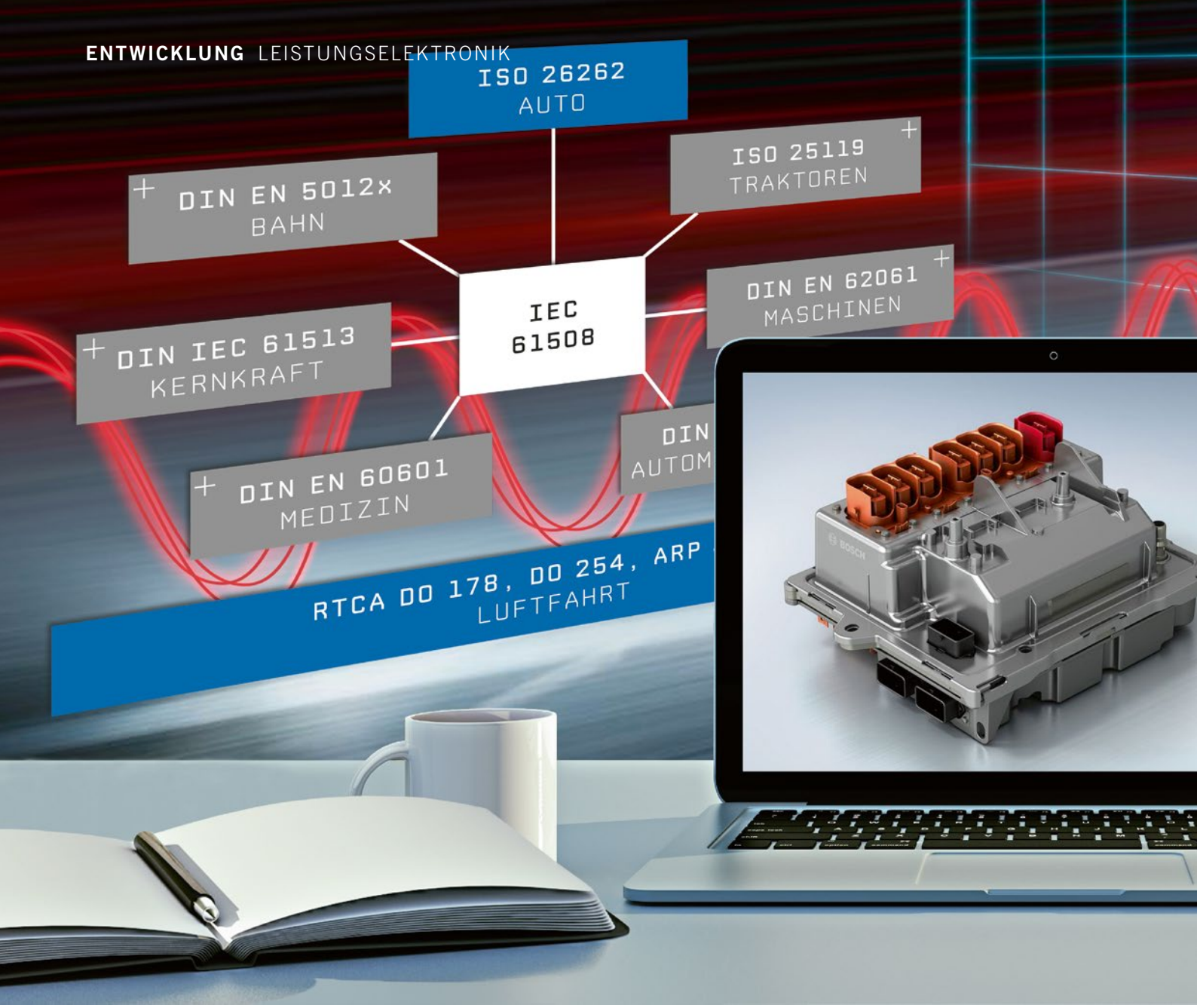

AUTOREN

Dipl.-Ing. (FH) Martin Heininger
ist Inhaber von Heicon
in Schwendi bei Ulm.

Dipl.-Ing. (FH) Horst Hammerer
ist Geschäftsführer der
SET Power Systems GmbH
in Wangen/Allgäu.

