



© unsplash.com/Denys Nevozhai

MESSEN – TESTEN – DIAGNOSE

Alle reden mit!

Nicht nur, dass sich Fahrzeuge der verschiedenen Hersteller und Marken untereinander verständigen können müssen – mit der Einbeziehung der Infrastruktur in ein V2X-Netzwerk wächst auch die Anzahl der beteiligten Kommunikationsteilnehmer und damit zwangsläufig auch die Zahl von möglichen Fehlerquellen.

Bisher war der Testumfang auf klar definierbare Systemgrenzen beschränkt, die sich aus der Bordnetzarchitektur, den darin eingebetteten Sensoren und den Daten, die letztere liefern, ergeben haben. Restbussimulationen in HiL-Testumgebungen sind deshalb schon seit langem etabliert und Stand der Technik. Mit der V2X-Kommunikation kommen nun jedoch externe Datenquellen ins Spiel, ohne die ein funktionales Testen der V2X-Anwendung gar nicht möglich ist.

Beim Testen von Kommunikationslösungen ist die Konformität und Kompatibilität auf der physikalischen Ebene eine Grundvoraussetzung für eine erfolgreiche Übertragung von Informationen. Sprich: Fragen wie Frequenzstabilität oder Out-of-Band-Emissionen sind auch bei V2X-Testlösungen grundlegende Testumfänge. Allerdings sind sie nur der Anfang von weiterführenden Testverfah-

ren, die für eine erfolgreiche Kommunikation erforderlich sind. Auf Transport- und Protokollebene muss die Konformität gegen die entsprechenden Spezifikationen getestet werden. Bereits an diesem Punkt unterscheiden sich die Testverfahren für V2X-Systeme von anderen Kommunikationsstandards wie etwa WiFi oder Bluetooth.

Beim Datenaustausch über V2X gibt es bei der Kommunikation keinen bidirektionale Datenstrom, der auf dem Prinzip „Anfrage und Antwort“ beruht. Vielmehr verwenden die Teilnehmer in einem V2X-Netzwerk in der Regel Broadcasts (in einigen Fällen auch Multicast oder Unicast), um Informationen auszutauschen. Je nach Nachrichtentyp werden diese Broadcast-Nachrichten entweder periodisch oder bei Eintreten eines definierten Ereignisses (Event) generiert und ausgesendet. Die Datenstruktur der Nachrichten, sprich der Auf-

bau, Feldlängen, Datentypen sowie die gültigen Wertebereiche der einzelnen Datenelemente sind hierbei standardisiert. Wobei an dieser Stelle anzumerken ist, dass es nicht „den Einen“ weltweiten Standard für die Nachrichtenformate gibt, sondern derer verschiedene in den unterschiedlichen Weltregionen wie etwa der EU, den USA oder China.

Basistest auf Konformität mit TTCN-3

Bei der Konformitätsprüfung des Kommunikationsstacks – also der Teil, der für den korrekten Aufbau und den spezifikationskonformen Inhalt einer Nachricht verantwortlich ist – wird üblicherweise auf TTCN-3 als Testsprache gesetzt. Dabei wird der V2X-Softwarestack über eine speziell hierfür implementierte Testschnittstelle mit Test-Daten beschickt und die Ausgabedaten mit dem erwar-

teten Ergebnis oder einem Ergebnis-muster verglichen. Die Prüfung auf Protokoll-Konformität wird schon seit vielen Jahren in der Telekommunikationsbranche verwendet und hat sich bewährt. Mit den entsprechenden Tools wie etwa „Titan“ können diese Tests in TTCN-3 erstellt und ausgeführt werden.

Diese Vorgehensweise ist in sich korrekt und Stand der Technik, sie liefert jedoch nur insofern valide Ergebnisse, als dass der Prüflauf immer nur einen begrenzten Satz von Test-Daten verwendet. Ob sich das „System Under Test“ bei vom Test abweichenden Input-Daten

ebenfalls korrekt verhält, lässt sich anhand dieser Methode nicht feststellen. Der Test auf Konformität mit der zugrundeliegenden Spezifikation beschränkt sich deshalb auf Konformität gegenüber den Testfällen. Letztlich kann über diese Testmethode nur punktuell geprüft werden, ob der Kommunikationsstack die eingehenden Nachrichten entsprechend der Spezifikation verarbeitet und ausgehende Nachrichten korrekt erzeugt. Die auf TTCN-3 basierenden Testverfahren entsprechen damit einer klinischen Stichprobenprüfung auf Konformität. Das Dilemma dabei ist, dass es rein

rechnerisch selbst bei relativ einfach aufgebauten Nachrichtentypen (z.B. DENM) etwa 1040 Wertekombinationen gibt, die der Kommunikationsstack alle korrekt und vor allen Dingen zuverlässig abarbeiten können muss. Das Abtesten sämtlicher Kombinationen ist aufgrund der schieren Menge nicht möglich.

V2X-Lasttests – wie lässt sich die Last erzeugen?

Die Stabilität eines V2X-Systems hängt unter anderem damit zusammen, wie es auf eingehende Nachrichten reagiert. Nachrichten, die der Spezifikation entsprechen, müssen selbstredend sicher und zuverlässig verarbeitet werden. Die Frage, wie robust ein System ist, hängt im Wesentlichen von zwei Faktoren ab: Toleranz gegenüber sogenannten „mal-formed Messages“, also fehlerhaften Nachrichten, sowie das Verhalten bei sehr hoher Last. Die Durchführung von Lasttests im Bereich der V2X-Kommunikation führt schnell zu der Frage, wie eine hohe Last – sprich sehr viele Nachrichten von vielen Netzwerkknoten – erzeugt werden kann. Die naheliegendste Lösung für die Lasterzeugung wäre die Ausrüstung einer ganzen Fahrzeugflotte mit V2X-Sendern für die Testdurchführung. Theoretisch ist dies zwar möglich, der Aufwand hierfür jedoch viel zu groß. Bleibt die Installation und der Betrieb von hunderten V2X-Modems im Labor als Lastquelle? Allein der Anschaffungs- und Installationsaufwand wäre enorm. Der Betrieb auf engem Raum, etwa in einer Testkammer, ist auch angesichts der damit einhergehenden EMV-Probleme nicht ratsam. Ein weiterer Punkt, den es bei Lasttests zu berücksichtigen gilt, sind die verschiedenen Nachrichtentypen. In einem realen Lastszenario, wie es auch auf einer viel befahrenen, mehrspurigen Kreuzung der Fall ist, sind neben einer Vielzahl von CAM- und DENM- bzw. BSM-Nachrichten auch noch SPATEM-, MAPEM oder IVIM-Nachrichten in den Lasttest mit einzubeziehen. Betrachtet man die verkehrliche Situation zum Beispiel in den Großstädten Chinas mit mehrstöckigen Fahrbahnen, wird schnell klar, dass die Anzahl der Nachrichten bis zur Kanalauslastung führen kann. Die Betrachtung unterschiedlicher Nachrichtentypen ist deshalb erforderlich, da der Rechenaufwand »

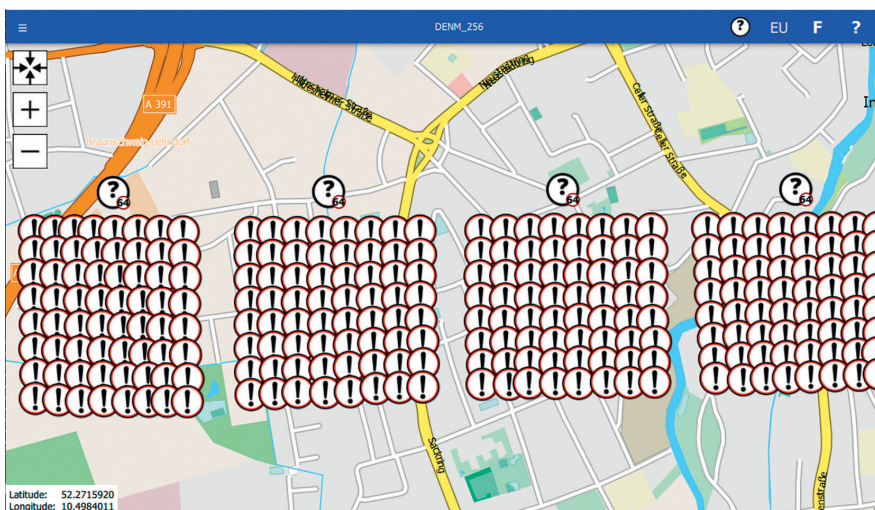


Bild 1: Ein Beispiel für ein Lasttest-Szenario: Vier V2X-Stationen erzeugen insgesamt 256 DENM Nachrichten pro Sekunde. Das Szenario wird in einem Editor erstellt und kann jederzeit reproduziert werden. © Nordsys

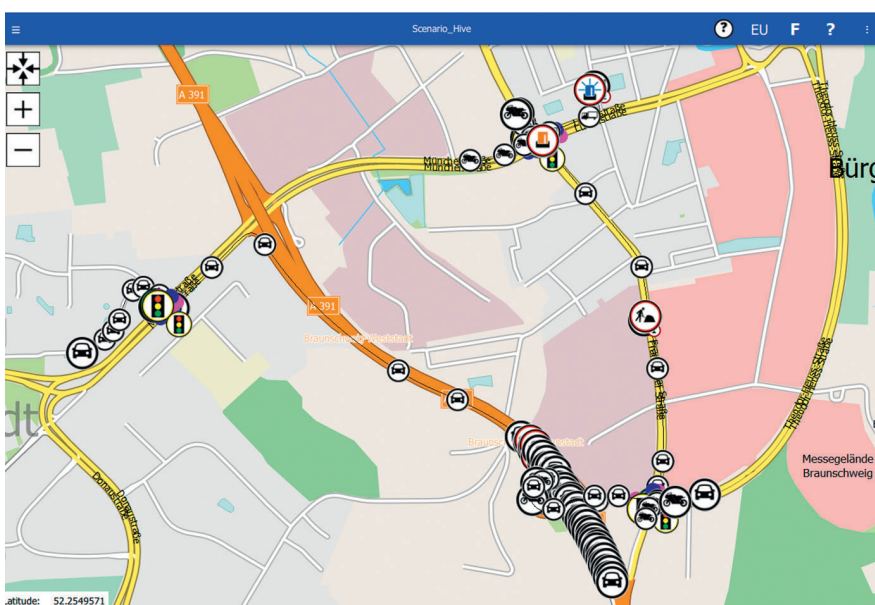


Bild 2: Ein realitätsnahes Verkehrsszenario mit vielen V2X-Netzwerkknoten und verschiedenen Nachrichtentypen, einer Stausituation und Ampeln. Im Laborprüfstand waveBEE hive können solche komplexen Testszenarien geprüft werden.

© Nordsys

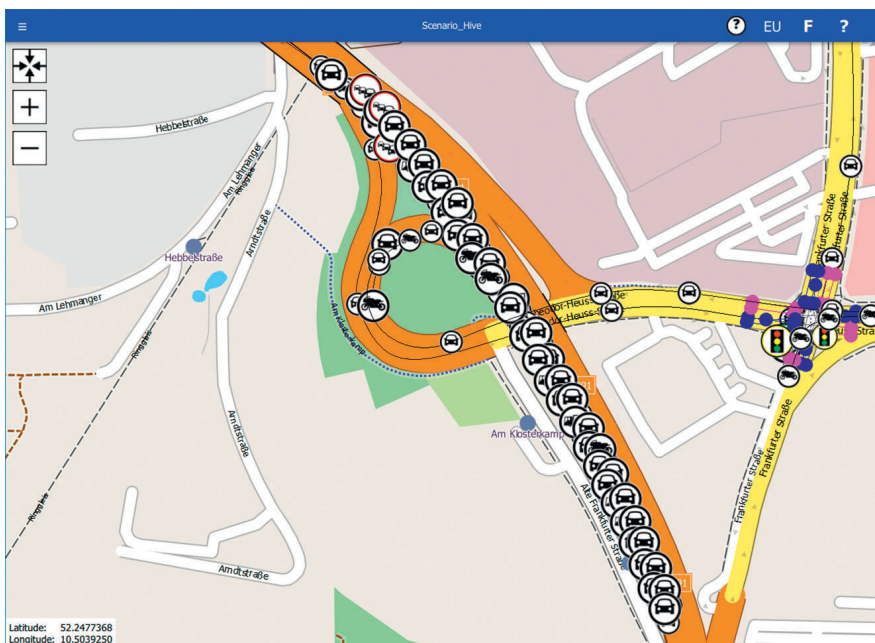


Bild 3: Detailsicht auf eine Stausituation an einer Autobahnabfahrt mit sich anschließender Ampelkreuzung. Die Anzahl der V2X-Netzknoten steigt in einem solchen Fall schnell an und erfordert entsprechende Tests. (© Nordsys)

sich bei den verschiedenen Nachrichtentypen unterscheidet. Ebenso spielen die Sendefrequenz und die Anzahl der Netzknoten bei den Tests eine Rolle.

