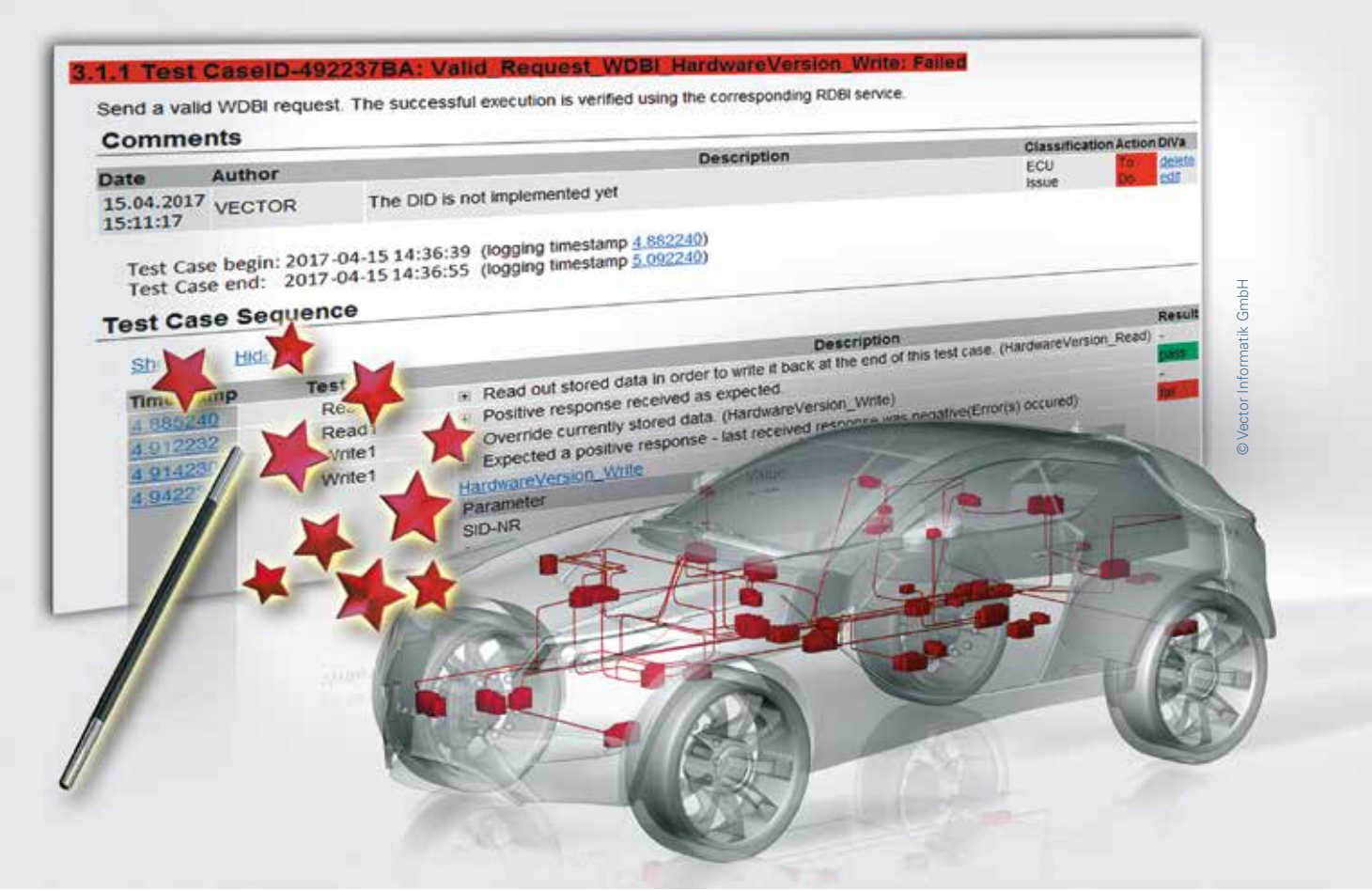

Automatische Diagnose-validierung ist kein Hexenwerk

Der Diagnoseumfang von Steuergeräten und die Anforderungen an die Qualität werden weiter wachsen. Jedoch existieren schon heute automatisierte Lösungen, die die Aufwände für die Diagnosevalidierung signifikant reduzieren und gleichzeitig die Testbreite und -tiefe signifikant erhöhen.

Häufig beginnen Fachartikel über die Diagnosevalidierung wie folgt: Mit zunehmender Komplexität der Steuergeräte im Fahrzeug wächst auch der Umfang der Diagnose und damit auch der Aufwand für die Diagnosevalidierung. Das damit implizierte lineare Aufwandswachstum gibt es aber – glücklicherweise – dank aktueller Testwerkzeuge so nicht mehr. Tatsächlich können bereits seit vielen Jahren vor allem Diagnoseprotokolltests vollautomatisch generiert und ausgeführt werden. Der Aufwand für die Erstellung und Ausführung von Tests bleibt trotz weiter wachsendem Funktionsumfang eher konstant. Mit den etablierten Standards der einheitlichen Diagnosekommunikation (UDS) und Diagnosebeschreibungsformaten (ODX) kann mit vergleichsweise wenig Aufwand eine hohe Testautomatisierung und folglich eine hohe Diagnosequalität erreicht werden. Aber auch das Testen der Diagnoseapplikation und des Software-Updates ist automatisierbar. Heute gibt es wenige Bereiche in der Entwicklung von Automobilelektronik, die über ein ähnlich hohes Potenzial zur Testautomatisierung verfügen.

Für die Automatisierung der Diagnosetests stellte die Verabschiedung des Unified Diagnostic Services Standards (ISO 14229) [1] im Jahr 2006 einen großen Schritt dar: Mit der

Harmonisierung der Diagnosedienste war erstmals die Umsetzung von herstellerübergreifenden tiefergehenden Diagnoseprotokolltests möglich. Das Vorgängerprotokoll KWP2000 (ISO 14230) [2] erlaubte noch viele Freiheiten und verlangt daher nach OEM-spezifischer Konkretisierung, was eine allgemeingültige Testimplementierung erschwert. Im Jahr 2013 wurde die UDS in einer überarbeiteten Version veröffentlicht, was die Formulierung von noch detaillierteren Protokolltests ermöglicht.

Formale Diagnosebeschreibung

Neben der Protokolldefinition stellen formal beschriebene Diagnosedaten die zweite wichtige Voraussetzung zur Testgenerierung dar. Der Funktionsumfang eines Fensterhebers unterscheidet sich wesentlich von dem eines Motorsteuergerätes – entsprechend unterscheidet sich auch die umgesetzte Diagnosefunktionalität. Um einen Test automatisch generieren zu können, müssen die im Steuergerät umgesetzten Diagnosedienste bekannt sein. Zur Spezifikation der Diagnose ist das Werkzeug CANdelaStudio der Vector Informatik weltweit etabliert. Es unterstützt u. a. den internationalen Standard Open diagnostic data exchange (ODX, ISO 22901) [3], der im Jahr 2008 verabschiedet wurde und mittlerweile bei den meisten Fahrzeugherstellern weltweit zum Einsatz kommt.

Die technischen Voraussetzungen für eine automatische Generierung von Diagnoseprotokolltests sind also bereits lange erfüllt. So verwundert es nicht, dass es auch schon seit über zehn Jahren Lösungen zur automatischen Diagnosetestgenerierung und -ausführung gibt, wie beispielsweise das Werkzeug CANoe.DiVa von Vector. Basierend auf Diagnoseinformation im CANdela oder ODX-Format und dem Diagnoseprotokoll (zum Beispiel UDS, KWP2000, OBD, WWH-OBD, …) werden automatisch sehr umfangreiche Tests generiert. Diese Tests umfassen gültige Anfragen genauso wie ungültige, die die Fehlerbehandlung im Steuergerät auf die Probe stellen. Die Tests werden in die Testumgebung (CANoe) geladen, automatisiert ausgeführt und die Testergebnisse in einem detaillierten Report dokumentiert (Bild 1). Für größere Steuergeräte werden schnell über 10.000 Testfälle generiert, ohne dass redundant getestet wird.

Faktisch gibt es heute für nahezu jedes Steuergerät eine formale Diagnosebeschreibung im CANdela und/oder ODX-Format. Von der Diagnosespezifikation zu einem umfassenden automatischen Protokolltest ist es daher nur ein kleiner Schritt: Protokollfehler können schon lange einfach mit wenig initialem Aufwand erkannt werden.

