CySiVuS

Cyber-Sicherheit für Verkehrsinfrastruktur- und Straßenbetreiber

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2016	**Status**	laufend
Projektstart	02.10.2017	**Projektende**	31.03.2020
Zeitraum	2017 - 2020	**Projektlaufzeit**	30 Monate
Keywords			

Projektbeschreibung

Cybersicherheit und Privacy bilden große Herausforderungen für kooperative Verkehrsinfrastrukturen und autonom fahrenden vernetzten Fahrzeuge, welche diese nutzen. Die Fahrzeuge benötigen detaillierte Daten über die Umgebung, um ein umfassendes Lagebild in Echtzeit erstellen zu können und um sich darin sicher zu bewegen. Die Integrität dieser Daten ist eine wesentliche Voraussetzung für autonomes vernetztes Fahren. Cybersicherheit ist nicht nur für effizientes Verkehrsmanagement, kooperative Funktionen und koordinierte Autonomie notwendig, erfolgreiche Angriffe können auch direkt Menschenleben gefährden. Österreich ist Technologieführer für kooperative Verkehrsinfrastrukturen und darauf basierendes autonomes vernetztes Fahren. Cybersicherheit ist essentiell, um diese Technologien sicher für die Gesellschaft verfügbar zu machen.
Das Projekt CySiVus (Cybersicherheit für Verkehrsinfrastruktur- und Straßenbetreiber) wählt die Cybersicherheit der Straßen- und Verkehrsinfrastruktur als spezifischen Ansatzpunkt für die Situationsanalyse. Es wird die bestehende und zukünftige Struktur des kritischen Infrastruktursystems Straße einschließlich der digitalen Infrastruktur erfasst und autonome Fahrszenarien gesammelt. Ein Bedrohungskatalog für Fahrzeug- und Kommunikationssysteme bildet die Basis für eine breit angelegte Risikoanalyse, um aus praxisorientierten Anwendungsfällen Bedrohungsszenarien zu entwickeln und adressierte Cybersicherheits-Maßnahmen formuliert. Eine cybersichere Referenzarchitektur zur Einordnung bestehender und in naher Zukunft zu entwickelnder Technologieinnovationen bildet einen strukturellen Rahmen für die kommenden Entwicklungen. Die Referenzarchitektur wird einer umfassenden Compliance-Analyse im rechtlichen und gesellschaftlichen Rahmen unterzogen und die Auswirkungen auf die Stakeholder erfasst. Ausgewählte Ergebnisse werden am Projektende münden in einem demonstrativen Laborprototyp mit realer Hardware, sodass damit zusätzlich die Bewusstseinsbildung für den Themenkomplex Cybersicherheit in kooperativen Verkehrsinfrastrukturen unterstützt wird.
Im Projekt CySiVus sind alle wesentlichen Interessengruppen für eine zukünftige digitale österreichische Straßen- und Verkehrsinfrastruktur als Konsortialpartner oder Stakeholder eingebunden und stellen dadurch die interdisziplinäre Einbindung der unterschiedlichen Perspektiven der Anspruchsgruppen sicher. Signifikante Innovationsaspekte umfassen unter anderem weiterentwickelte Cybersicherheitsstandards im Kontext des sich momentan verändernden rechtlichen Rahmens, Cybersicherheits-Selbsttest beim Fahrzeugstart und Nutzung physikalischer Eigenschaften der V2X-

Kommunikation. Das Projekt wird sowohl bei der technischen und rechtlichen Betrachtung als auch bei den entwickelten Methoden den Stand der Technik erweitern.

Abstract

Cyber Security and Privacy are major challenges for cooperative traffic infrastructures and autonomously driving interconnected cars which rely on it. The cars need detailed data about the environment to generate a comprehensive overview of the current situation in real time to ensure their safe movement. The integrity of the data is a prerequisite for autonomous interconnected driving. Cyber security is not only necessary for efficient traffic management, cooperative functions and coordinative autonomy – successful attacks threaten human lives. Austria is a technology leader for cooperative traffic structures and autonomous interconnected driving based-on them. Cyber security is essential to make these technologies available to society.
The project CYSiVuS (cyber security for traffic infrastructure- and road service provider) selects cyber security of the road and traffic infrastructure as a specific starting point for situation analysis. The existing and future structure of the road system as a critical infrastructure together with the digital infrastructure is analysed and autonomous driving scenarios are collected. A threat catalogue for car and communication systems is the basis for a broadly based risk analysis, in order to derive threat scenarios from practical use cases and develop cyber security countermeasures. A cyber-secure reference architecture to integrate existing and other technology innovations which will be developed in the near future forms the structural frame for upcoming developments. The reference architecture will be analysed regarding its legal and social compliance and the impact on the stakeholders will be identified. At the end of the project, selected results will lead to a research demonstrator with real hardware. This will support awareness for the topic cyber security in cooperative traffic infrastructures.
In this project CySiVuS all essential stakeholder groups for a future digital road and traffic infrastructure in Austria are involved as consortium partners or stakeholders, which ensures the interdisciplinary integration of the different perspectives of the stakeholders. Significant innovation aspects include more developed cyber security standards in the context of the changing legal framework, cyber security self-test when starting a car, and using physical characteristics of V2X communication. The project, as well as through the methods that are developed, improves on the technical state of the art from a technological and legal perspective.

Projektkoordinator

AIT Austrian Institute of Technology GmbH

Projektpartner

Nokia Solutions and Networks Österreich GmbH

TÜV TRUST IT TÜV AUSTRIA GMBH

TÜV AUSTRIA AUTOMOTIVE GMBH

T-Systems Austria GesmbH

Universität Wien

SWARCO FUTURIT Verkehrssignalsysteme Ges.m.b.H.

Bundesministerium für Inneres (BMI)

Bundesministerium für Landesverteidigung

Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft