V digitálním věku je potřeba čím dál víc štítů. V následujících letech čeká českou i evropskou dopravu komunikační revoluce, stane se mnohem flexibilnější, inovativnější a chytřejší díky projektu C-ROADS. Ale jak bezpečná bude?

Kybernetická bezpečnost na silnicích? Nejvyšší ochrana...

Doprava v Evropě se (z)mění. *„Nacházíme se v jednom z klíčových bodů v historii mobility, kdy dochází k revoluci v tom, jak vnímáme řízení dopravy – nejen z pohledu centrálních a informačních systémů, ale i z pohledu uživatele, tedy řidiče,“* říká **Jiří Vítek**, architekt dopravních a inovativních řešení ze společnosti O_2, která je partnerem Ministerstva dopravy v projektu C-ROADS – technologické platformy, která umožňuje vozidlům komunikovat s jinými vozidly, dopravní signalizací, silniční infrastrukturou i ostatními účastníky silničního provozu.

Otázky zní: Jaká je/bude ochrana datových komunikačních center a integrační platformy? Jaká je/bude bezpečnost a ochrana osobních údajů? Jaká jsou zadní kolečka kooperativních inteligentních dopravních systémů (C-ITS) a co je/bude v pozadí toho, že celé řešení bude fungovat bezpečně?

DOBA DATOVÁ

Informační vlny zpráv, dat a údajů se už teď šíří od palubních jednotek v autech, tramvajích, hasičských vozidlech k jednotkám u silnic, na křižovatkách, na přejezdech až po datová centra. Všechno se vším komunikuje.

Postupnou evolucí se z auta stal IT systém, navíc systém, který intenzivně komunikuje se svým vzdáleným, ale nově i blízkým okolím. *„Cílem této komunikace je nabídnout uživateli co největší bezpečnost a komfort při cestování.“* upozorňuje Jiří Vítek.

C-ROADS zatím jede v pilotní fázi, ale už brzy bude vše v ostrém provozu. Jaké jsou předpoklady k tomu, aby se všechny zprávy dostaly tam, kam se dostat mají, a aby se uživatelé nemuseli bát, že se jim zobrazí třeba podvržená zpráva?

DATOVÁ KOMUNIKAČNÍ CENTRA...

Důležitým prvkem toku informací je Datové komunikační centrum (DKC). Každá jednotka a každá aplikace, které slouží uživateli, jsou připojeny vždy k právě jednomu datovému komunikačnímu centru. Takovým provozovatelem mohou být stát, kraj, město nebo telekomunikační operátor. DKC, ke kterému jsou připojeny jednotky a/nebo aplikace, se stará o jejich bezproblémový provoz, zajišťuje update software v jednotkách, řeší problémy, ke kterým může docházet. Zároveň přijímá a zpracovává C-ITS zprávy, které od jednotek chodí mobilní sítí – je tedy tou stranou, která zprávy přijímá, vyhodnocuje, validuje a předává je dalším uživatelům nebo dalším provozovatelům datových komunikačních center.

... INTEGRAČNÍ PLATFORMA...

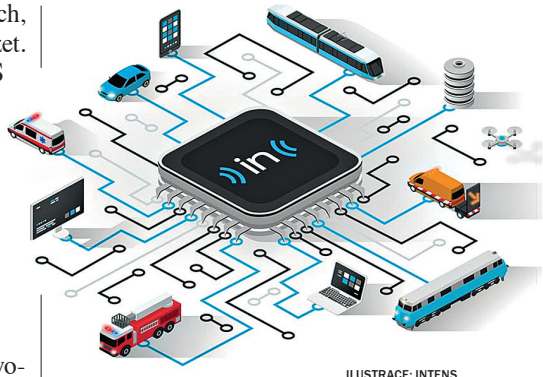
Aby se zprávy mezi jednotlivými provozovateli a mezi jednotlivými DKC dostaly vždy ke všem a co nejrychleji, o to se stará tzv. Integrační platforma. Kromě toho, že zajišťuje neuvěřitelně rychlý přenos zpráv všude tam, kde je potřeba, připojuje i Národní dopravní informační centrum (NDIC) a zprostředkovává zprávy, které jsou zde uloženy. Integrační platforma slouží také jako centrální propojovací bod na C-ITS řešení v rámci dalších států Evropy. Zajišťuje tak i spojení s jednotkou, se kterou se uživatel vydá za hranice po Evropě.

... A BEZPEČNOST

A to všechno vyžaduje soubor technických zařízení, procesních kroků a kontrol…

Prostě bezpečnost.

Projekt C-ROADS garantuje, že systém a zprávy, které se v něm pohybují, jsou bezpečné, nejsou podvržené nebo pozměněné. Každá C-ITS jednotka, která se v systém vyskytuje, je napojena na systém, který v pravidelných intervalech do jednotky doručuje sady certifikátů, které pak jednotka používá k podepisování všech zpráv. Jednotka, která zprávu přijímá, tak má možnost si zkontrolovat, zda je zpráva správně podepsána platným certifikátem a pochází z jednotky, která je v systému oprávněně. Na základě typu certifikátu lze i poznat, od koho zprávy putují – odliší tak sanitku, která může požádat o bezpečnostní uličku, od běžného auta.



ILUSTRACE: INTENS

Na úrovni architektury řešení základních principů fungování IT systémů a komunikace je nezbytné akcentovat bezpečnost.

VE SVĚTĚ JEDNOTEK C-ITS

Pokud dojde k odcizení jednotky, nebo se jednotka v systému chová nepatřičně (např. generuje opakovaně matoucí zprávy), dojde ke zneplatnění certifikátu, a dojde tak velmi rychle k vyřazení jednotky, a ostatní jednotky přestanou akceptovat zprávy podepsané zneplatněným certifikátem.

Další vrstvou bezpečnosti je tzv. *„protection profile“*, tedy soubor pravidel na úrovni hardware zařízení a software. Takovýto „bezpečnostní profil“ existuje pro jednotky v infrastruktuře, jednotky v autě nebo mobilní aplikace.

Poslední vrstvou systému je audit řešení, kdy dochází k posouzení všech propojení, rozhraní, vazeb, pravidel a procesů, tak aby byla potvrzena bezpečnost a odolnost systému proti externím, ale i interním útokům.

JAN ZELENKA

C-ROADS CZECH REPUBLIC MEMBER OF C-ROADS PLATFORM
Spolufinancováno Nástrojem Evropské unie pro propojení Evropy