AUTOSAR steigert die Diagnoseprotokoll-Qualität

Mit dem Einsatz von AUTOSAR-Software-Komponenten für die Diagnose wird eine Reihe von Protokollverletzungen durch den Tester, beispielsweise Formatverletzungen, bereits von der Basissoftware behandelt. Da die Basissoftware in der Regel direkt mit den verfügbaren Diagnosedaten parametriert wird, sind in der Regel auch die Diagnoseantworten eines Steuergeräts protokollkonform. Der Anteil der einfachen Protokollfehler sinkt mit der Verwendung von AUTOSAR-Komponenten erkennbar. Entsprechend sinkt auch der Aufwand für die Testauswertung und die Fehlerbehebung. Trotzdem bleibt der Protokolltest unter anderem aus folgenden Gründen weiter wichtig:

- Bei der Konfiguration der AUTOSAR-Komponenten, der Integration und der Applikationsentwicklung können Fehler passieren.
- Passt die Diagnose-Implementierung im Steuergerät nicht zu den vom Diagnosetester verwendeten Diagnosedaten, kann trotz „korrekter" Umsetzung im Steuergerät nicht richtig diagnostiziert werden.
- Lücken in der Fehlerbehandlung der Anwendungs-Implementierung können potenziell zum Einspielen von Schad-Code verwendet werden.

Da in Zeiten von DoIP und OTA („over the air") keine direkte physikalische Verbindung mit dem Diagnosetester mehr vorliegen muss, kann sich ein Protokollfehler gegebenenfalls negativ auf diese Dienste für eine ganze Flotte von Fahrzeugen auswirken: beispielsweise durch eingeschränkte Möglichkeiten bei der Fernwartung, weil benötigte Diagnosefunktionen nicht wie gewünscht arbeiten und daher (doch) ein Werkstattaufenthalt erforderlich wird. Im schlimmsten Fall könnte ein Protokollfehler einen sicherheitskritischen Angriff auf das Fahrzeug ermöglichen. Durch die ständige Verfügbarkeit des Fahrzeugs werden sich neue, auch auf Diagnosefunktionalität basierende, für den Kunden erlebbare Anwendungsfälle entwickeln, wodurch es voraussichtlich zu einem häufigeren und breiteren Einsatz der Diagnose- »

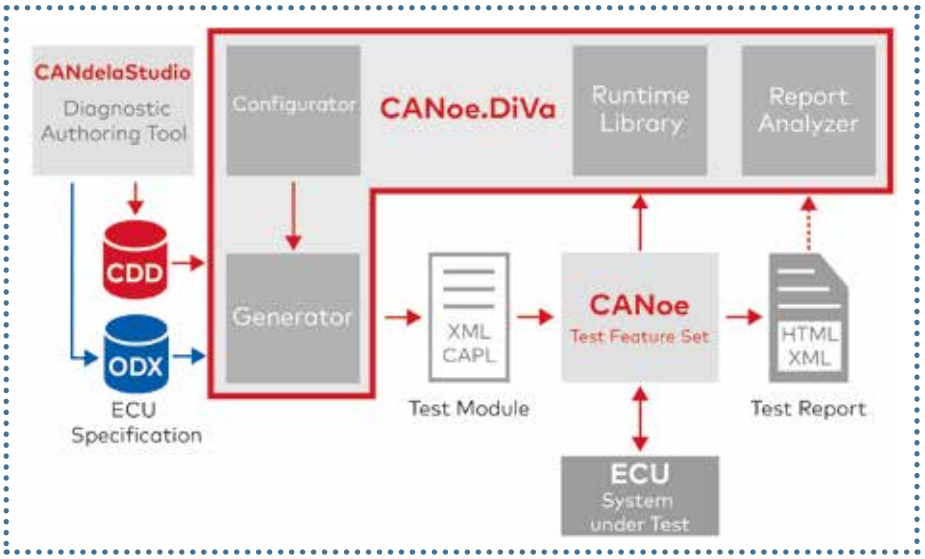

Bild 1: Funktionsbausteine der automatisierten Testumgebung CANoe.DiVa.

(© Vector Informatik GmbH)

funktionen kommt. Entsprechend ist abzusehen, dass die Qualitätsanforderungen an die Diagnoseumsetzung noch weiter wachsen.

