TargetLink für sicherheitskritische Systeme

- ATENA Engineering nutzt automatische Code-Generierung
- Standards für Software in sicherheitskritischen Systemen
- TargetLink eingebettet in firmenspezifische Werkzeugkette

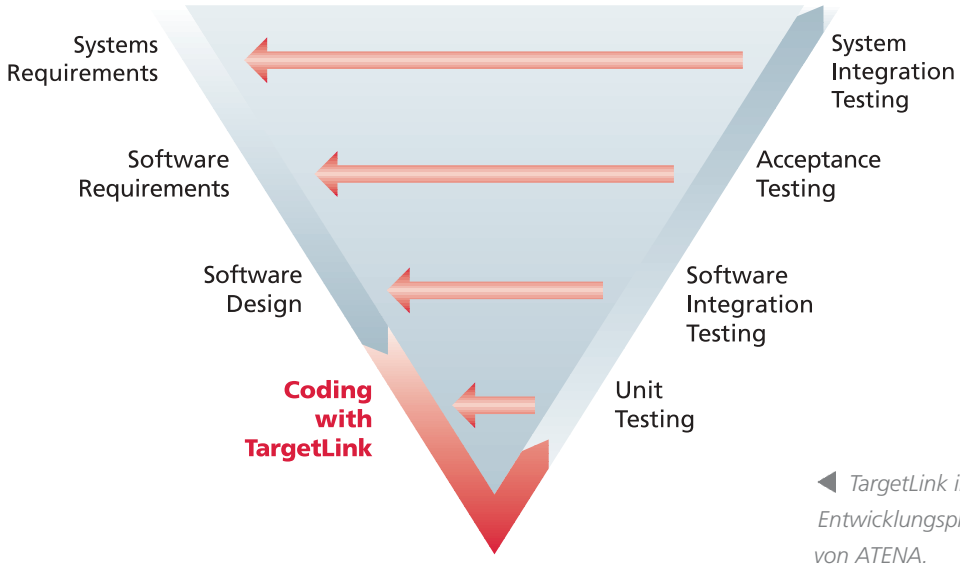
Zukünftig werden Fahrzeuge in immer größerem Maße elektronische, sicherheitskritische Systeme enthalten. Ihre Entwicklung wird die Industrie vor erhöhte Anforderungen stellen. ATENA Engineering ist schon heute in der Lage, Herstellern und Zulieferern aus der Automobilindustrie umfassende Kompetenz bei der Entwicklung sicherheitskritischer Systeme anzubieten. Der für solche Systeme bei ATENA Engineering eingesetzte Entwicklungsprozess basiert auf Erfahrungen und Standards aus der Luftfahrtindustrie und verwendet dSPACE TargetLink zur automatischen Seriencode-Generierung.

Know-how für sicherheitskritische Systeme

Die Anzahl sicherheitskritischer Systeme in der Automobilelektronik nimmt rapide zu. Vor einigen Jahren zog die Fehlfunktion eines Systems im schlimmsten Fall den Ausfall einer Funktion nach sich. Bei zukünftigen Systemen kann eine Fehlfunktion dagegen ein Sicherheitsrisiko für Fahrzeuginsassen und andere Verkehrsteilnehmer darstellen. Um die von solchen Systemen ausgehenden Gefahren zu minimieren, wurde für die Automobilelektronik die Sicherheitsnorm IEC 61508 als Richtlinie etabliert, deren Beachtung besondere Herausforderungen bei der Software-Entwicklung bedeutet.

Bei ATENA Engineering können wir durch die enge Zusammenarbeit mit unserer Muttergesellschaft MTU Aero Engines GmbH auf jahrzehntelange Erfahrung in der Entwicklung sicherheitskritischer Systeme aus dem Luftfahrtsektor zurückgreifen. Von der MTU Aero Engines GmbH werden die Triebwerksregler für eine Zahl europäischer Luftfahrtprojekte entwickelt und gefertigt. Bei diesen Reglern, die höchste Sicherheitsanforderungen zu erfüllen haben, handelt es sich um mehrkanalige Steuergeräte mit 4 bis 10 Prozessoren. Die Entwicklung dieser Systeme erfolgt seit Jahren nach der Norm RTCA DO178, die eine für den Automobilbereich

ATENA Engineering nutzt Know-how aus der Luftfahrtindustrie für sicherheitskritische Automobilelektronik.



◀ *TargetLink im Entwicklungsprozess von ATENA.*

geeignete Konkretisierung der Sicherheitsnorm IEC 61508 darstellt. Dadurch ist ATENA bereits heute in der Position, Software-Entwicklungsstandards für sicherheitskritische Systeme auch in Automobilen umfassend anzuwenden.

Da Projekte häufig hohen Änderungsraten unterliegen können, haben wir uns für den Einsatz eines automatischen Code-Generators entschieden. Zudem liegt das Software-Design oft schon als ausführbare Spezifikation vor, die durch einen Code-Generator mit weit geringerer Fehlerrate umgesetzt wird, als es bei Handprogrammierung der Fall ist. Ein Code-Generator ist wesentlich zuverlässiger. Er macht keine Flüchtigkeitsfehler, und es gibt keine Fehlinterpretationen bei der Modellumsetzung.

ATENA setzt auf TargetLink

Wir haben bei ATENA einen Software-Entwicklungsprozess für sicherheitskritische Systeme unter Nutzung des automatischen Seriencode-Generators TargetLink definiert und umgesetzt. TargetLink integriert sich nahtlos in MATLAB®/Simulink® und ermöglicht eine sichere Umsetzung unseres in Form von Simulink/Stateflow®-Modellen vorliegenden Software-Designs in C-Code.

Unserer Entscheidung für TargetLink ging eine detaillierte Evaluierung der am Markt verfügbaren Code-Generatoren voraus. Maßgeblich für unsere Wahl waren die hohe Produktqualität, insbesondere die Qualität des generierten Codes, sowie die technischen Eigenschaften von TargetLink. Ganz wichtig ist, dass TargetLink umfassende Konfigurationsmöglichkeiten anbietet, die unser Prozess nutzt, um den Anforderungen an Code für sicherheitskritische Systeme gerecht zu werden.

Bewährter Entwicklungsprozess bei ATENA

Der Software-Entwicklungsprozess, dessen Implementierungsphase maßgeblich von TargetLink unterstützt wird, wird nun seit November 2002 bei ATENA angewandt. TargetLink ist dabei in eine projektspezifische Werkzeugkette eingebettet. Diese Werkzeugkette garantiert einerseits die Einhaltung der Qualitätskriterien für sicherheitskritische Anwendungen, andererseits ermöglicht sie einen hohen Automatisierungsgrad bei der Implementierung. Wir entwickeln damit sicherheitskritische Fahrzeugsysteme, die entsprechend IEC 61508 SIL3 eingestuft sind, und deren Software-Anteil bis zu 25000 Programmzeilen umfasst. Der automatischen Code-Generierung kommt dabei ein sehr hoher Stellenwert zu. So ist es uns mit TargetLink gelungen, ca. 80% des gesamten Seriencodes inklusive unserer Hardware-Schnittstellen automatisch zu erzeugen.

ATENA und dSPACE stehen in engem Kontakt miteinander, um bei Folgeversionen von TargetLink die Integration in unsere Werkzeugkette weiter auszubauen und sicherheitskritische Aspekte in der Code-Generierung noch stärker zu berücksichtigen.

Hermann Tauber
Teamleiter Elektronik
ATENA Engineering GmbH
Deutschland

Michael Jungmann
MTU Aero Engines GmbH
Deutschland