Designfehler früh erkennen

Modellierung von Ausfällen in der virtuellen Produktentwicklung

Die modellbasierte Entwicklung wird in der Elektronik- und Softwareindustrie bereits seit vielen Jahren angewandt. Zum Beispiel werden in der Schaltungsentwicklung computerunterstützte Modelle wie Spice bereits seit den 1970er-Jahren eingesetzt. Im Bereich des Systems Engineering kam diese Entwicklung für Branchen wie Aerospace, Automatisierungstechnik oder Medizingeräte zwar etwas später, durchdringt aber auch hier immer mehr Bereiche. Die Vorteile, die das frühe Erkennen von Designfehlern bietet, sind signifikant.

Alexander Wille, Wolfram Luithardt, Wolfgang Berns

Das klassische V-Modell (Bild 1), das im Rahmen von Systementwicklungen häufig eingesetzt wird, zeigt die Phasen einer typischen Entwicklung von komplexen Systemen sowie den Konkretisierungsgrad des Produkts, auf dessen Ebene gearbeitet wird, in der Tiefe. Der Konkretisierungsgrad ist als Mass dafür zu verstehen, wie oft die Entwicklung in weitgehend unabhängige Teilentwicklungen (meist durch unterschiedliche Teams) separiert wurde, um die Komplexität des Produkts zu beherrschen: Auf oberster Ebene wird das Produkt als Ganzes betrachtet, auf unterster seine Bausteine auf der Ebene der einzelnen Komponenten. Auf der linken Seite des «V» wird das System konzipiert, spezifiziert und entworfen. An der unteren Kante erfolgt die Implementierung. Auf der rechten Seite werden die Konkretisierungsgrade in umgekehrter Reihenfolge erneut durchlaufen, die Teile des Produkts integriert und die Übereinstimmung von integrierten Produktsegmenten bzw. des finalen Produkts mit den entsprechend spezifizierten Anforderungen sichergestellt. Jeder Schritt in diesem Bereich wird nur dann abgeschlossen, wenn Integration und Verifikation auf der entsprechenden Ebene erfolgreich abgeschlossen werden konnten.

Aufwand bei Designfehlern

Ein grosses Problem jeder Entwicklung von immer komplexer werdenden Systemen ist, dass Spezifikationsfehler bzw. Designfehler oft erst kurz vor der Zulassung oder Produktion erkannt werden. Eine Korrektur erfordert in solchen Fällen einen erneuten Durchlauf aller Aktivitäten auf beiden Seiten des «V» ab der Ebene, in der der Fehler vorliegt. Früh im V-Modell verursachte Fehler sind deshalb sehr teuer, wenn sie erst im Aufwärts-Ast auf gleicher Höhe erkannt werden. Deshalb werden modellbasierte Methoden im Systems Engineering eingesetzt. Ein Schlüsselkonzept dieser Methodenfamilie ist die übersichtliche Darstellung oder sogar das «spielbar»-Machen von spezifiziertem Systemverhalten mithilfe von Modellbildung und Simulation. Fehler in der Spezifikation oder im Design fallen so schon auf, wenn die zur Korrektur nötige Änderungsschleife noch klein ist. Natürlich benötigt eine solche Vorgehensweise entsprechend gute deskriptive bzw. analytische Modelle, welche meist nur aus theoretischen Überlegungen und viel Erfahrung gewonnen werden können.

Modellierung zeigt Realisierbarkeit früh auf

Aktuelle Modellierungsumgebungen und Simulationssoftware sind in der Lage, für eine Vielzahl von Systemen die Korrektheit von Anforderungen sehr früh untersuchbar zu machen. Der nächste Schritt liegt nun in der Erweiterung dieser Konzepte vom linken «Ast» des «V» zum rechten. Bei der virtuellen Systemintegration wird die Taktung der Integration anhand der Spezifikations- bzw. Designebenen des Produkts aufgebrochen, und anstelle noch unfertiger Teile treten Simulationen, also virtuelle Elemente des Produkts: Ein Teil des Produkts (z.B. die Mechanik) liegt schon in einer realen Form vor, während z.B. embedded Hard- und Software noch als Modell in PC-basierten Modellumgebungen abgebildet sind. Heutige Modellierungssprachen erlauben meist eine genaue Parametrisierung des stationären und dynamischen Verhaltens des eingebetteten Systems, um die physikalischen Schnittstellen zwischen modellbasiertem, virtuellen Teil und realem Teil charakterisieren zu können. In einer weiteren Phase der Entwicklung kann dann z.B. die Software für das eingebettete System bereits vorliegen, während die Hardware immer noch in virtueller Form auf einer computergestützten Anlage verwendet wird. Entscheidend für die Realitätstreue des Gesamtverhaltens ist in der Praxis oft das Timing: Reales Verhalten enthält kleine Totzeiten und andere geringe Abweichungen der Dynamik, die sich entscheidend auf das feine Zusammenspiel von digitalen und physikalischen Anteilen des Produkts auswirken können. Zu

