Höchste Sicherheit

Nord-Micro: TargetLink seit dem Jahr 2000 in unterschiedlichsten Flugzeugtypen im Einsatz

In Flugzeugen mit Druckkabine muss der Luftdruck über spezielle Ventile und Regelalgorithmen mit höchster Zuverlässigkeit gesteuert werden. Die Sicherheit der Passagiere und der Crew in großer Flughöhe steht an erster Stelle. Mit dem Seriencode-Generator TargetLink entwickelt Nord-Micro bereits seit dem Jahr 2000 erfolgreich Kabinendruckregelungen für unterschiedlichste Flugzeugtypen. Die mit TargetLink generierte Software erfüllt in Verbindung mit den Entwicklungsprozessen problemlos die strikten Vorgaben von Flugzeugherstellern wie Boeing und Airbus sowie der Luftaufsichtsbehörden FAA und EASA.

Kabinendruckregelung: Sicherheit geht vor

Die automatische Regelung des Kabinendrucks gehört bei Flugzeugen mit Druckkabine zu den Funktionalitäten, die von Passagieren und Crew außer während des Sinkflugs und in der Landephase kaum wahrgenommen werden. Eine zuverlässige Kabinendruckregelung ist für die Insassen jedoch von größter Wichtigkeit. Unter den Bedingungen außerhalb des Flugzeugs wäre ein Überleben ab einer bestimmten Flughöhe nicht mehr möglich. Deshalb ist eine Kabinendruckregelung, über Komfortaspekte hinaus, zu allererst eine sicherheitskritische Funktionalität, die jederzeit fehlerfrei funktionieren muss. Bei einer fehlerhaften Steuerung oder einem Systemausfall müsste ein sofortiger Notsinkflug eingeleitet werden, während die Flugzeuginsassen unmittelbar zu den Sauerstoffmasken greifen müssten. Als mechanische Komponenten einer Kabinendruckregelung sind besonders die elektronisch gesteuerten Auslassventile von Bedeutung, die in Abhängigkeit von der Frischluftzufuhr die Ver-

teilung und bedingt durch die Abluft den Kabinendruck regeln. Diese komplexen Ventile sind auf jeden Flugzeugtyp exakt abgestimmt. Die zur Ventilsteuerung notwendige Software ist auf mehreren elektronischen Controllern implementiert. Die Controller sind jeweils über eine spezielle Schnittstelle zur Signalanpassung (Remote Data Concentrator) an den Flugzeug-Datenbus und somit an das Flight Management System (FMS) angebunden (Abbildung 1). Während Druckinformationen über Sensoren aus der Kabine an die zuständigen Controller gelangen, werden die Umgebungsdaten vom FMS geliefert. Neben der Sicherstellung des Kabinendrucks innerhalb vorgegebener Limits kontrolliert die Kabinendruckregelung auch weitere Aspekte. Dies sind zum Beispiel die für den Komfort der Passagiere relevante Druckänderungsrate sowie der Schutz der Flugzeugaußenhülle vor Beschädigungen, die durch zu große Unterschiede zwischen Außen- und Innendruck auftreten könnten.

Nord-Micro: Erfolgreicher TargetLink-Einsatz seit 2000

Nord-Micro besitzt langjährige Erfahrung in der Entwicklung von leistungsstarken und zuverlässigen Kabinendruckregelungen, insbesondere für Passagierflugzeuge mit über 80 Sitzen. Bereits seit 2000 setzt Nord-Micro für die Entwicklung und Code-Generierung der Controller-Software erfolgreich den dSPACE-Seriencode-Generator TargetLink ein. Zahlreiche Flugzeuge von Regionaljets bis hin zum Airbus A380 haben daher heute Kabinendruckregelungen an Bord, die mit TargetLink entwickelte und codierte Controller-Software enthalten (Abbildung 2). Die so entwickelte, sicherheitskritische Software erfüllt die strikten Anforderungen, die von den Flugzeugherstellern und den Zulassungsbehörden für die Verwendung im Flugzeug gefordert werden, einschließlich einer Zertifizierung bis hin zum Sicherheitslevel A (Abbildung 2). Maßgeblich ist vor allem der Standard DO-178B, der die Anforderungen an die Software-Entwicklung in der Luftfahrt beschreibt. In neueren Projekten setzt Nord-Micro TargetLink als Design- und Codierungswerkzeug ein, macht aber auch von der umfangreichen Testunterstützung in TargetLink Gebrauch, etwa zum vereinfachten Durchführen von Code-Reviews, Modultests auf dem Zielprozessor sowie einer Werkzeugintegration mit IBM® Rational® Test RealTime (RTR) zur Analyse der erforderlichen Code-Abdeckung.