Das kleine 1x1 der Lastgenerierung

So können beispielsweise 1000 Nachrichten pro Sekunde von 100 Netzknoten bei 10 Hz erzeugt werden, oder aber eben auch von 200 Netzknoten bei 1 Hz. In den beiden skizzierten Fällen werden zwar jeweils 1000 Nachrichten pro Sekunde für den Test herangezogen, die dabei entstehende Last für das zu prüfende System ist jedoch verschieden. Wie bereits erwähnt, spielt es auch eine Rolle, um welche Nachrichtentypen es sich handelt. Da in den derzeit spezifizierten Nachrichten nicht alle Datenelemente verpflichtend mit Werten befüllt sein müssen, lässt auch der Aspekt des tatsächlichen Payloads – also des Nachrichteninhalts – viel Spielraum für noch weiterführende Setups bei der Durchführung von Lasttests. Die derzeit häufig in Lastenheften gestellte Anforderung, „das V2X-System muss x-tausend Nachrichten pro Sekunde verarbeiten können“ greift daher ohne nähere Definitionen nach den oben skizzierten Kriterien viel zu kurz, ist aber in der Praxis weit verbreitet.

Die Teilnahme im V2X-Netzwerk ist im Realbetrieb mittels Zertifikatsketten abgesichert. Gemeinhin wird dies als

„Security“ bezeichnet. Ausgehende Nachrichten werden dabei mit einem über den Nachrichteninhalt gebildeten Hash-Wert signiert. Die Empfängerseite validiert den Hash-Wert und damit die Gültigkeit des auf Senderseite verwendeten Zertifikats. Somit kann der Empfänger die Vertrauenswürdigkeit des Senders und des Nachrichteninhalts feststellen. Das bedeutet, dass alle eingehenden Nachrichten aller Netzwerkteilnehmer entsprechend geprüft werden sollten. Für die Durchführung von Lasttests bedeutet dies, dass sowohl die Validationsgeschwindigkeit von Nachrichten auf Empfängerseite und die Signierungsgeschwindigkeit von Nachrichten auf Senderseite geprüft werden muss. Dabei ist die Anzahl der Nachrichten, die validiert werden müssen, wesentlich größer. Um einen Lasttest korrekt durchzuführen, müssen alle Knoten im Netzwerk mit jeweils eigenen Zertifikaten für das Signieren der Nachrichten ausgestattet sein. Das bedeutet, dass alle eingehenden Nachrichten beim Prüfling mit einer für den Absender spezifischen Signatur versehen sind und jeweils verifiziert werden müssen. Die Verwendung von denselben Zertifikaten für verschiedene Sender führt zu einem wenig aussagekräftigen Testergebnis, da das Verifizieren der mittels der Zertifikate erzeugten Signaturen nicht für jeden Netzknoten separat durchgeführt werden muss, wie dies im realen Betrieb der Fall ist.

Auf die Signaturen kommt es an

Die Durchführung von realitätsnahen Lasttests kann letztlich nur mittels signierter Nachrichten erfolgen. Insofern bietet es sich an, auch das korrekte Signieren und Verifizieren durch den Prüfling im Testsystem mitzuberücksichtigen. Dabei ist zu prüfen, ob der Prüfling korrekte Signaturen aus validen Zertifikaten erzeugt. In der Empfangsrichtung muss das Device und der Test gültige Signaturen erkennen und die Nachrichteninhalte anschließend verarbeiten. Im Fall des Empfangs von nicht signierten oder ungültig signierten Nachrichten muss das System dies zumindest erkennen. Wie mit solchen Nachrichten dann zu verfahren ist, bleibt dem jeweiligen Hersteller überlassen. In der Regel werden ungültig signierte Nachrichten verworfen.

