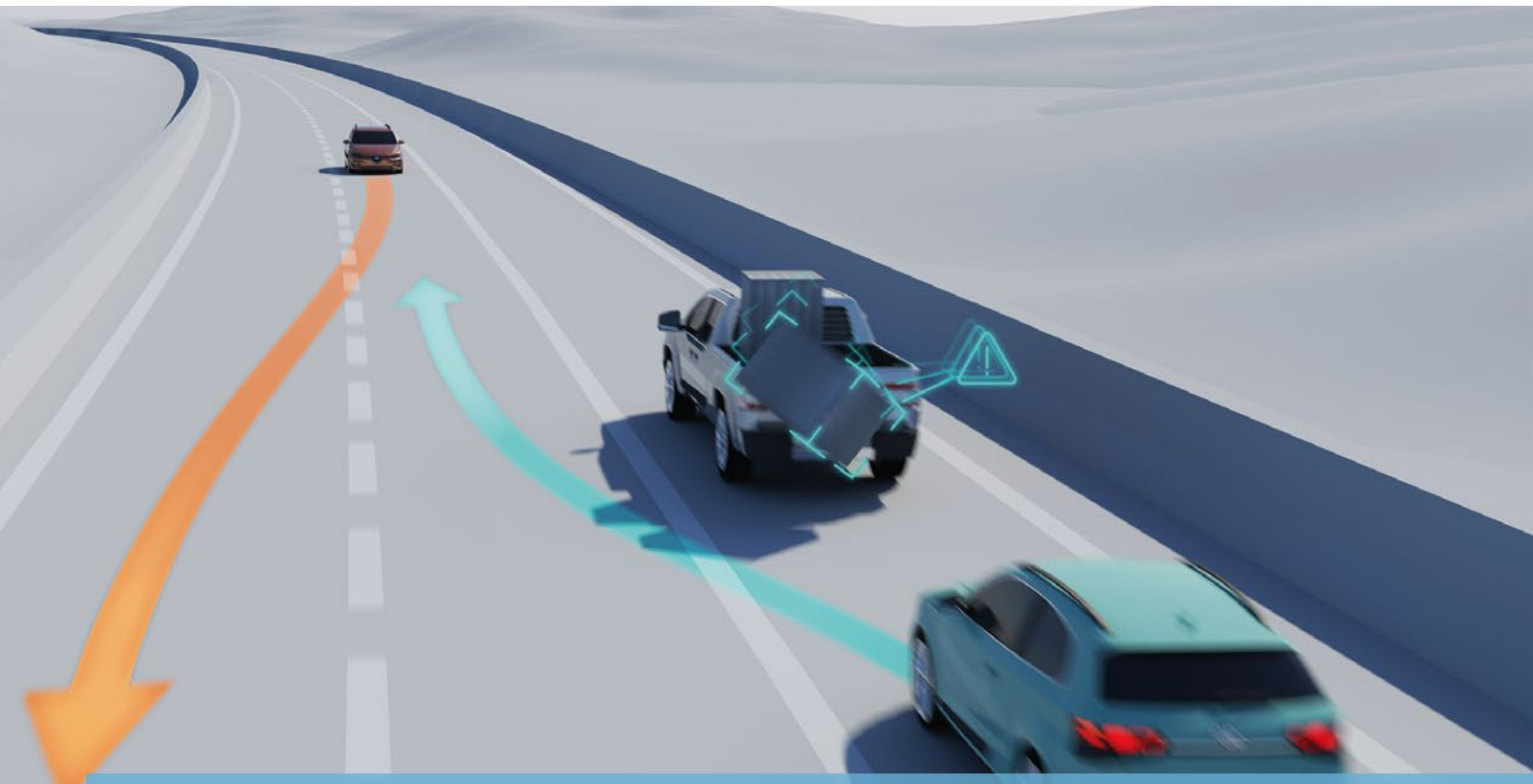
PROFILREGION
MOBILITÄTSSYSTEME
KARLSRUHE



VERNETZTE MOBILITÄT

Die Teilnahme von zuerst hoch automatisierten und später auch fahrerlosen Fahrzeugen am Straßenverkehr ist – zumindest in einigen Szenarien – schon heute absehbare Zukunft. Während computergesteuerte Fahrzeuge heute noch einer Verkehrssituation gegenüberstehen, die praktisch ausschließlich von menschlichen Verkehrsteilnehmern bestimmt ist, wird sich das Verhältnis zuerst auf der Autobahn und später auch im urbanen Verkehr zunehmend zum automatisierten Fahren verschieben. Entsprechend kann das Potenzial des automatisierten Fahrens im Gegensatz zu rein individuellen Manöverplanungen durch zunehmende Vernetzung, Abstimmung und Kooperation intelligenter Fahrzeuge schrittweise weiter ausgeschöpft werden.