Software-Update-Validierung

Trotz aller Diagnose-Standardisierungsmaßnahmen sind die Abläufe für ein Steuergerät-Software-Update (Flashen) weiterhin OEM-spezifisch. Zwar sind die eingesetzten Dienste standardisiert, aber Funktionen wie inkrementelles Update oder Mechanismen zur Absicherung der übertragenen Daten (Identifikationsdaten, Checksummen, Signaturen, etc.) führen in der Praxis zu recht unterschiedlichen Flash-Abläufen. Außerdem werden unterschiedliche Flash-Container-Formate verwendet, um den Prozessanforderungen des jeweiligen Herstellers gerecht zu werden.

In der Praxis bedeutet das, dass es für nahezu jeden OEM ein eigenes Werkzeug zum Software-Update gibt. Ein Zulieferer muss also nicht nur mit verschiedenen Werkzeugen arbeiten, sondern oft auch für jeden OEM eine eigene Testumgebung entwickeln und pflegen. In Produktion und Service ist ein funktionierender Flash-Ablauf seit jeher unverzichtbar. Wenn man an zukünftige Software-Updates „over the air" (SOTA) denkt, so ist eine verlässliche Software-Update-Funktion im Fahrzeug wichtiger denn je. Mit den neuen Möglichkeiten wird neue Software voraussichtlich häufiger eingespielt, möglicherweise ähnlich oft wie man es bereits von mobilen Endgeräten her kennt, zum Beispiel um Sicherheitslücken zu schließen. Situationen, in denen ein Steuergerät nach einem fehlgeschlagenen Update nicht mehr funktioniert, sollen natürlich unbedingt vermieden werden. Aber selbst bei etablierten Herstellern von Smartphones laufen Software-Updates nicht immer reibungslos ab – trotz ausgeklügelter Absicherungsmaßnahmen.

Mit dem Werkzeug vFlash von Vector werden schon seit einigen Jahren herstellerübergreifend Software-Updates durchgeführt, und das für zurzeit über 90 unterschiedliche Bootloader-Spezifikationen aller relevanten Fahrzeughersteller. Das Testautomatisierungswerkzeug CANoe.DiVa nutzt die Automatisierungsschnittstelle von vFlash und bietet so für alle von vFlash unterstützten Bootloader zusätzlich automatisierte Software-Update-Tests an. Neben den Variablen (Timing, Format, ...) im gültigen Flash-Ablauf werden automatisch auch klassische Fehlersituationen, wie etwa Unterspannung und Abbrüche, an verschiedenen Stellen des Flash-Ablaufs getestet. Damit lässt sich die Robustheit der Steuergeräte-Software einfach und umfassend prüfen.

Bei den skizzierten Tests handelt es sich im Wesentlichen um Blackbox-Tests. Darüber hinausgehende Tests, wie etwa die Plausibilisierung prozessrelevanter Daten wie Identifikationsdaten oder Signaturen, erfordern herstellerspezifisches Detailwissen. Auch für diese Art von Tests gibt es bereits spezifische Erweiterungen für namhafte Hersteller.

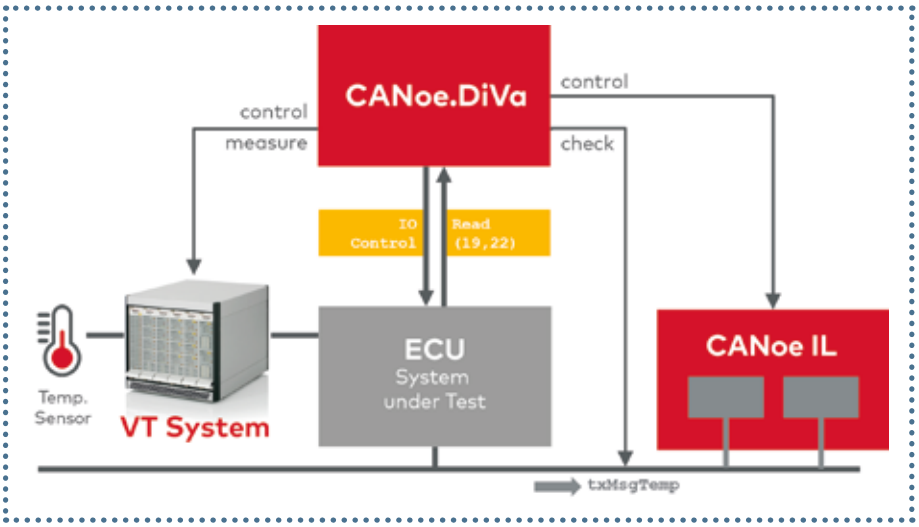

Bild 2: CANoe.DiVa: Software- und Hardware-in-the-Loop. (© Vector Informatik GmbH)

Die Software-Update-Tests sichern die wesentlichen Update-Features wie verlässliche Datenübertragung und robustes Verhalten im Fehlerfall ab. Sie sind ähnlich komfortabel automatisierbar wie die Diagnose-Protokolltests.