Der Blick auf die Applikationsebene

Für eine funktionierende V2X-Kommunikation ist die Standardisierung der Kommunikation unerlässlich. Naheliegender ist die Standardisierung nach dem OSI-Referenzmodell auf den Schichten 1–5. In Wirklichkeit geht die erforderliche Stan-

INFO

Die Standardisierung auf Applikationsebene, sprich die Beschreibung der Auslösebedingungen und die daraus resultierenden zu sendenden Nachrichteninhalte (Payload), ist beim Car-to-Car-Communication Consortium (C2C-CC) angesiedelt. Da die beschriebene SSVW-Nachricht auch von Infrastrukturkomponenten ausgesendet werden kann, etwa durch die Auslösung aus einer Verkehrsleitzentrale, erfordert die Standardisierung eine enge Abstimmung zwischen der Fahrzeugseite (also dem C2C-CC) und der Infrastrukturseite. Letztere wird durch die europäische ITS-Plattform C-ROADS repräsentiert, welche sich die Harmonisierung von ITS-Diensten und das Deployment in den Mitgliedsstaaten der EU (und darüber hinaus) zum Ziel gemacht hat.

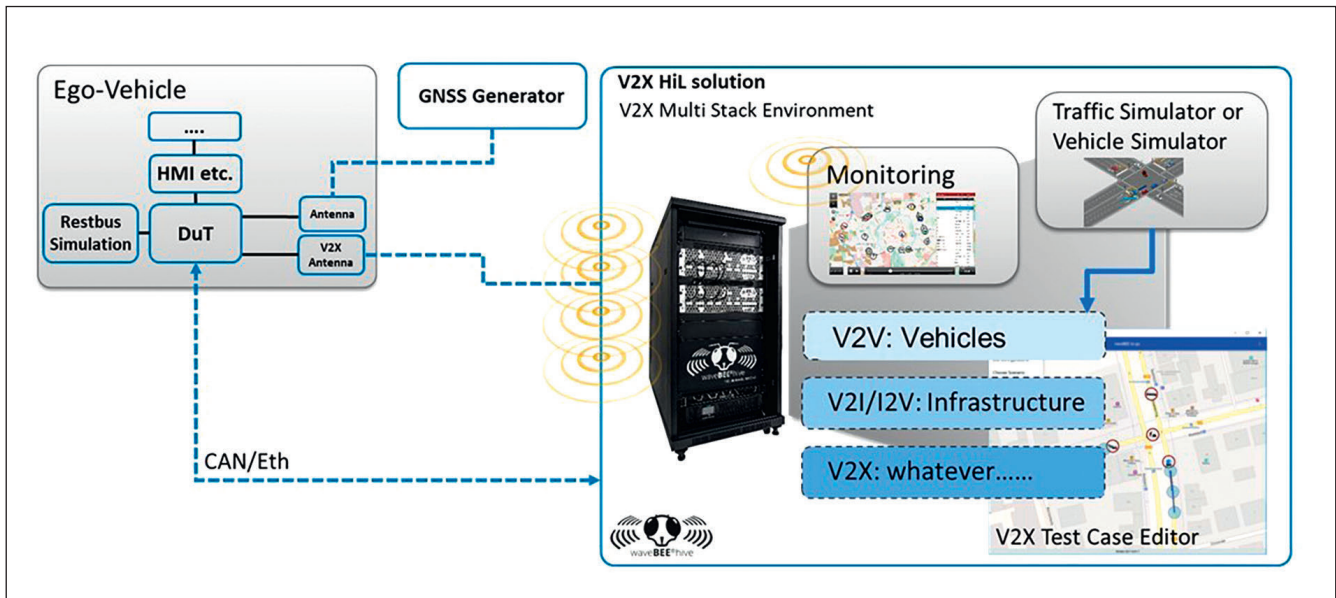


Bild 4: Test-Setup HiL. © Nordsys

dardisierung jedoch noch weiter und umfasst neben allen sieben OSI-Schichten noch zusätzlich die auf Schicht 7 aufsetzende ITS-Anwendungsebene (ITS = Intelligent Transportation Systems). Auf Seite des Empfängers ist die ITS-Anwendungsebene dagegen nicht näher standardisiert. D. h., der Empfänger kann weitgehend selbst entscheiden, ob und wie er die empfangenen Daten verarbeitet.