Hohe Anforderungen durch Zulassungsbehörden und Flugzeughersteller

Da Nord-Micro die entwickelte Software für ein sicherheitskritisches System einsetzt, ergeben sich zahlreiche Anforderungen an TargetLink in Bezug auf die Qualität der Modelle und des generierten Codes:

- ***Unterstützung von Codierrichtlinien***
  Nord-Micro und die Flugzeughersteller schreiben im Hinblick auf DO-178B Codierrichtlinien vor. In der Praxis zeigt sich, dass TargetLink Code generiert, der konform mit den Vorgaben ist. Dies betrifft etwa die Einhaltung von MISRA-Richtlinien, die in den hauseigenen Codier-Standard bei Nord-Micro eingeflossen sind. Spezielle Anforderungen, wie beispielsweise die Erzwingung eines expliziten Return-Statements in jeder Funktion, lassen sich gut durch Einhaltung eines bestimmten Modellierungsstils erfüllen.

- ***Lesbarkeit des Codes***
  Der von TargetLink generierte Code ist übersichtlich strukturiert, verständlich kommentiert und mit aussagekräftigen Symbolnamen versehen. Die gute Lesbarkeit vereinfacht bei Nord-Micro maßgeblich die Durchführung von Code-Reviews.

- ***Anforderungen an den modellbasierten Entwurf***
  Der modellbasierte Entwurf wird noch nicht von der DO-178B reglementiert. Daher machen die europäischen und amerikanischen Luftfahrt-Zulassungsbehörden mittlerweile Vorgaben, wie Anforderungen aus der DO-178B in Anforderungen an den modellbasierten Entwurf zu übersetzen sind. Die Vorgaben betreffen unter anderem die sinnvolle Benennung von Signalen in Modellen und den eingesetzten Modellierungsstil. Mit TargetLink lassen sich die strengen Vorgaben leicht umsetzen.

- ***Deterministische Code-Generierung***
  Die Effizienz der Testprozesse von Nord-Micro profitiert von einer deterministischen Code-Generierung. Durch den Determinismus lässt sich sicherstellen, dass sich Änderungen an einer Teilfunktion nur lokal auswirken und bereits getestete Funktionalitäten von

Änderungen in anderen Modellsegmenten unberührt bleiben. Dies wird beispielsweise durch einen intelligenten Mechanismus zur Durchnummerierung von Subsystemen erreicht, der Code-Änderungen lokal eingrenzt.

> „Die strengen Anforderungen der europäischen und amerikanischen Luftfahrt-Zulassungsbehörden an die modellbasierte Entwicklung werden von TargetLink problemlos erfüllt."
>
> *Andreas Alaoui, Nord-Micro*

■ ***Hohe Code-Effizienz***

Der von TargetLink generierte Code ist auch auf Optimierungslevel 0, wie er für sicherheitskritische Anwendungen in der Luftfahrt in der Regel eingesetzt wird, immer noch hinreichend effizient, um auf dem Controller in der geforderten Zeit ausgeführt werden zu können.