Validierung der Diagnoseapplikation

Die Diagnosefunktionen im Steuergerät müssen selbstverständlich nicht nur formalen Aspekten genügen, sondern auch inhaltlich korrekt sein. Nur so kann ein Fahrzeug sinnvoll diagnostiziert werden. Die aktuellen Diagnoseformate, wie beispielsweise ODX, konzentrieren sich vor allem auf die Definition der Protokollaspekte. Trotzdem können daraus applikationsrelevante Informationen für eine automatische Testerzeugung gewonnen werden: beispielsweise lässt sich aus der Beschreibung der definierten Wertebereiche ein automatischer Test zur Plausibilisierung der übertragenen Werte ableiten. Mit heuristischen Methoden und/oder herstellerspezifischem Wissen können aus nicht-formalen Fehlercode- oder Diagnoseparameter-Beschreibungen konkrete Fehlerursachen abgeleitet werden. Um die gewonnen Erkenntnisse in konkrete automatische Testläufe umsetzen zu können, müssen die Zugriffsmöglichkeiten auf die (Test-)Umgebung und damit die Möglichkeiten zur Stimulation des Steuergerätes bekannt sein. Üblicherweise sind diese Informationen bei der Steuergeräteentwicklung aber ohnehin verfügbar:

- Die Netzwerkarchitektur ist beschrieben in AUTOSAR (.arxml) oder CANdb (.dbc). Signale können einfach vom Bus gelesen und über eine Restbussimulation manipuliert werden.
- Das Speicherlayout eines Steuergeräts ist beschrieben in a2l-Dateien. Parameter können einfach über XCP gelesen und manipuliert werden.
- Die elektrischen Ein- und Ausgänge und die Test-Beschaltung sind üblicherweise in maschinenlesbaren Formaten beschrieben. Diese können gemessen und angesteuert werden, wie etwa über einen Hardware-in-the-Loop-(HiL)-Test im Zusammenspiel mit dem VT System von Vector (Bild 2).

CANoe.DiVa unterstützt zusätzlich die Ankopplung von proprietären Parameter- und DTC-Beschreibungen über ein Excel-Austauschformat. In einer integrierten Testumgebung

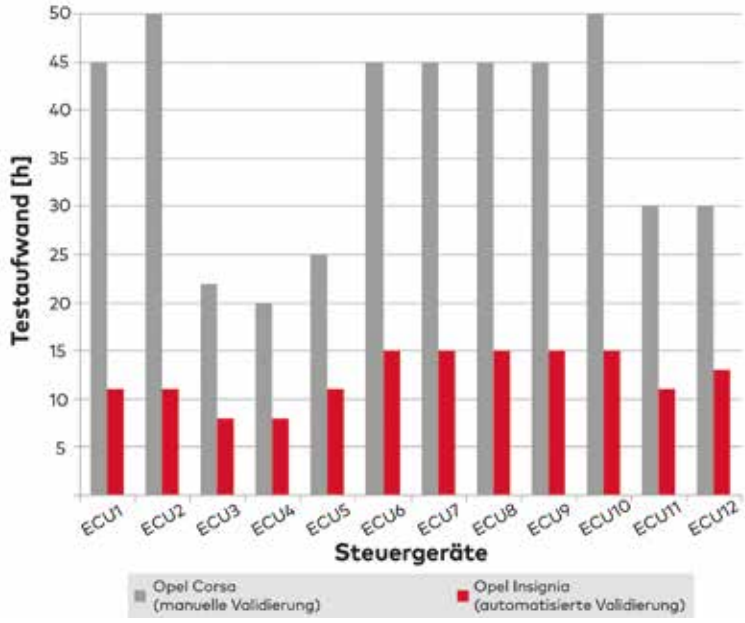

Bild 3: Aus der Praxis: Testaufwand manueller Validierung im Vergleich zur automatisierten Validierung [5]. (© Vector Informatik GmbH)

wie Vector CANoe können all diese Quellen in einem Test kombiniert und genutzt werden.