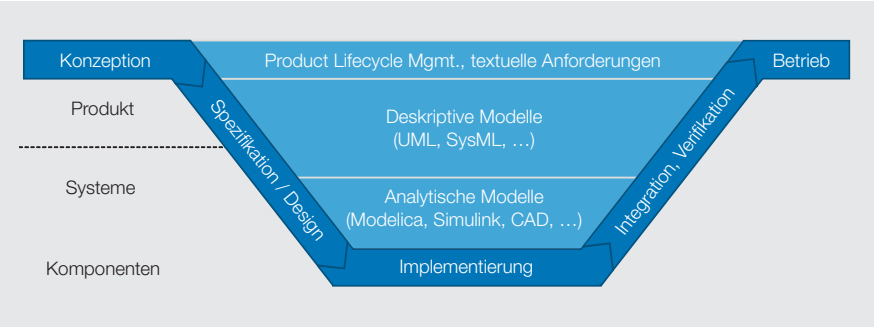


Bild 1 Klassisches V-Modell.

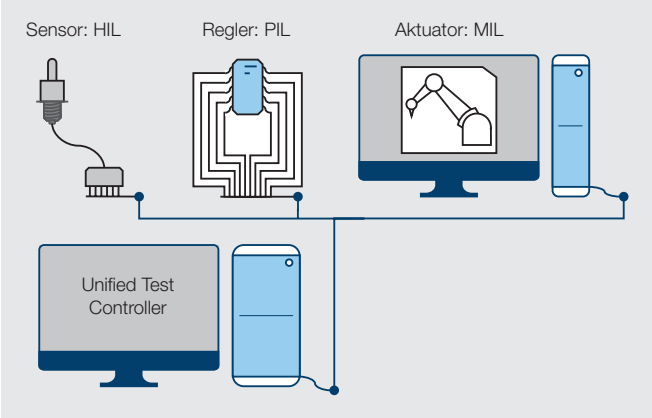


Bild 2 Einzelne Teile des Systems werden durch virtuelle Komponenten ersetzt.

grosse Verzögerungen z.B. durch zu langsame Simulation sind gleichermassen verfälschend. Simulation in Echtzeit erfordert in diesem (erweiterten) Sinne die Einhaltung von maximalen und minimalen Bearbeitungszeiten.

Übergang zwischen Phasen

In Bild 2 ist der Übergang von einer rein modellbasierten Entwicklungsphase in eine teilweise vorhandene reale Umgebung symbolisiert. Während in reinen Modellen zwischen HIL (Hardware in the Loop), SIL (Software in the Loop) und MIL (Model in the Loop) unterschieden wird, kann in einer kombinierten Umgebung jeder einzelne Teilbereich einzeln modelliert werden und das Ganze durch einen gemeinsamen Kontrollteil verbunden werden. Dies hat den Vorteil, dass nun jedes Teilgerät einzeln durch seine reale Komponente ersetzt werden kann. Natürlich benötigt eine reale Software auch einen kompatiblen Prozessor, dieser wird aber immer häufiger ebenfalls als Modell abgebildet. Man spricht dann je nach Tiefe der Modellierung von PIL (Processor in the Loop) bzw. VIL (Virtualisation in the Loop). [1] Im Beispiel von Bild 2 wird der Sensor, der vorher noch in einem HIL-Modell vorhanden war, durch seine reale Komponente ersetzt, ebenso wie die Software, welche nun als «reales» Kompilat in einer modellierten PIL-Umgebung läuft.

