

## **STANDARDI INFORMACIONE BEZBEDNOSTI PRIMENJENI U BEZBEDNOSTI DRUMSKOG SAOBRAĆAJA**

Miroslav Petrović<sup>1</sup>, Dušan Mladenović<sup>2</sup>, Mladen Nedeljkov<sup>3</sup>

<sup>1</sup>Devellop d.o.o, Beograd, Srpsko društvo za ITS, [miroslav.petrovic@devellop.com](mailto:miroslav.petrovic@devellop.com)

<sup>2</sup>Univerzitet u Beogradu - Saobraćajni fakultet, Srpsko društvo za ITS,  
[d.mladenovic@sf.bg.ac.rs](mailto:d.mladenovic@sf.bg.ac.rs)

<sup>3</sup>Srpsko društvo za ITS, [mladen.nedeljkov@itsserbia.rs](mailto:mladen.nedeljkov@itsserbia.rs)

**Rezime:** *Uvođenjem informaciono-komunikacionih tehnologija (IKT) u pojedinim vidovima saobraćaja nastali su inteligentni transportni sistemi (ITS). U drumskom saobraćaju količina komponenti koje su prisutne u samim vozilima, ali i u pratećoj infrastrukturi, a koje su zasnovane na korišćenju IKT-a je od tada narasla do neslučenih granica – luksuzna i kompleksnija vozila već nekoliko godina mogu da imaju i preko 150 elektronskih upravljačkih jedinica (ECU). Povećanjem zastupljenosti ovakvih vozila na putevima, uz investiciona ulaganja u drumske infrastrukturne ITS sisteme, otvorio se i prostor za nove vrste zloupotreba kojima se ugrožava bezbednost saobraćaja. Povećanim prisustvom IKT sistema, neminovno se povećava i uticaj njihove ranjivosti na bezbednost celokupnog sistema drumskog saobraćaja. Važnost koju sa sobom ovaj trend donosi blagovremeno je prepoznat kod vodećih aktera na globalnom nivou, te stoga već nekoliko godina postoji nekoliko specijalizovanih inicijativa i standarda koji uređuju ovu oblast. U ovom radu biće predstavljena trenutna situacija u svetu po ovom pitanju, kao i postojeći trendovi u pogledu daljeg uređenja ove oblasti.*

**Ključne reči:** *informaciona bezbednost, inteligentni transportni sistemi (ITS), drumski saobraćaj, UNECE, WP.29*

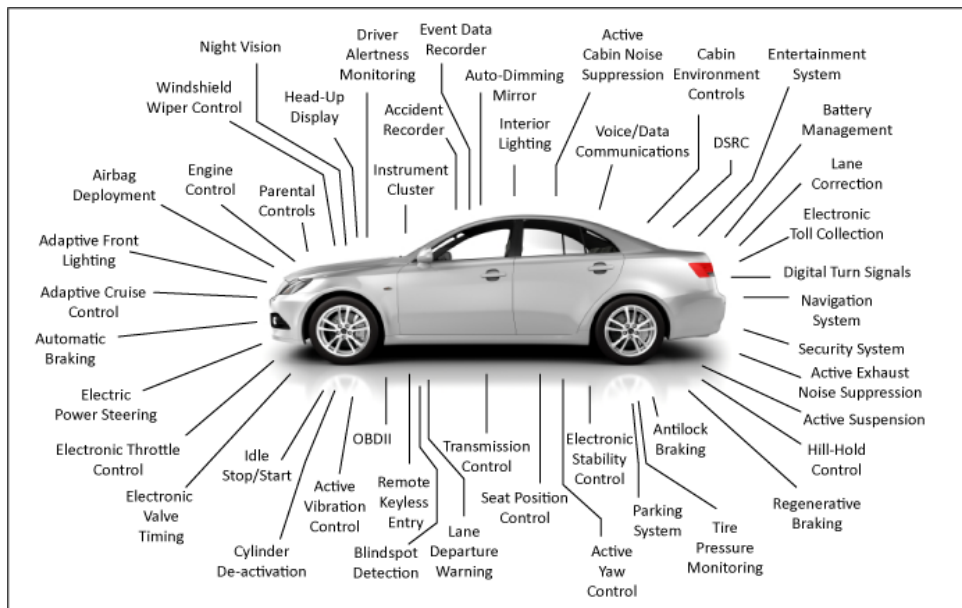
### **1. Uvod**

Smatra se da je prva elektronska upravljačka jedinica (*Electronic Control Unit*, ECU) uvedena u automobilske proizvodni program 1977. godine. Bio je to, iz današnje perspektive, relativno jednostavan mikrokontroler ugrađen u General Motors Oldsmobile Toronado i koji je regulisao trenutak paljenja. Već sledeće, 1978, godine General Motors je nudio kupcima modela Cadillac Seville kao opciju putni računar zasnovan na modifikovanom Motorola 6802 mikroprocesorskom čipu, koji je prikazivao informacije o brzini, nivou goriva, kilometraži i informacijama o statusu motora [1].