VON DER LUFTFAHRT LERNEN

Die Automobilindustrie hat eine „Funktionale Sicherheit“ erst 2011 mit der ISO 26262 eingeführt. In der Luftfahrtindustrie ist die Methodik hingegen schon seit Jahrzehnten etabliert, ohne dass sie den Begriff geprägt hätte. Vor allem Anforderungen an die Software(SW)-Entwicklung haben in der Luftfahrtindustrie eine lange Historie. Bereits 1982 erschien die erste Fassung der RTCA DO 178, einer Richtlinie zur Zertifizierung von Avionik-Software. Die ARP 4754, eine Norm für die Entwicklung ziviler Luftfahrtsysteme, wurde 1996 veröffentlicht. Beide Standards prägen bis heute die System- und Softwareentwicklung in der Luftfahrt. Die enorme Erfahrung im Umgang mit System- und Software-Entwicklungsprozessen sowie den zugehörigen Testprozessen ist von großem Interesse für die Automobilindustrie. Die ISO 26262 und die RTCA DO178/ARP4754 weisen viele gemeinsame Vorgehensweisen auf.

DIE NORMENWELT

Ziel der funktionalen Sicherheit ist, dass von dem komplexen Gesamtprodukt Auto durch elektrische oder elektronische Systeme (E/E-Systeme) keine Gefahr für Mensch und Umwelt ausgeht. Dies ist auch ein wichtiger Beitrag zur von der Automobilindustrie postulierten „Vision Zero“, also der möglichst voll-

© Bosch, SET Power Systems

Leistungselektronik nach ISO 26262 prüfen

Im Automobil übernimmt Leistungselektronik häufig wichtige Aufgaben in sicherheitsrelevanten Applikationen wie Servolenkung, Bremsen oder elektrischen Antriebssträngen. Die Anforderungen für die funktionale Sicherheit sind in der ISO 26262 festgelegt. Um sie besser zu verstehen, hilft ein Vergleich mit den schon lange etablierten Entwicklungs- und Prüfmethoden in der Luftfahrtindustrie. Das Beratungsunternehmen Heicon vergleicht in diesem Artikel die Testprinzipien der Automobilindustrie mit denen der Luftfahrt. Anhand der E-Maschinen-Emulatoren von SET Power Systems wird gezeigt, wie sich diese Prinzipien bei der Prüfung von E-Motor-Steuergeräten praktisch umsetzen lassen.

ständigen Vermeidung von Unfällen. Die Norm gliedert sich in zehn Teile. Sie beschreiben die Anforderungen an die E/E-Systeme des Automobils in ihrer Gesamtheit. Darüber hinaus beschreibt die Norm Anforderungen an den gesamten Produktlebenszyklus. So beschäftigt sich der dritte Teil beispielsweise mit der sehr frühen Konzeptphase eines Produkts. Teil 7 behandelt die Produktion, den operationellen Betrieb (inklusive Reparatur und Instandhaltung) sowie die Außerbetriebnahme.

Die Teile 4 bis 6 widmen sich dem Entwicklungsprozess des Produkts. **BILD 1** zeigt die Struktur der Norm ISO 26262. Sie berücksichtigt schon in ihrem Aufbau mindestens zwei Ebenen der Entwicklung. Über der Software- (Teil 6) und Hardware-Ebene (Teil 5) liegt die Systemebene (Teil 4). Ein klassisches System ist beispielsweise ein elektrischer Antriebsregler. Diese Leistungselektronik-Komponente ist im Fahrzeug Bestandteil eines größeren Systems wie dem elektrischen Antriebsstrang. Dieser wiederum bildet ein Teilsystem des gesamten Fahrzeugs. Ein Auto besteht also aus unterschiedlichen Teilsystemen auf mehreren Ebenen.

In der ISO 26262 (Teil 1) ist der Begriff „System“ wie folgt definiert: „A system is a set of elements that relates at least a sensor, a controller and an actuator with one another.” (Note 1: The related sensor or actuator can be included in the system, or can be external to the system, Note 2: An element of a system can also be another system.)

Obwohl sich die funktionale Sicherheit auf die Gefahren, die sich aus dem Endprodukt ergeben, konzentriert, definiert die Norm mehrere Ebenen. Auf jeder Ebene sind Tätigkeiten und Arbeitsprodukte definiert, die durchzuführen sind und erstellt werden müssen. Dieses Zerlegen dient dazu, die Systemkomplexität zu beherrschen. Die Summe der funktional sicheren Einzelteile führt zu einem insgesamt funktional sicheren Gesamtsystem. Dieser umfassenden Betrachtung entsprechen in der Luftfahrt die Normen RTCA DO254 (Hardware), RTCA DO178 (Software) und ARP4754 (System).