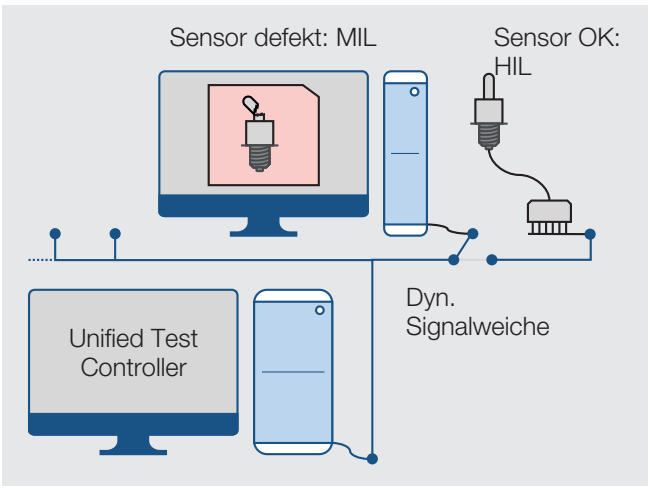
Sicherheit als Schwierigkeit

Als eine der letzten Barrieren für eine vollständige Durchdringung der modellbasierten Systementwicklung sind allerdings Ausfall- und Sicherheitsbetrachtungen noch nicht vollständig umgesetzt. Wie verhält sich das Gesamtsystem, wenn Komponenten bzw. Untersysteme ausfallen oder sich falsch verhalten? In einer reinen Modellumgebung sind solche Verhaltensweisen natürlich relativ leicht zu simulieren, sofern die dynamischen Ausfallmodelle vorliegen. Aber auch hier ist es interessant, modellbasierte Fehlerverhaltensweisen in ein bereits teilweise vorliegendes reales System einspeisen zu können. Vor allem bei sicherheitsrelevanten Produkten verlangen die Normen für funktionelle Sicherheit neben einer disziplinierten Entwicklungsmethodik noch zusätzlich Tests, die beweisen, dass Ausfälle keinen Schaden an Menschen und Umwelt anrichten. Solche Tests sind teuer und in einer frühen Prototypenphase mangels Vorhandensein von Testexemplaren selten durchführbar. Das virtuelle Einspeisen von modellbasiertem Fehlverhalten in ein reales System kann hier einen enormen Nutzen bringen.

Genau in diesem Bereich greifen die vom Kompetenzzentrum Rosas (Robust and Safe Systems Center Fribourg) [2] vorgeschlagenen Lösungen an. Eine vollständige Integration von Sicherheitsbetrachtungen wird nicht nur in der Modellphase eingesetzt, sondern kann auch während der schrittweisen Umsetzung auf reale Komponenten transparent durchgeführt werden. Dafür wurden Komponenten entwickelt, welche Fehler- bzw. Ausfallmodelle in vollständig bzw. teilweise vorhandene Systemkomponenten einbringen können, ohne die Funktion dieser Systemkomponenten im Normalbetrieb zu stören. So können verschiedene Ausfallszenarien simuliert und das implementierte Sicherheitsverhalten des Systems validiert werden (Bild 3). Durch Kopplungskomponenten können Teile des Produkts aus Sicht der übrigen Teile ersetzt werden. Dies ermöglicht Ausfallsimulationen, deren Fehlersignale durch die Schnittstellen zwischen den Komponenten übertragen werden. Dabei muss zwischen analogen und digitalen Signalen unterschieden werden: Während sich die Datenschalter für analoge Signale durch analoge Schalter realisieren lassen, werden die «Weichen» für digitale Signale durch feldprogrammierbare Gate-Arrays (FPGA) implementiert. Diese ermöglichen nicht nur das Einspeisen von komplett fehlerhaften Daten, sondern auch die Simulation von z.B. einzelnen «umgefallenen» Bits oder einer beabsichtigten zeitlichen Verzögerung von eingehenden Daten. Heutige FPGAs sind meist auch schnell genug, um die Verzögerung, die durch das Umgestalten des Datenstroms erzeugt wird, unter den Schwellenwerten für die Echtzeitforderungen der übrigen Teile des Produkts zu halten.

Entwicklungsbeschleuniger

Das hier vorgeschlagene Design kann nicht nur zur Verifizierung von Sicherheitsmechanismen für Einfachfehler herangezogen werden, sondern es können damit auch Mehrfachfehler getestet werden. Was passiert mit dem Aktor, wenn zusätzlich zu einem ausgefallenen Sensor noch ein Fehler in einer Datenübertragung (z.B. verursacht durch eine elek-



Bilder: HEFR

Bild 3 In die Kommunikation zwischen den Systemkomponenten werden simulierte Fehlerwerte eingespeist.

tromagnetische Störung) auftritt? Systematische Analysen ermöglichen dann Tests an sehr komplexen Kombinationen unterschiedlicher Fehlerquellen, welche in einer nicht-modellbasierten Umgebung nur schwer möglich wären. Auch hier zeigt sich der Vorteil einer Kombination von real existierenden und modellbasierten Komponenten: Während bei einer klassischen Herangehensweise ohne modellbasierte Komponenten die Reaktion auf Fehler erst nach der Entwicklung aller Systemkomponenten verifiziert werden kann, ist es so möglich, bereits vor der Implementierung Fehlerszenarien aufzustellen und diese nachher in jeder einzelnen Komponente sukzessive zu testen. Dadurch werden zusätzliche Iterationsschleifen vermieden, das Produkt schneller entwickelt und im Ergebnis sogar sicherer. Ein sehr breites Feld von Fehlerkombinationen kann frühzeitig simuliert und im Endgerät mit der gleichen Anordnung getestet werden.