Ein vereinfachtes Beispiel soll den beschriebenen Sachverhalt verdeutlichen: Die ITS-Anwendung „Slow or Stationary Vehicle Warning (SSVW)“ soll vor langsam fahrenden oder stehenden Fahrzeugen warnen. Hierzu muss unter anderem definiert sein, ab wann ein Fahrzeug als stehendes Hindernis zu betrachten ist und bis zu welcher Geschwindigkeit es als „langsam“ gilt. Die Bedingungen, unter denen dann die entsprechende Warnnachricht in Form einer DENM (Decentralized Environmental Notification Message) erzeugt und gesendet werden darf, sind entsprechend standardisiert. Die DENM selbst muss als Nachricht natürlich auch standardisiert sein.

Das oben beschriebene Szenario erfordert für die funktionalen Tests eine andere Vorgehensweise, als dies bei herkömmlichen, in sich abgeschlossenen Bordnetzen der Fall war: Bestandteil des Testszenarios ist dann nicht mehr die Restbussimulation wie im fahrzeugeigenen Bordnetz, sondern es muss vielmehr eine Restverkehrssimulation

bereit gestellt werden, die zumindest die Nachrichten auf der Luftschnittstelle möglichst realitätsnah abbildet. Eine nähergehende Betrachtung des umgebenden Verkehrs ist meist nicht nötig, denn letztlich sind nur die ausgesendeten Nachrichten für den Test entscheidend.

Fahrzeuge, Ampeln und sonstige Infrastruktur

Externe Daten können von anderen Fahrzeugen stammen (V2V-Kommunikation) oder von der Infrastruktur (I2V-Kommunikation). Insofern ist bei Testlösungen nicht nur der Restbus des eigenen Fahrzeuges (das Ego-Fahrzeug) zu betrachten, sondern insbesondere die Simulation des verkehrlichen Umfelds. In Analogie zum Bordnetz-Restbussimulation kann diese als „Restverkehrssimulation“ auf Ebene der V2X-Nachrichten bezeichnet werden.

Da die Installation von hunderten V2X-Modems kein gangbarer Weg ist, stellt sich die Frage, wie die Tests mit vertretbarem Aufwand überhaupt durchgeführt werden können. Die Erzeugung von Netzwerklast wie auch des Restverkehrs kann in einem V2X-Netzwerk auch über simulierte Netzwerkteilnehmer erfolgen. Eine solche Netzwerksimulation stellt die Testlösung waveBEE hive (hive = Bienenstock) der Nordsys GmbH bereit. Mit lediglich fünf Modems können bis zu 100 Netzknoten vollständig und inklusive Security abgebildet werden, wobei das System nach oben skaliert werden kann.

Die Restverkehrssimulation wie auch Netzknoten für die Lasterzeugung können auf einfache Weise per Mausklick in der im Teststand integrierten Software erzeugt werden. Die auf diese Weise erzeugten Testfälle oder auch komplexe Testszenarien sind zeitlich und räumlich reproduzierbar. Als Option können Verkehrssimulationen an den Teststand angebunden werden, wobei auch hier die Reproduzierbarkeit gegeben ist. Gerade die Reproduzierbarkeit von Testfällen für Regressionstests stellt bei V2X-Nachrichten ein Problem dar. Da die Nachrichten mit Zertifikaten signiert werden und über den Inhalt gehasht wird, reicht ein simples Abspielen von Testdaten nicht aus. Der Test schlägt fehl, weil weder Zeitstempel noch Signaturen vom Device Under Test als gültig eingestuft werden.

Der waveBEE hive unterstützt dabei die Standards in Europa sowie Nordamerika. Eine Anpassung an LTE-V/C-V2X erfolgt bei Bedarf über entsprechende modulare Modemeinschübe. ■ (oe)

www.nordsys.de



Manfred Miller ist geschäftsführender Gesellschafter und Gründer der NORDSYS GmbH. Er und sein Unternehmen beschäftigen sich seit fast 15 Jahren mit der Entwicklung von V2X-Kommunikationslösungen für die Automobilindustrie.