Kooperierende Fahrzeuge können den Verkehrsfluss optimal ausnutzen, ihre Manöver zur Erhöhung der Verkehrssicherheit abstimmen und gleichzeitig komfortables und energiesparendes Fahren ermöglichen.
Mit geeigneten Sicherheitslösungen müssen jedoch mögliche Risiken, die das autonome Zusammenspiel vernetzter Fahrzeuge mit sich bringt, systemimmanent abgesichert werden. Schon während des Entwurfs der Hard- und Software dieser neuen Fahrzeuge sind entsprechend wirksame Mechanismen zum Schutz gegen Missbrauch („security by design“) und zum Schutz der Privatsphäre der Verkehrsteilnehmer („privacy by design“) zu integrieren.

Im Rahmen des Initialisierungsprojekts „Vernetzte Mobilität“ werden durch die unterschiedlichen Partner potentielle Angriffsrisiken aus allen relevanten Blickrichtungen untersucht und entsprechende Gegenmaßnahmen erarbeitet. Ein erstes Ergebnis der Gruppe ist die Entwicklung eines beispielhaften Angriffsszenarios auf den Teilbereich Gruppenbildung, der am Anfang kooperativer Fahrmanöver steht.
Dabei wird eine Hackingsituation angenommen, in der der Angreifer ein sendefähiges Gerät (beispielsweise ein gehacktes Smartphone) in einem menschlich gesteuerten Fahrzeug (im Bild rot) unterbringt, das dieses Fahrzeug fälschlich als kooperierend ausweist, und mit einem vollautomatisch fahrenden Fahrzeug (im Bild grün) eine gemeinsame Manöverplanung in einer Notfallsituation einleitet (s. Abb. 1).
In Erwartung des ausgehandelten Ausweichmanövers des gehackten Fahrzeugs entscheidet sich das vollautomatische Fahrzeug für das Ausscheren auf die Gegenfahrspur, obwohl auch nicht-kooperative Manöver möglich gewesen wären, die aber weniger vorteilhaft waren.
Kurz nach Einleitung des Notfallmanövers erkennt das vollautomatische Fahrzeug, dass das entgegenkommende Fahrzeug nicht entsprechend des Plans auf die Außenspur ausweicht.

Abb. 1

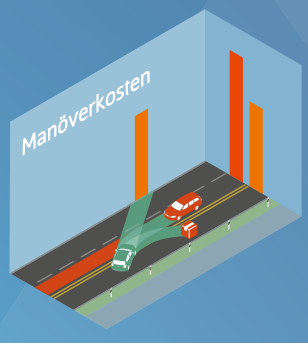


Abb. 2

Manöveroptionen zu Beginn der Notfallsituation (Abb. 1) mit Kooperationsmöglichkeit und während bei der Erkenntnis eines Hackingangriffs (Abb. 2)

Das Manöver resultiert in einer deutlich kritischeren Notfallsituation, in der das vollautomatische Fahrzeug lediglich Manöveroptionen zur Verfügung hat, die allesamt gravierende Auswirkungen verursachen (s. Abb. 2).

Verlässt sich das vollautomatische Fahrzeug also auf eine (ungesicherte) kooperierende Manöverplanung, kann in Risikosituationen ein erheblicher Schaden entstehen, der nicht mehr abzuwenden ist, wenn die fehlende Kooperationsfähigkeit erkannt wird.

Kontakt:

Dr. Dieter Willersinn

Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB),
Fraunhofer Str. 1, 76131 Karlsruhe
Tel: 0721 6091-387
dieter.willersinn@iosb.fraunhofer.de