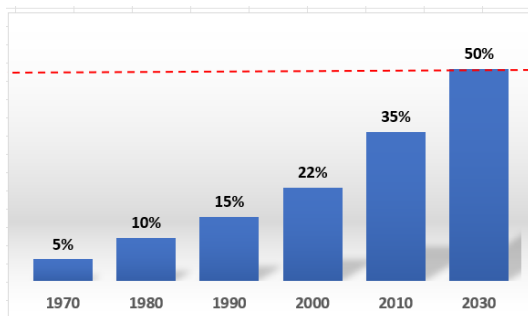
Od tih pionirskih početaka do današnjih dana, put pređen u razvoju i upotrebi informaciono-komunikacionih tehnologija u drumskom saobraćaju doveo je do korišćenja okvira 150 ECU u složenijim luksuznim vozilima. Kada se u obzir uzme i

razvoj prateće inteligentne drumske infrastrukture (signalizacija, nadzor, upravljanje, naplata, itd.), količina informaciono-komunikacionih tehnologija koja je već uključena u saobraćaj je enormna. Robert N. Charette je u članku iz 2009. („*This Car Runs on Code*“) vizionarski naveo da vozila više ne pokreće gorivo, već softverski programi [2].

U prilog tome, slika 1 pokazuje tipične komponente savremenog vozila koje su danas upravljane pomoću specijalizovanih kompjuterizovanih ECU jedinica. Na slici ih ima 47, a kao što smo već naveli, taj broj je u realnim primenama značajno nadmašen.



Slika 1. Tipične ECU jedinice današnjeg vozila [3]



Slika 2. Procenat učešća cene elektronike u ukupnoj vrednosti tokom godina [5]

Očigledno je da se rastući trend na ovome neće zaustaviti. Na horizontu su uveliko električna i autonomna vozila, a pomalaju se i kooperativni inteligentni sistemi (C-ITS). Stoga se isti autor, Robert N. Charette, samo 12 godina kasnije, na istom mestu oglašava sa zabrinutošću („*How Software is Eating the Cars*“) – da li automobilska industrija može da izdrži i kako da podrži ovakvu transformaciju [4].

Projekcije već prognoziraju da će nakon pola veka razvoja, 2030. godine, vrednost elektronike u ukupnoj vrednosti vozila dosegnuti 50%. Na slici 2 prikazana je evolucija učešća informaciono-komunikacionih tehnologija tokom poslednjih pet decenija i trend porasta njenog učešća od početaka krajem sedamdesetih godina dvadesetog veka [5].

## 2. Glavne tačke informacione ranjivosti sistema drumskog saobraćaja

Osnovne komponente drumskog saobraćaja predstavljaju vozilo, put i prateća putna infrastruktura i korisnik – učesnik u saobraćaju.

Sa druge strane, u slučaju potpune digitalizacije i automatizacije ovog vida saobraćaja kroz sistem povezanih, kooperativnih i automatizovanih vozila (*Cooperative, Connected, and Automated Mobility*, CCAM), sa stanovišta informaciono-komunikacionih tehnologija, izdvajaju se takođe tri dominantne komponente: vozilo sa svojim mnogobrojnim elektronskim upravljačkim jedinicama, komunikacioni sloj kojim se razmenjuju poruke sa vozilima i hijerarhijski nadređen aplikativni nivo, koji predstavlja treću dominantnu komponentu ovog modela.



Slika 3. Tipične pretnje informacionoj bezbednosti u sistemu drumskog saobraćaja

Iz perspektive informacione bezbednosti, svaka od ovih komponenti, predstavlja potencijalnu metu zlonamernih napada:

### a) Vozilo:

Svaki od mnogobrojnih mikroračunarskih informacionih sistema na vozilu predstavlja potencijalnu tačku zlonamernih hakerskih napada, kako putem kontaktne, tako i putem beskontaktne komunikacije kratkog dometa koju ovi moduli sve više podržavaju;

### b) Komunikacioni sloj:

Sistemi na vozilu imaju potrebu da komuniciraju sa spoljnim svetom; taj spoljni svet sačinjavaju druga vozila, drugi učesnici u saobraćaju (biciklisti,

pešaci, druge ranjive grupe...), drumska infrastruktura (signalizacija, senzori...), kontrolni i upravljački centri – hakerske metode prisutne na internetu mogu da se primene i na ovu komunikaciju;

c) Aplikativni/nadzorni nivo:

Ovakvim konceptom razvoja sistema vozila i drumskog saobraćaja uopšte, kroz horizontalnu komunikaciju (kooperativna sa drugim učesnicima u saobraćaju) i vertikalnu (sa hijerarhijski nadređenim nadzornim nivoima – kontrolnim centrima raznih namena), otvara se prostor za posredne hakerske napade preko ostalih učesnika u ovoj komunikaciji.