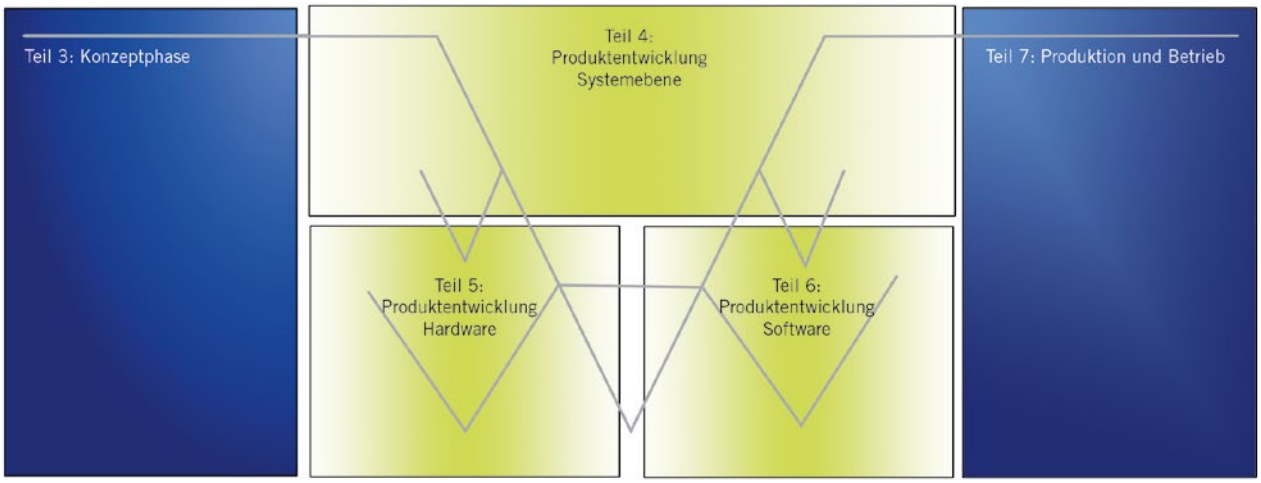

BILD 1 Struktur der ISO 26262 mit möglichen Verifikationsprozessen nach dem V-Modell

FRÜHE, EINFACHE VERIFIKATION

In der Luftfahrt ist die Verifikation eines Gesamtsystems auf verschiedenen Ebenen seit langer Zeit etabliert und bewährt. Die Vorteile sind offensichtlich: Durch die Unterteilung in verschiedene Ebenen kann schon früh im Entwicklungszyklus mit der Verifikation begonnen werden. Die Fehlersuche ist auf niedrigen Ebenen deutlich weniger aufwendig, als auf der Ebene des Gesamtsystems wie dem Flugzeug oder dem Fahrzeug.

Am Beispiel der Verifikation eines klassischen Steuergeräts betrachten wir schwerpunktmäßig die System- und Softwareverifikation. **BILD 2** zeigt die anhand des V-Modells zu verifizierenden, in der ISO 26262 definierten Ebenen. Reale Hardware steht anfangs oft nur eingeschränkt oder gar nicht zur Verfügung, beispielsweise der Elektromotor bei elektrischen Antriebssträngen. Das hat Rückwirkungen auf die Verifikation des Umrichters. Solche wechselseitigen Abhängigkeiten führen schnell zu Problemen in der Verifikationsschleife, wichtige Erkenntnisse gewinnt man erst sehr spät.

Solche Schwierigkeiten lassen sich durch konsequente Verifikation auf den verschiedenen Ebenen gut vermeiden. Es ermöglicht außerdem eine weitere Parallelisierung von Hardware- und Software-Entwicklung. Darüber hinaus kann die Robustheit der einzelnen Elemente der Software vergleichsweise einfach getestet werden. Die Stimulation selbst extremer Szenarien ist auf Software-Integrations- oder Software-Unit-Ebene deutlich weniger aufwendig als beispielsweise auf Fahrzeugebene. Viele Szenarien, die auf unteren Ebenen simuliert werden können, lassen sich auf Fahrzeugebene gar nicht mehr testen. Der Erfolg einer solchen Verifikationsstrategie hängt von zwei wichtigen Voraussetzungen ab: Die eingesetzten Testumgebungen selbst müssen fehlerfrei sein und die Testumgebungen die realen Einsatzbedingungen widerspiegeln. Auf höheren Integrationsebenen sind zudem umfangreichere Simulationen und Emulationen notwendig.

