Cybersecurity für Nutzfahrzeuge früh verankern

Artikel vom **7. September 2026**
OHNE_UNTERKATEGORIE

Driventic zeigt, wie Automotive Cybersecurity bei Nutzfahrzeugen von Beginn an in Entwicklung und Betrieb einfließt. Im Fokus stehen UNECE R155, R156 und ISO/SAE 21434, abgesicherte Steuergeräte sowie Unterstützung für OEMs mit begrenzten Ressourcen.

Automotive Cybersecurity: Vier Kompetenzsäulen aus einer Hand (Bild: Driventic GmbH).

Mit den UNECE-Regelungen R155 und R156 sowie der ISO/SAE 21434 sind die Anforderungen an die Cybersecurity moderner Nutzfahrzeuge deutlich gestiegen. Für Fahrzeughersteller und Zulieferer ist Cybersicherheit damit ein fester Bestandteil der Produktentwicklung und in vielen Fällen eine Voraussetzung für die Typgenehmigung von Fahrzeugplattformen. Seit dem Aufbau eines eigenen Cybersecurity-Teams im Jahr 2022 arbeitet das Unternehmen daran, entsprechende Anforderungen systematisch in Produkte und Lösungen zu integrieren. Dabei fließen Erfahrungen aus der Entwicklung von Steuergeräten und Antriebssystemen für Nutzfahrzeuge ein. Ziel ist es, Cybersecurity nicht nachträglich zu ergänzen, sondern bereits ab der Konzeptphase mitzudenken. **Cybersecurity über den Lebenszyklus** Die Entwicklung von Steuergeräten orientiert sich an den Anforderungen der ISO/SAE 21434. Dadurch

werden relevante Cybersecurity-Aspekte in den Entwicklungsprozess eingebunden und sicherheitsrelevante Entscheidungen nachvollziehbar dokumentiert. Der Ansatz reicht von der ersten Konzeptidee über Entwicklung, Serienproduktion und Betrieb bis zur Stilllegung des Nutzfahrzeugs. Zu den Anwendungen zählen die elektrischen Antriebssysteme »VEDS 1.5« und »VEDS 2.2« sowie das Automatikgetriebe »DIWA NXT«. Cybersecurity ist hier Bestandteil der Produktentwicklung und betrifft sowohl Hardware- als auch Softwareebene. **Vier Kompetenzsäulen** Das Leistungsportfolio im Bereich Automotive Cybersecurity gliedert sich in vier Bereiche. Beim Cybersecurity Engineering werden Anforderungen, Risikoanalysen und die Dokumentation sicherheitsrelevanter Entscheidungen strukturiert in Entwicklungsabläufe eingebunden. In der Cybersecurity Analysis dienen Threat Analysis and Risk Assessments dazu, mögliche Bedrohungen zu identifizieren und passende Schutzmaßnahmen abzuleiten. Ein weiterer Schwerpunkt ist die Security-by-Design-Entwicklung. Cybersecurity-Anforderungen werden dabei schon während der Hard- und Softwareentwicklung berücksichtigt. Genannt werden unter anderem Secure Flash, Secure Diagnostic, kryptografische Algorithmen und die Absicherung der Hardware. Hinzu kommt die Unterstützung bei regulatorischen Anforderungen, insbesondere bei der Umsetzung von Vorgaben für Nutzfahrzeugarchitekturen, Steuergeräte und Antriebssysteme. **Unterstützung für kleinere OEMs** Besonders kleine und mittlere Nutzfahrzeughersteller müssen umfangreiche Cybersecurity-Anforderungen häufig mit begrenzten eigenen Ressourcen erfüllen. Hier setzt die Unterstützung bei Entwicklungsprojekten an: Anforderungen werden in bestehende Fahrzeugarchitekturen integriert, ohne den Blick auf die praktische Fahrzeugintegration zu verlieren. Das betrifft die Umsetzung auf Hardware- und Softwareebene ebenso wie die Dokumentation für regulatorische Nachweise. Weitere Informationen zu Automotive Cybersecurity und zu Innovationen aus dem Portfolio werden vom **14. bis 20. September** auf der IAA Transportation 2026 in Hannover, Halle 11, Stand B06, gezeigt.

Hersteller aus dieser Kategorie