Slika 3 ilustruje neke tipične bezbednosne pretnje kada je informaciona bezbednost sistema drumskog saobraćaja u pitanju. Za razliku od nekih drugih industrija, kao što su finansijske usluge, energetika ili recimo telekomunikacije, automobilski sektor nije tako brzo reagovao na rastuće prisustvo informacionih tehnologija i potencijalne pretnje koje se, ugrožavanjem informacione bezbednosti, reflektuju na bezbednost drumskog saobraćaja uopšte.

### 3. UNECE

Od sredine dvadesestog veka, Ujedinjene nacije, preko svoje ekonomske komisije za Evropu (*United Nations Economic Commission for Europe*, UNECE), utiču na poboljšanje bezbednosti drumskog saobraćaja, prvenstveno kroz unapređenja bezbednosti vozila, poput regulisanja upotrebe sigurnosnih pojaseva, svetlosne signalizacije, upravljačkih sistema itd. Pod institucionalnim okriljem UNECE komiteta za kopneni transport, formiran je svetski forum za harmonizaciju regulative za vozila - WP.29, kako bi se obezbedilo da sva vozila koja se isporučuju na teritorijama država koje su prihvatile sporazum budu u skladu sa usaglašenim standardima u pogledu bezbednosti i zaštite životne sredine.

Pravni okvir sačinjavaju tri kategorije UN dogovora koji obezbeđuju pravni okvir za države pristupnice sporazumu, članicama WP.29 foruma da uspostave regulatorne instrumente u vezi sa motornim vozilima i njihovom opremom:

- a) UN odredbe u skladu sa ugovorom iz 1958. godine koje se bave uređivanjem procedura za vozila, njihove podsisteme, delove i opremu u vezi sa poštovanjem standarda u oblasti bezbednosti i zaštite životne sredine, kako u pogledu administrativnih procedura, tako i u pogledu zahteva za testiranje performansi. Time se definišu procesi sertifikacije tipova podsistema, delova i opreme vozila, usklađenost proizvodnih procesa sa definisanim normama i uzajamna priznanja sertifikata izdatih od strane sertifikovanih ustanova drugih zemalja potpisnica sporazuma.
- b) UN globalna tehnička pravila (GTR), u skladu sa ugovorom iz 1998. godine, koja definišu same globalno usklađene tehničke zahteve i test procedure, čime se obezbeđuje jasne tehničke standarde za globalnu automobilsku industriju, potrošače i relevantna udruženja.
- c) UN pravila, u skladu sa ugovorom iz 1997. godine, koja se bave periodičnom tehničkom inspekcijom vozila koja su u upotrebi i međusobnim međunarodnim priznavanjem rezultata tih inspekcija.

Pored država koje su pristupile ugovoru iz 1958. godine u potpunosti, postoje i posebni uslovi i procedure za pojedine zemlje i grupe zemalja, kao što su: Kanada, Kina, Indija, Japan, Republika Koreja, Rusija, SAD i Evropska Unija [6].

Svetski forum WP.29 se na sistemski globalan način posvetio pitanjima informacione bezbednosti u automobilske industriji od decembra 2016. godine. Tada je u okviru WP.29, preciznije, u okviru radne grupe o inteligentnim transportnim sistemima/automatizovanoj vožnji kreirana ekspertska grupa koja se bavi informacionom bezbednošću i daljinskim ažuriranjem softvera. Danas je ta grupa pod okriljem radne grupe za autonomna, automatizovana i povezana vozila (GRVA).

#### **4. Standardi**

Od januara 2021. godine, kao rezultat rada pomenute specijalizovane radne grupe, stupile su na snagu u obliku aneksa osnovnog ugovora iz 1958. dve uredbe koje se tiču sertifikacije vozila kada su u pitanju informaciona bezbednost i upravljanje sistemom informacione bezbednosti (Uredba br. 155 uz tri manja amandmana 2022, 204 i 2025), kao i ažuriranja softvera i upravljanje sistemom za ažuriranje softvera (Uredba br. 156).

Ovim uredbama obezbeđeno je okruženje za automobilske sektor kojim se standardizuju procesi vezani za informacionu bezbednost u celokupnom životnom ciklusu vozila, čime se akteri obavezuju na uspostavljanje mera koje će služiti za minimiziranje pretnji i sprečavanje efekata ugrožavanja informacione bezbednosti. To uključuje uspostavljanje namenskog robusnog sistema menadžmenta informacione bezbednosti, kontinuirano praćenje potencijalnih ranjivosti i pretnji uz periodičnu procenu rizika, kao i pravovremenu adekvatnu reakciju na njihovo otkrivanje.

Tesno povezan sa ovim uredbama je i međunarodni standard ISO/SAE 21434 (Inženjering informacione bezbednosti za drumska vozila), objavljen iste 2021. godine u saradnji međunarodne organizacije za standardizaciju (ISO) i udruženja automobilske inženjerske (SAE), koji definiše zahteve za menadžment sistema informacione bezbednosti koji treba da budu ispunjeni za nove tipove inteligentnih vozila. Za razliku od standarda ISO 27001 koji je namenjen upravljanju sistemom informacione bezbednosti u svim oblastima jedne organizacije, nezvezano od industrije kojom se ona bavi, ISO/SAE 21434 prilagođen specifičnim pitanjima informacione bezbednosti vezanim za vozila i ranjivosti njihovih elektronskih sistema na informacione rizike i pretnje.

#### **5. Zaključak**

Pitanja informacione bezbednosti u automobilske industriji i drumskom saobraćaju uopšte postepeno postaju jednako važna kao i pitanja klasične bezbednosti saobraćaja. Kontinuirani višedecenijski trend povećanja učešća informaciono-komunikacionih tehnologija u ovoj industriji nameće kao neminovnost uspostavljanje namenskog odgovora na izazove koje ovaj trend sa sobom nosi.

Incidenti u oblasti informacione bezbednosti mogu imati posledice po širi krug aktera; od funkcionalnosti i bezbednosti samih vozila, preko bezbednosti imovine, pa sve do bezbednosti svih učesnika u saobraćaju.

Pored samih dizajnera/proizvođača vozila, pitanja informacione bezbednosti i adekvatno upravljanje bezbednosnim rizicima moraju da se sagledaju u celokupnom

lancu opsluživanja vozila tokom celokupnog životnog ciklusa – dizajna, proizvodnje, distribucije i eksploatacije.

Stoga će kvalitetno upravljanje rizicima informacione bezbednosti u celokupnom lancu tokom celog životnog ciklusa vozila zahtevati definisanje adekvatne strategije koja će morati da se prioritarno posveti sistemskom rešavanjem pitanju informacione bezbednosti. Očigledno je da će biti neophodno uspostavljanje novih radnih procesa i radnih mesta koja će zahtevati posedovanje novih znanja i novih veština koja nisu u tolikoj meri bila do sada zastupljena u automobilskej industriji. I to ne samo kod proizvođača, već u kompletnom dizajnerskom, proizvodnom, prodajnom i servisnom lancu.

## Literatura

- [1] Jonas Bereisa, Applications of Microcomputers in Automotive Electronics. IEEE Transactions on Industrial *Electronics*, 2, 87–96, 1983
- [2] Robert N. Charette, This Car Runs on Code, *IEEE Spectrum*, February 2009
- [3] The Clemson University Vehicular Electronics Laboratory, Automotive Electronic Systems, Available at: <https://cecas.clemson.edu/cvel/auto/systems/auto-systems.html>
- [4] Robert N. Charette, How Software is Eating the Cars, *IEEE Spectrum*, June 2021
- [5] Chou W, Shao J, Chung R, Chen L, Chen A and Zhou L, Semiconductors – the Next Wave Opportunities and winning strategies for semiconductor, Deloitte Touche Tomatsu Limited, 2019
- [6] UNECE, World Forum For Harmonization of Vehicle Regulations (WP.29), How it works - How to join it, Revised Fourth Edition, 2022

**Abstract:** *By introducing information and communication technologies (ICT) in transport modes, intelligent transport systems were born. Since then, a number of components using ICT solutions which are present in vehicles itself and in the overall road infrastructure has been grown enormously – luxurious and complex vehicles contain more than 150 electronic control units (ECU). Increased presence of these vehicles on the roads, alongside with investments into road infrastructure, imminently increase the potential for new types of malicious impacts on the road traffic safety. Importance of this trend has been timely recognized by major stakeholders on global level and for the last few years several dedicated activities and standards dealing with this segment exist. This paper presents an overview of the current situation in this matter on a global level, together with the existing trends dealing with the further improvements in this segment.*

**Keywords:** *cybersecurity, intelligent transportation system (ITS), road traffic, UNECE, WP.29*

**CYBERSECURITY STANDARDS  
FOR THE ROAD TRAFFIC SAFETY**  
Miroslav Petrović, Dušan Mladenović, Mladen Nedeljkov