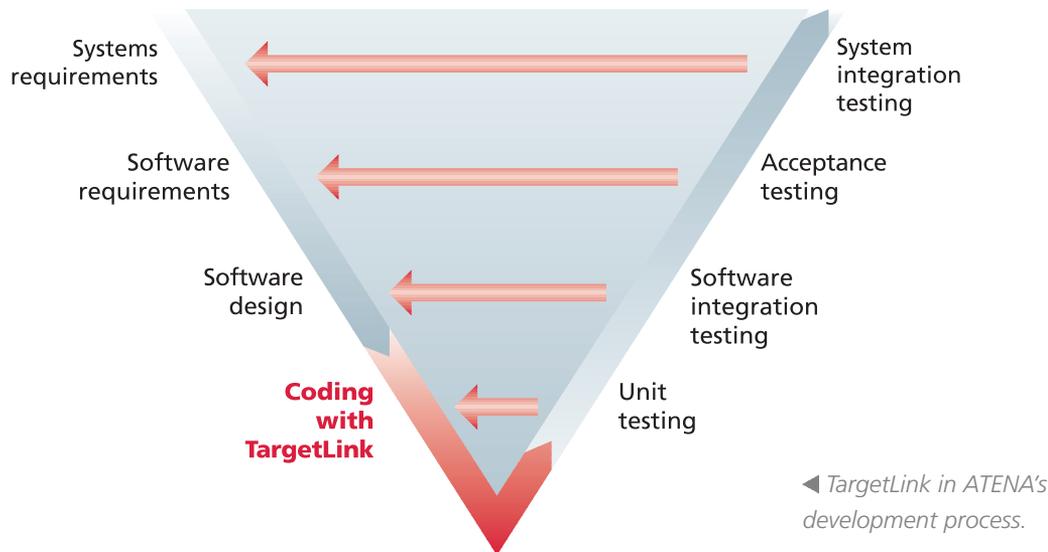
Know-How for Safety-Critical Systems

The number of safety-critical systems in vehicle electronics is rapidly increasing. Just a few years ago, the worst that could happen if a system had an error was that a function failed. In future systems, it will be a safety hazard for the vehicle's occupants and other road users. The IEC 61508 safety standard for automotive electronics was set up to minimize the hazards of such systems. Complying with it poses a particular challenge to software development.

At ATENA Engineering, we have many years of experience in developing safety-critical systems in the aviation sector through close cooperation with our parent company, MTU Aero Engines GmbH. MTU Aero Engines GmbH develops and produces the engine controllers for a number of European aviation projects. The aircraft engine controllers are multichannel electronic control units (ECUs) with between 4 and 10 processors and have to meet tough safety requirements. The standard governing



▲ ATENA Engineering uses know-how from the aviation industry for safety-critical automotive electronics.



the development process for these controllers is RTCA DO178, a concrete form of the IEC 61508 safety standard that is suitable for the automotive industry. This means that ATENA is in a position to apply software development standards for safety-critical systems comprehensively in automobiles.

Because projects are often subject to frequent modification, we decided to use an automatic production code generator. Moreover, the software design is often available as an executable specification, which a production code generator implements with a far lower error rate than does handcoding. A production code generator is much more reliable. It does not make careless mistakes, and there are no misinterpretations in implementing the model.

ATENA Chose TargetLink

At ATENA we have defined and implemented a software development process for safety-critical systems using dSPACE's automatic production code generator TargetLink. TargetLink can be seamlessly integrated into MATLAB®/Simulink® and allows software designs that are available as Simulink/Stateflow® models to be reliably converted into C code.

Before deciding in favor of TargetLink, we evaluated the code generators available on the market in depth. The reasons for our decision were high product quality, especially the quality of the generated production code, and TargetLink's technical features. A vital factor is that TargetLink offers comprehensive configuration

options that our process uses to meet the requirements of code in safety-critical systems.

Proven Development Process at ATENA

The software development process, whose implementation phase TargetLink supports, has now been in use at ATENA since November 2002. TargetLink is embedded in a project-specific tool chain. The tool chain ensures compliance with the quality criteria for safety-critical applications and also allows a high degree of automated implementation. We use it to develop safety-critical vehicle systems that are classified according to IEC 61508 SIL3 and whose software comprises up to 25,000 lines of code. Automatic code generation plays a very important part in all this. Using TargetLink, we have succeeded in automatically generating approx. 80% of the entire production code, including our hardware interfaces.

ATENA and dSPACE are cooperating closely to extend integration into our tool chain in future versions of TargetLink and to reinforce the support given to safety-critical aspects of code generation

*Hermann Tauber
Team Leader, Electronics
ATENA Engineering GmbH
Germany*

*Michael Jungmann
MTU Aero Engines GmbH
Germany*