Effiziente Entwicklungsschritte mit TargetLink

Der Einsatz von TargetLink im Entwicklungsprozess bei Nord-Micro beschränkt sich nicht auf die automatische Codierung, sondern umfasst darüber hinaus die folgenden Features bzw. Prozessschritte (Abbildung 3):

■ ***Definition der Software-Anforderungen***

Die Anforderungen werden von Nord-Micro in dem Anforderungsmanagement-Werkzeug Telelogic® DOORS® verwaltet und unter Nutzung der Anforderungsmanagement-Schnittstelle von The MathWorks mit TargetLink-Modellen verknüpft. Hierdurch wird eine hinreichende Rückverfolgbarkeit aller Arbeitsprodukte im Entwicklungsprozess zu den Software-Anforderungen sichergestellt.

■ ***Modell-Design***

Für die grafische Modellierung nutzt Nord-Micro MATLAB®/Simulink®/Stateflow®/TargetLink. Zusätzlich wird auch ein UML-Werkzeug verwendet.

■ ***Automatische Skalierung***

Durch Worst-Case-Scaling-Analyse von TargetLink für Fixed-Point-Arithmetik konnte Nord-Micro im Vergleich zur manuellen Codie-

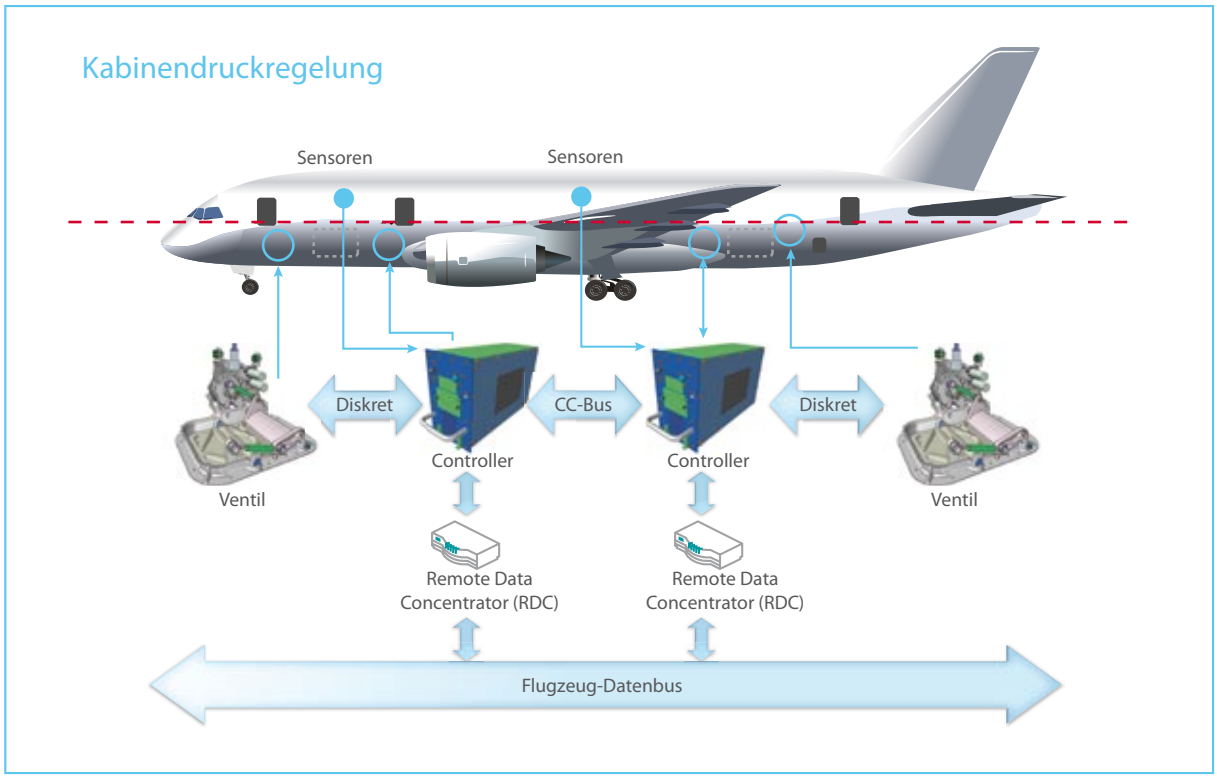


Abbildung 1: Die für die Regelung der Ventile zuständigen Controller sind über den zentralen Flugzeug-Datenbus mit dem Flight Management System (FMS) verbunden.