Ausblick

Was für eine solche Herangehensweise allerdings noch vertieft untersucht werden muss, sind Fehlermodi in den Modellen bzw. den realen Komponenten. Rosas hat solche Fehlermodelle in jüngster Vergangenheit modelliert sowie durch Messungen parametrisiert. Aus diesen Messungen können nun die dynamischen Ausfallmodelle für ganze Baugruppen berechnet werden, die dann in die realen Komponenten eingespeist werden. Dies ermöglicht eine vollständige Abdeckung aller Ausfallmöglichkeiten und damit den vollständigen Test von komplexen Geräten oder Baugruppen.

Die modellbasierte Entwicklungsmethodologie unter Einbezug von Fehler- bzw. Ausfallmodellen wird in den nächsten Jahren enorm an Bedeutung gewinnen. Insbesondere die Kombination von modellbasierten und realen Komponenten bietet gute Möglichkeiten, Systeme zu entwickeln, welche zuverlässig und sicher arbeiten und damit Mensch und Umwelt schützen.

Résumé

Une détection précoce des erreurs de conception

La modélisation de défaillances dans la conception virtuelle de produits

La conception à base de modèles est utilisée depuis de nombreuses années déjà dans les domaines de l'industrie électronique et logicielle. Par exemple, des modèles assistés par ordinateur pour la conception de circuits tels que Spice sont utilisés depuis les années 1970. Dans le domaine de l'ingénierie des systèmes, cette évolution est certes apparue un peu plus tard pour les branches telles que l'aérospatiale, l'automatisation ou les dispositifs médicaux, mais elle s'infiltre ici aussi dans plus en plus de secteurs.

Les atouts présentés par la détection précoce d'erreurs de conception sont considérables. La combinaison de composants existants réellement et de composants basés sur des modèles offre par exemple l'avantage de pouvoir établir des scénarios de défaillance avant la mise en œuvre et de les tester ensuite successivement sur chaque composant. Ce processus permet à la fois d'éviter des boucles d'itération supplémentaires, de concevoir le produit plus rapidement et même avec un résultat plus sûr. Sans composants basés sur des modèles, il n'est possible de vérifier la réaction aux erreurs qu'après la conception de tous les composants du système.

No

Electrosuisse / ITG-Kommentar

Die Chancen von Modellen und Simulationen

Der Artikel vermittelt einen guten Einblick in die modellbasierte Produktentwicklung, wobei moderne Konzepte wie Hardware-in-the-Loop (HIL) oder Processor-in-the-Loop (PIL) zur Sprache kommen. Die Kombination von Simulationsmodellen und realen Baugruppen wird anschaulich skizziert und die daraus resultierenden Chancen bei der Entwicklung von Systemen mit hohen Anforderungen an die funktionale Sicherheit herausgearbeitet.

Die Autoren weisen mit Recht auf die Bedeutung der Echtzeitfähigkeit solcher Simulationssysteme hin und führen in diesem Zusammenhang die Datenverarbeitung mittels FPGA an. Interessant wäre an dieser Stelle eine quantitative Aussage, bis zu welchen maximalen Signal-Abtastraten bzw. minimaler zeitlicher Auflösung entsprechende Systeme typischer Weise betrieben werden können (Zitat: «FPGAs sind meist auch schnell genug»). Daraus wiederum liessen sich Schlussfolgerungen bezüglich der Applikationen ziehen, welche mit dieser Methodik gegenwärtig bearbeitet werden können.

Prof. Dr. **Jürgen Wassner,** Dozent an der Hochschule Luzern.

Referenzen

[1] Frank Poppen, «Holodeck auf der Spur», Gründe für die Virtualisierung eingebetteter Systeme, IX Developer 2/2014 – Embedded Software.

[2] Wolfram Luithardt, «Robustheit für die Industrie», Swiss Engineering, STZ, Vol. 111, September 2014, No. 9, 27–28.

Autoren

Alexander Wille ist wissenschaftlicher Mitarbeiter am Robust und Safe Systems Centre Freiburg (Rosas).

HES-SO/FR, 1705 Freiburg, alexander.wille@hefr.ch

Wolfram Luithardt ist Professor für Embedded Systems und Zuverlässigkeitstechnik an der Hochschule für Technik und Architektur Freiburg.

wolfram.luithardt@hefr.ch

Wolfgang Berns ist Professor an der Hochschule für Technik und Architektur Freiburg und Direktor des Rosas-Zentrums.

wolfgang.berns@hefr.ch