Beim Einsatz eines virtualisierten Steuergeräts in der Entwicklung, zum Beispiel Vector vVIRTUALtarget, ist der Testaufbau für den Applikationstest vergleichsweise einfach möglich, da Hardware-I/Os einfach per Software stimuliert werden können.

Der mögliche Automatisierungsgrad bei Applikationstests reicht sicher nicht an den der Protokolltests heran, dennoch ergeben sich zahlreiche Möglichkeiten zur halb- oder sogar vollautomatischen Testgenerierung, die es sich zu nutzen lohnt.

Testumfang, Testauswertung und Weiterverarbeitung

Der durch entsprechende Werkzeuge gewonnene hohe Automatisierungsgrad bei der Diagnose-Protokollvalidierung ermöglicht eine höhere Testtiefe – bei gleichbleibendem Aufwand – durch weitere automatisierte Tests oder zusätzliche eigene Tests: Immer mehr OEMs nutzen die Automatisierungsmöglichkeiten, um die für Sie besonderes wichtigen Diagnoseanwendungsfälle, wie zum Beispiel für Produktion und Service, systematisch abzusichern. Entsprechend kann die Diagnosefunktion bereits in frühen Entwicklungsphasen vom Lieferanten nachweisbar abgesichert werden.

Weltweit setzen heute viele der großen OEMs auf die Testunterstützung von CANoe.DiVa. Sie profitieren dabei auch von der umfangreichen Unterstützung bei der Weiterverarbeitung der Testergebnisse, die in Praxis sehr viel Zeit einspart (Bild 3):

- Sortieren und Filtern, für eine gezielte und bedarfsgerechte Sicht auf die Testergebnisse,
- Verknüpfen von Fehlern mit derselben Ursache,
- Kommentieren einzelner Testergebnisse, um den Fehler und seine Ursache zu klassifizieren, Hinweise zur Korrektur zu dokumentieren und die Behebung zu steuern,
- Übertragen der Fehleranalyseergebnisse eines Testlauf auf einen anderen,
- Anbinden der Testlösung an bestehende Testdatenmanagement- oder Anforderungssysteme, zur Integration in existierende Prozesse.

Fazit und Ausblick

Der Diagnoseumfang von Steuergeräten und die Anforderungen an die Qualität werden weiter wachsen. Jedoch existieren schon heute automatisierte Lösungen, die die Aufwände für die Diagnosevalidierung signifikant reduzieren und gleichzeitig die Testbreite und -tiefe signifikant erhöhen. Die dazu benötigten formal beschriebenen Daten sind in der Regel ohnehin verfügbar. Die Wiederverwendung dieser Daten auch für Testzwecke ist nur konsequent.

Mit der zunehmenden Vernetzung über die Fahrzeuggrenzen hinaus gewinnt das Thema Automotive Cyber Security auch in der Diagnose rasant an Sichtbarkeit. „Testen von Security" und „Testen trotz Security" [4] sind in vielen Bereichen der Entwicklung mittlerweile Fokusthemen. Der erweiterte Fahrzeugzugriff „Over The Air" eröffnet neue Anwendungsfelder für die Fahrzeugdiagnose – die wiederum abgesichert werden müssen.

Viele Innovationen lassen sich nur dann schnell in Serie bringen, wenn sie schon frühzeitig und anwendergerecht in Software und den zentralen Werkzeugen unterstützt werden. Auch das ist kein Hexenwerk. Aber eine spannende Herausforderung für Anbieter von Software. ■ (oe)

» www.vector.com

Literaturhinweise:

[1] - [3] International Organization for Standardization: ISO 14229 (UDS), ISO 14230 (KWP2000), ISO 22901 (ODX)

[4] Metzger E.; 2016: Vortrag: Die Vector Security Solution, Vector Cyber Security Symposium 2016

[5] Peti P., Timmerberg A., Pfeffer T., Müller S., Rätz C.; 2008: Automatische Validierung der Diagnoseservices, ATZ elektronik 06I2008

» www.hanser-automotive.de/3259392

Hier finden Sie die Download-Version des Beitrags.

Simon Müller ist bei der Firma Vector Informatik in der Produktlinie Diagnose als Produktmanager verantwortlich für CANoe.DiVa.

Christoph Rätz leitet die Produktlinie Diagnose bei der Firma Vector Informatik.