rung viele Fehler im Vorfeld beseitigen und somit Zeit sparen und Kosten senken. Auch dient die Worst-Case-Autoscaling-Funktionalität zur Unterstützung bei der formalen Verifikation der System-Software.

■ *Automatische Dokumentation*
Die vom Code-Generator automatisch erstellte Dokumentation ist auch gleichzeitig ein Software-Design-Dokument, das folglich nicht mehr manuell angefertigt werden muss. Die Konsistenz zum erzeugten Code ist immer automatisch sichergestellt. Hierdurch spart Nord-Micro erhebliche Aufwände bei den geforderten Design-Reviews ein.

■ *Code-Reviews*
Die Code-Reviews bei Nord-Micro werden durch die klare Struktur, Namensvergabe und Kommentierung des generierten Codes sowie die direkte Rückverfolgbarkeit zwischen Code und Modell maßgeblich vereinfacht.

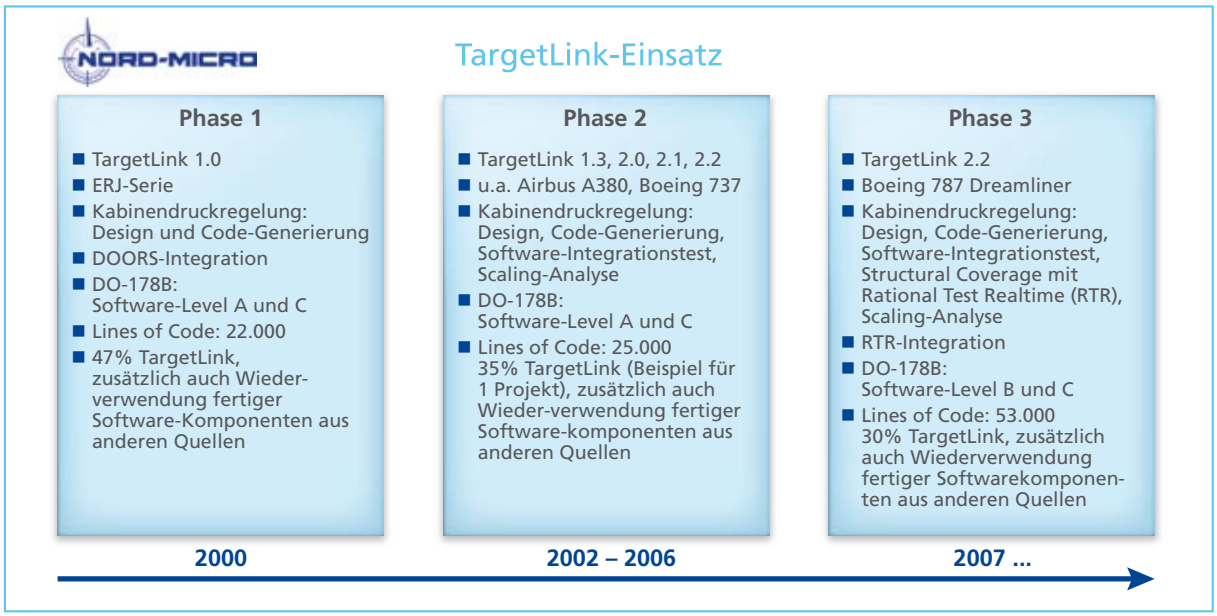
> „Mit TargetLink haben wir erfolgreich mehrere Software-Entwicklungen nach DO-178B durchgeführt, die für Sicherheitslevel A zertifiziert wurden."
>
> *Andreas Alaoui, Nord-Micro*