In der Luftfahrt gibt es für den Einsatz solcher Testumgebungen folgende bewährte Prinzipien:

- Bei Software-Unit-Tests verwendet man die Original-Compiler mit zum operationellen Betrieb identischen Einstellungen. Das setzt allerdings voraus, dass die Compilerhersteller Simulatoren oder gegebenenfalls Emulatoren liefern, um die Tests auf einem Host-PC zu ermöglichen.
- Es muss jederzeit plausibel gemacht werden können, dass eine verwendete Testumgebung den realen Anforderungen entspricht. Insbesondere muss eine Nachweisstrategie entwickelt werden, dass die Simulation korrekt ist und sie die realen Bedingungen ausreichend gut abbildet. Da ein Tool nicht „allgemein“ qualifiziert werden kann, ist hierfür eine Toolqualifikation erforderlich, welche die Besonderheiten jeder Testumgebung bei der Qualifikation berücksichtigt. Der Aufwand hierfür hält sich jedoch in Grenzen, da übli-

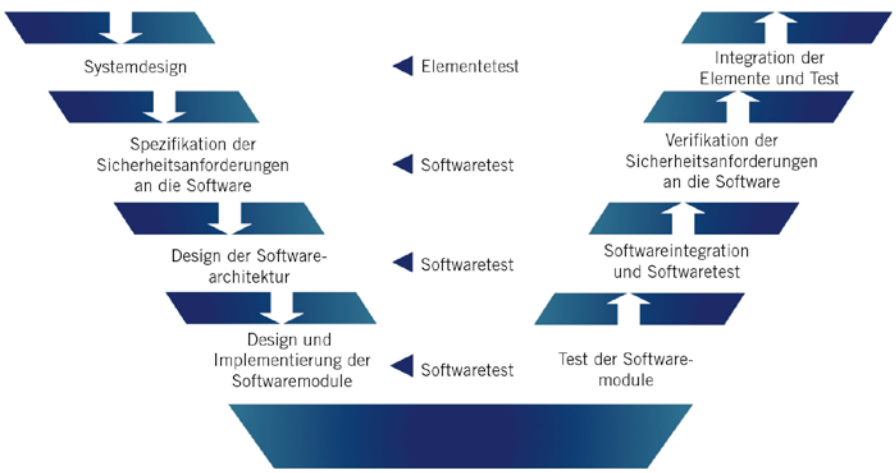

BILD 2 Vorbild Luftfahrt: Durch Unterteilen in verschiedene Ebenen kann ein Gesamtsystem bereits in einem frühen Entwicklungsstadium auf funktionale Sicherheit getestet werden

cherweise vorgefertigte Tests verfügbar sind. Diese müssen dann „nur“ im jeweiligen Projekt wiederholt werden.

– Der Prüfling darf nicht verändert werden. Dieser Punkt ist äußerst wichtig. Der Umfang des Prüflings hängt naturgemäß von der Testebene ab. Bei Software-Unit-Tests kann der Prüfling im Extremfall aus einer einzigen Software-Funktion bestehen. Diese Funktion, die dann als Prüfling definiert ist, darf keinesfalls verändert werden. Das gilt auch für höhere Testebenen. So bedeutet dies beispielsweise auf der Systemebene eines Antriebsumrichters, dass die Tests mit einem Originalgerät, bestehend aus Hardware und Software, durchgeführt werden. Jegliche Abweichung von der Version, die später im Auto verbaut wird, bedeutet ein Risiko für die Aussagekraft der Tests und damit für die funktionale Sicherheit.

VERIFIKATION AUF SW-INTEGRATIONS-UND UNIT-EBENE

Für die Software-Unit-Ebene und Software-Integrationsebene ergibt sich der große Vorteil, dass keine Hardware benötigt wird. Sogenannte Testtreiber beziehungsweise Stubs simulieren die Schnittstellen zur Hardware, um eine lauffähige

