CybSiVerkehr

Cyber Sicherheit für zukünftige Verkehrssysteme

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS F&E-Dienstleistungen 2015	**Status**	abgeschlossen
Projektstart	01.11.2016	**Projektende**	31.10.2017
Zeitraum	2016 - 2017	**Projektlaufzeit**	12 Monate
Keywords			

Projektbeschreibung

Transportsysteme für Fracht und Personen unterliegen durch die breite Anwendung von In-formations- und Telekommunikationstechnologien einem grundlegenden Wandel. Computer, IT, sowie alle Arten von Kommunikation im Fahrzeug, zwischen Fahrzeugen oder zwischen Fahrzeugen und Infrastruktureinrichtungen für Straße, Schiene, Wasser und Luft sind die Bausteine kooperativer und intelligenter Verkehrssysteme (Cooperative Intelligent Transport Systems, C-ITS). Disruptive Technologien wie autonome Autos mit entsprechender künstlicher Intelligenz werden unser Verständnis von Mobilität und Logistik grundlegend ändern. Die technologischen, wirtschaftlichen, sozialen und politischen Auswirkungen dieser Technologien sind tiefgreifend.

Als ein Teil der kritischen Infrastrukturen können Ausfälle von Transportsystemen auf nationaler und europäischer Ebene eine verheerende Auswirkung auf kritische Branchen und das Leben in der Gesellschaft haben. Die zugrunde liegende IT-Infrastruktur, wie beispielsweise C-ITS und Cyber-Systeme von autonomen Fahrzeugen sind ein Ziel von Cyber-Attacken. Aufgrund der zunehmenden Komplexität, Funktionalität und Konnektivität sind moderne Transportsysteme besonders anfällig. Diese komplexen Infrastrukturen sind sehr stark verteilt und schwer vor Angriffen zu schützen. Zudem birgt der Einsatz neuer Technologien auch neue Risiken und Gefahren, und führt zudem neue Abhängigkeiten ein. Cybersicherheit und Resilienz muss in den verschiedenen Arten von Transportsystemen schon beim Design und in der Konzeption fundamental berücksichtigt werden.

Die Studie „CybSiVerkehr“ stellt in Österreich einen ersten systematischen Ansatz dar, diese Fragen zu verstehen und zu beantworten. CybSiVerkehr wird dazu im Rahmen der globalen industriellen und technologischen Entwicklung eine eingehende Analyse der auf Österreich zukommenden Cyber-Herausforderungen durchführen. Die Studie wird auf die aktuellen Forschungstrends und Entwicklungen mit dem Fokus auf Cyber-Sicherheit Bezug nehmen, um so die spezifischen Herausforderungen und Auswirkungen auf die österreichische Gesellschaft zu identifizieren. Zudem wird die Studie versuchen, sowohl zu technischen als auch gesellschaftlichen Aspekten die Meinungen von Experten und Interessengruppen einzuholen. Ein Teil der Studie wird eine Reihe von umfassenden Handlungsempfehlungen an die entscheidenden Stakeholder sein, um so Österreich auf die kommenden Cyber-Herausforderungen künftiger Verkehrssysteme vorzubereiten.

Die Studie wird sowohl Leitlinien zu relevanten Themen wie Risikomanagement, Prävention, Cyber Situational Awareness, gesellschaftliche Bereitschaft oder Privatsphäre der Nutzer enthalten, als auch Hinweise geben, wie Österreich sich an die Spitze der EU im Bereich Cyber-Sicherheit von Transportsystemen stellen kann.

Abstract

Transport systems for people and freights are undergoing a fundamental transformation due to wide application of information and telecommunication technologies (ICT). Computers, IT and all types of communications are used in vehicle, between vehicles and between vehicles and road-side infrastructures for road, rail, water, and air transport to build Cooperative-Intelligent Transport Systems (C-ITS). Disruptive technologies such as autonomous car with belonging artificial intelligence will change our way of mobility and logistics. The technological, economic, social, and political impact is profound.

As a part of the critical infrastructures, failures of transport systems will have devastating effect on critical sectors and people's life at national and European level. The underlying ICT infrastructure such as C-ITS and cyber systems of autonomous car is a target of cyberattacks. Due to the increase in complexity, functionality and connectivity, modern and future transport systems have an increased vulnerability. The complex infrastructure is highly distributed and difficult to protect. Besides, new technologies also introduce new threats and risks, and more interdependencies. Thus cybersecurity and resilience must be considered across different types of transport systems.

As a first systematic approach to these concerns in Austria, CybSiVerkehr study will conduct an in-depth analysis of cybersecurity challenges facing Austria in the context of the global industrial and technological development. The study will research on existing development of C-ITS and autonomous car in order to identify specific challenges and their impact on Austrian society with respect to cybersecurity. The study will seek experts' and stakeholders' opinions on the identified issues and concerns covering both technical and societal aspects. A part of the study will be devoted to comprehensive recommendations to the stakeholders on how to prepare Austria and react to cybersecurity challenges future transport systems. The study will provide guidance on relevant topics including risk management, prevention, cyber situation awareness, legal and social readiness, and user privacy as well as how to position Austria at the front of transport system cybersecurity in EU.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Kompetenzzentrum Sicheres Österreich (KSÖ)
- Universität für Weiterbildung Krems
- Bundesministerium für Landesverteidigung