■ *Software-Integrationstests*
Nord-Micro nutzt TargetLink zur Durchführung von Software-Integrationstests (Abbildung 3). Es werden zunächst geeignete Teststimuli aus Anforderungen abgeleitet. Anschließend werden in TargetLink die Resultate einer Model-in-the-Loop-Simulation mit einer Processor-in-the-Loop-Simulation für diese Teststimuli verglichen, wobei C167- und MPC5554-Prozessoren zum Einsatz kommen. Die Integrationstests beinhalten insbesondere auch eine Analyse der strukturellen Code-Abdeckung, welche mit Hilfe einer Tool-Integration von TargetLink und Rational Test RealTime ermittelt wird. Dadurch reduziert Nord-Micro die Aufwände für Modultests auf das Notwendigste.

Software-Integrationstest mit TargetLink und Rational Test RealTime

Für eines der jüngsten Projekte bei Nord-Micro entwickelten dSPACE

Abbildung 2: Der Seriencode-Generator TargetLink wird seit vielen Jahren erfolgreich zur Entwicklung von sicherheitskritischer Software bei Nord-Micro eingesetzt.



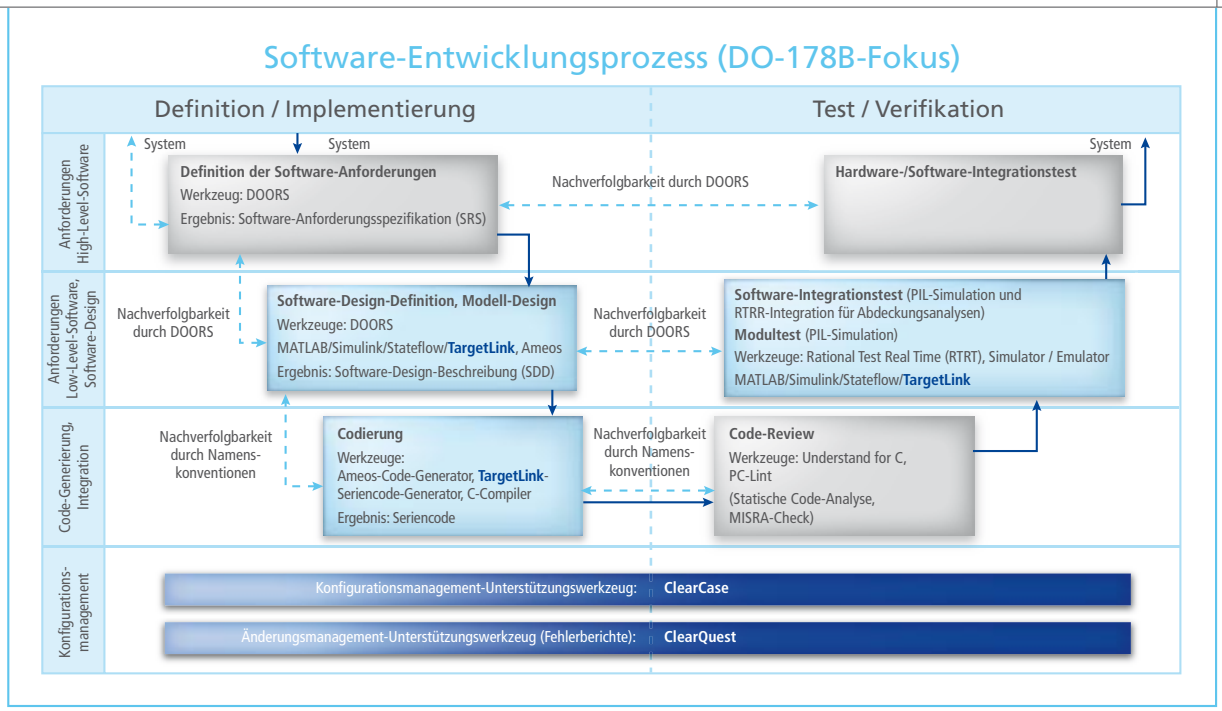


Abbildung 3: Einsatz von TargetLink im Entwickungsprozess bei Nord-Micro.