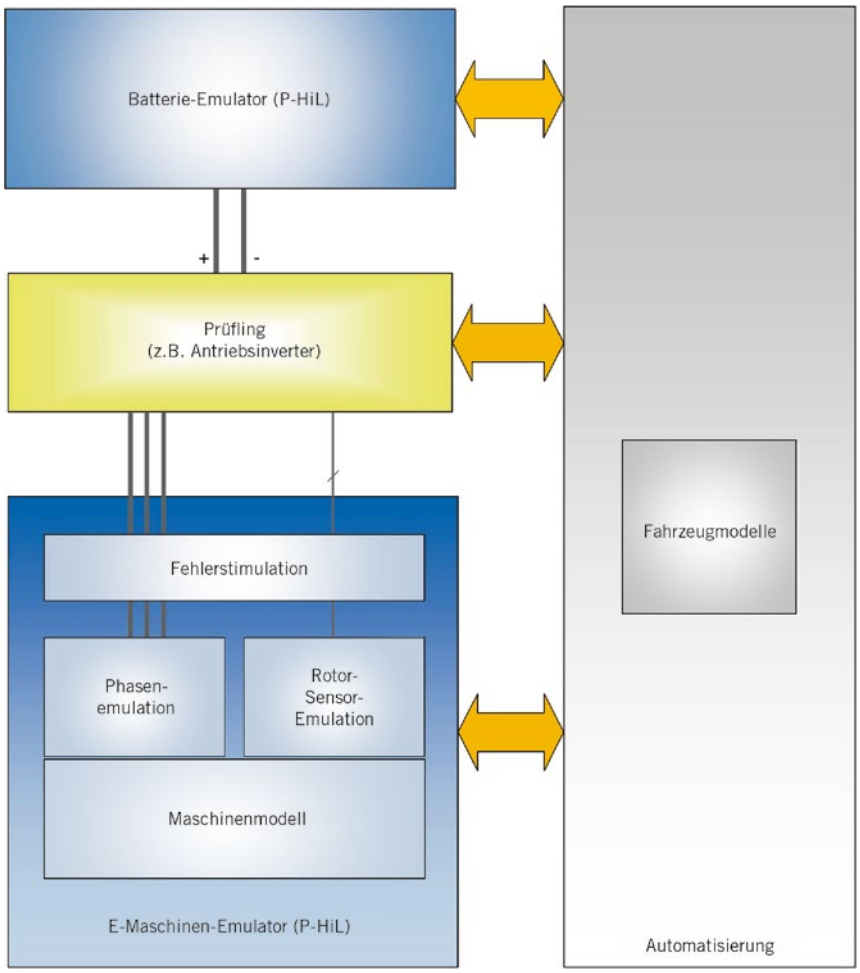

BILD 3 Test-Topologie mit einem E-Maschinen-Emulator

BILD 4 E-Motoremulator zur Entwicklung und Prüfung, unter anderem von Steuergeräten für Lenkantriebssysteme, Parkbremsen, Turbolader- und Pumpenantrieben

Softwareeinheit zu erhalten. Dies hat Kosten- und Zeitvorteile. Insbesondere Funktionalität und Logik der Software lassen sich dadurch schon frühzeitig im Projekt überprüfen. Fehler werden schnell gefunden, da nur wenige Softwaremodule als Ursache infrage kommen. Auf Systemebene ist die Fehlerursache hingegen oft schwierig und mit großem Aufwand verbunden: Das beginnt schon mit der Frage, ob es sich um einen Hardware- oder Softwarefehler handelt? Denkbar sind aber auch Folgefehler, bei denen die eigentliche Fehlerursache oft sehr weit von der Fehlerwirkung entfernt ist. Ein weiterer Vorteil des Prüfens auf Softwareebene: Die Robustheit jedes einzelnen Software-Moduls kann leicht festgestellt werden, da sich extreme und außergewöhnliche Szenarien dank der Testtreiber sehr einfach simulieren lassen. Als Testumgebung reichen meist der Compiler und ein professionelles Testtool, das die Generierung von Testtreibern unterstützt und automatisiert. Testumgebungen für Verifikationen auf höheren Ebenen sind im Vergleich deutlich aufwendiger und komplexer.

VERIFIKATION AUF INTEGRATIONS- UND SYSTEMEBENE

Auf Hardware/Software-Integrationsebene oder Systemebene sind oft komplexe Simulationen oder Emulationen notwendig, um trotz einer Teilintegration möglichst reale Umgebungsbedingungen garantieren zu können. Elektromotorische Aktuatoren, wie sie heute in Servolenkungen, Bremsverstärkern oder ganzen elektrischen Antriebssträngen zum Einsatz kommen, sind mit Steuergeräten ausgestattet. Prüfen lassen sie sich mithilfe von E-Maschinen-Emulatoren, **BILD 3**. Diese Test-Topologie erlaubt es zum Beispiel, die Komponente „Antriebsumrichter“ getrennt von der Komponente „E-Maschine“ zu verifizieren. Die Vorteile liegen auf der Hand: kleinere Komplexität, da nur die Elektronikkomponente selbst geprüft werden muss, und Entkoppelung der gegenseitigen Abhängigkeiten im Projektplan. Hinzu kommt: Meist ist es nicht möglich, typische Fehlerfälle eines Elektromotors direkt durch den Motor darzustellen. Anders bei einer E-Maschinen-Emulation: Phasenfehler, Fehler im Rotorsensor, Justagefehler, Toleranzen der Maschine etc. können einfach stimuliert werden.

Die im **BILD 3** gezeigte Anordnung ist ein sogenannter Power-Hardware-in-the-Loop(PHIL)-Aufbau. Gegenüber herkömmlichen HIL-Anordnungen auf Kleinsignalebene bietet der Einsatz eines Emulators für Leistungssteuergeräte deutliche Vorteile. Der Prüfling wird nicht manipuliert. Auch die Leistungspfade werden nicht abgeschaltet und durch Modelle ersetzt, sondern bleiben real vorhanden. Der Prüfling befindet sich also im „Original“-Zustand – eine der wichtigsten Voraussetzungen für eine aussagekräftige Qualifikation.

Ein solcher Systemaufbau kann auch die im realen Fahrbetrieb an einem Antriebsumrichter auftretenden Last- und Umgebungsbedingungen exakt reproduzieren und so im Labor nachbilden. Der Wegfall des realen Motors bringt nicht nur bessere Testmöglichkeiten und eine Trennung der Testaufgaben, sondern „holt“ die Testumgebung quasi ins Labor. Da der Motor nur „virtuell“ existiert, gibt es keine drehenden Teile oder Lastmaschinen – ein wichtiger Aspekt! Trotzdem kann der Prüfling unter voller elektrischer Leistung in allen normalen und auch abnormalen Betriebspunkten getestet werden. Je nach Applikation und Leistungsklasse bietet SET Power Systems die entsprechenden E-Maschinen-Emulatoren: von Niedervolt-Geräten, mit denen typischerweise Servolenkungs-Motoren, kleine Pumpen oder sonstige Hilfsaggregate emuliert werden, **BILD 4**, bis zu Hochleistungsemulatoren, die beispielsweise elektrische Antriebsmotoren mit weit über 1.000 A Phasenstrom emulieren.

Mit diesen Möglichkeiten der Verifikation können unter anderem folgende Forderungen des Teils 4 (Produktentwicklung auf Systemebene) der ISO 26262 umfassend erfüllt werden:

- Kapitel 7.4.8: (Item-Integration und Test): System Design Verifikation, (Methode: Simulation, mit deren Hilfe die Reaktion des zu testenden Systems auf Fehler getestet werden kann)
- Kapitel 8.4.2 und 8.4.3 (Hardware/Software- und System-Integrationstests): korrekte Implementierung von technischen Safety Requirements (Methode: Fault injection test und Requirements-based test); Robustness verifikation (Methode: Stress test); Effektivität der Safety-Mechanismen für die Hardwarefehler-Diagnose-Abdeckung (Methode: Fault injection test).

FAZIT

Die Gefahren, die von E/E-Systemen auf Fahrzeugebene ausgehen können, stehen im Mittelpunkt der Betrachtungen zur funktionalen Sicherheit nach ISO 26262. Die Norm fordert auf verschiedenen Systemebenen konstruktive und verifizierende Maßnahmen, um eine möglichst fehlerfreie und robuste Funktion der E/E-Systeme auf Fahrzeugebene zu erreichen. Sie folgt damit jahrzehntelang bewährten Methoden aus der Luftfahrtindustrie. Auf allen Ebenen der Verifikation, die oberhalb der Software-Integrations- oder -Unit-Ebene liegen, sind meist komplexe Testumgebungen notwendig. Realitätsnahe, genaue und korrekte Simulationen bilden eine Schlüsselfunktion. Für Systeme, die Elektromotoren steuern, stehen leistungsfähige E-Maschinen-Emulatoren von SET Power Systems zur Verfügung, die auch komplexe Verifikationsanforderungen der ISO 26262 für alle ASIL-Level abdecken. Diese ermöglichen beim Integrationstest den Einsatz des unveränderten Prüflings sowie eine realitätsnahe Testumgebung. Die Luftfahrtprinzipien „Originalität des Prüflings“ und „belastbare, funktional aussagekräftige Tests auch auf Integrationsebene“ können damit auch in der Automobilindustrie mit wenig Aufwand angewendet werden.