und IBM Rational eine Werkzeugintegration von TargetLink und Rational Test RealTime (RTR), um den Testprozess bei Nord-Micro noch effizienter zu gestalten. Zunächst wird TargetLink-Code geeignet mit RTR instrumentiert (Vorbereitung des Codes auf den Test) und anschließend ebenfalls RTR verwendet, um Code-Abdeckungsanalysen durchzuführen. Durch die Integration der beiden Tools ist Nord-Micro in der Lage, die Software-Integrationstests auf dem Target-Prozessor unter Benutzung der Simulationsfeatures in TargetLink vorzunehmen und somit die von der DO-178B geforderte strukturelle Abdeckung schon auf Software-Integrationsebene zu erreichen. Mit dieser Vorgehensweise konnte der Aufwand für Modultests radikal auf 20% seines ursprünglichen Wertes reduziert werden. TargetLink verfügt seit der Version 2.0 zwar auch über Funktionalitäten zur Messung der strukturellen Abdeckung, allerdings benötigt Nord-Micro eine formale Tool-Qualifikation für die strukturelle Abdeckung, die von RTR in Form eines Tool-Qualification-Kits bereits zur Verfügung gestellt wird. RTR wird bei Nord-Micro zudem für die Messung der strukturellen Abdeckung beim Hardware-/Software-Integrationstest eingesetzt. Für die Software-Integrationstests erstellt Nord-Micro auf Basis der Anforderungen Testdaten. Anschließend wird basierend auf einer Model-in-the-Loop-Simulation geprüft, ob sich das Modell entsprechend den Anforderungen verhält. Bei positivem Ergebnis wird Seriencode generiert, auf dem Target ausgeführt und diese Resultate gegen die Ergebnisse der Model-in-the-Loop-Simulation geprüft. Im nächsten Schritt wird instrumentierter Seriencode generiert, um die Simulationsresultate für instrumentierten und nicht instrumentierten Code auf Übereinstimmung testen zu können. Ergeben sich auch hier identische Resultate, so kann schließlich die Messung der strukturellen Abdeckung auf Basis des instrumentierten TargetLink-Codes und RTR durchgeführt werden, um die geforderte Abdeckung nachzuweisen. ■

Andreas Alaoui,
Manager Software Engineering,
Nord-Micro AG & Co OHG
Deutschland

Fazit

Die Projekte der letzten Jahre von 2000 bis heute haben uns gezeigt, dass TargetLink ideal als Entwicklungswerkzeug und Seriencode-Generator für sicherheitskritische Luftfahrtanwendungen geeignet ist. Die strikten Vorgaben von Flugzeugherstellern und Zulassungsbehörden im Hinblick auf Entwicklungsprozesse und Codierrichtlinien konnten mit Hilfe von TargetLink vollständig erfüllt werden, so dass von TargetLink generierter Code mittlerweile in zahlreichen Flugzeugtypen im Einsatz ist. Wir schätzen unter anderem auch die gute Lesbarkeit des TargetLink-Codes, die Rückverfolgbarkeit zwischen Code und Modell und den Determinismus bei der Code-Generierung, was unsere Testaufwände erheblich reduziert.

Die flexible Konfigurierbarkeit des Source-Codes erlaubt es uns darüber hinaus, ohne größere Probleme mehrere TargetLink-Modelle in unsere Echtzeitsoftware einzubinden. Der Source-Code ist so effizient, dass unsere Echtzeitanforderungen immer erfüllt werden. Die Integration mit anderen Entwicklungswerkzeugen wie DOORS und Rational Test RealTime gestaltete sich problemlos. Aufgrund der bisher gesammelten Erfahrung wird Nord-Micro TargetLink auch zukünftig für die Entwicklung von Kabinendruckregelungen in neuen Flugzeugen einsetzen.