vitesco TECHNOLOGIES

ENGINEERING TALKS

IMPACTUL SECURITĂȚII CIBERNETICE ÎN AUTOMOTIVE

Noiembrie 2020

Răzvan Coban

Public

INTRO

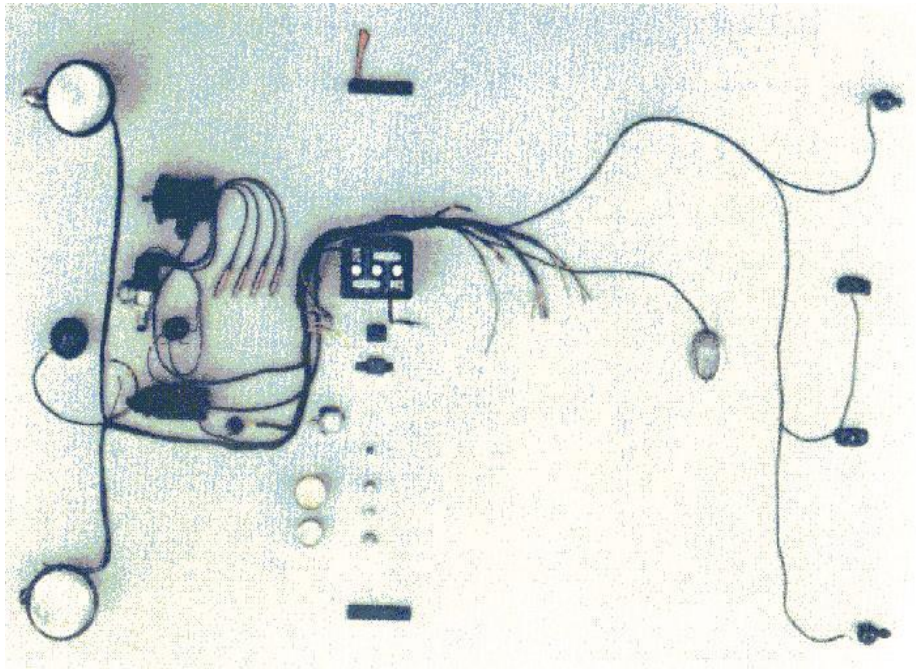
Răzvan Coban

Locație:	Iași, România
În Continental / Vitesco din	2013
Rolul curent:	Responsabil pentru activitățile de CyberSecurity Penetration Testing din cadrul Vitesco Technologies

TEHNOLOGIA DE IERI

CUM A ÎNCEPUT TOTUL

> Mercedes Benz 170V 1949

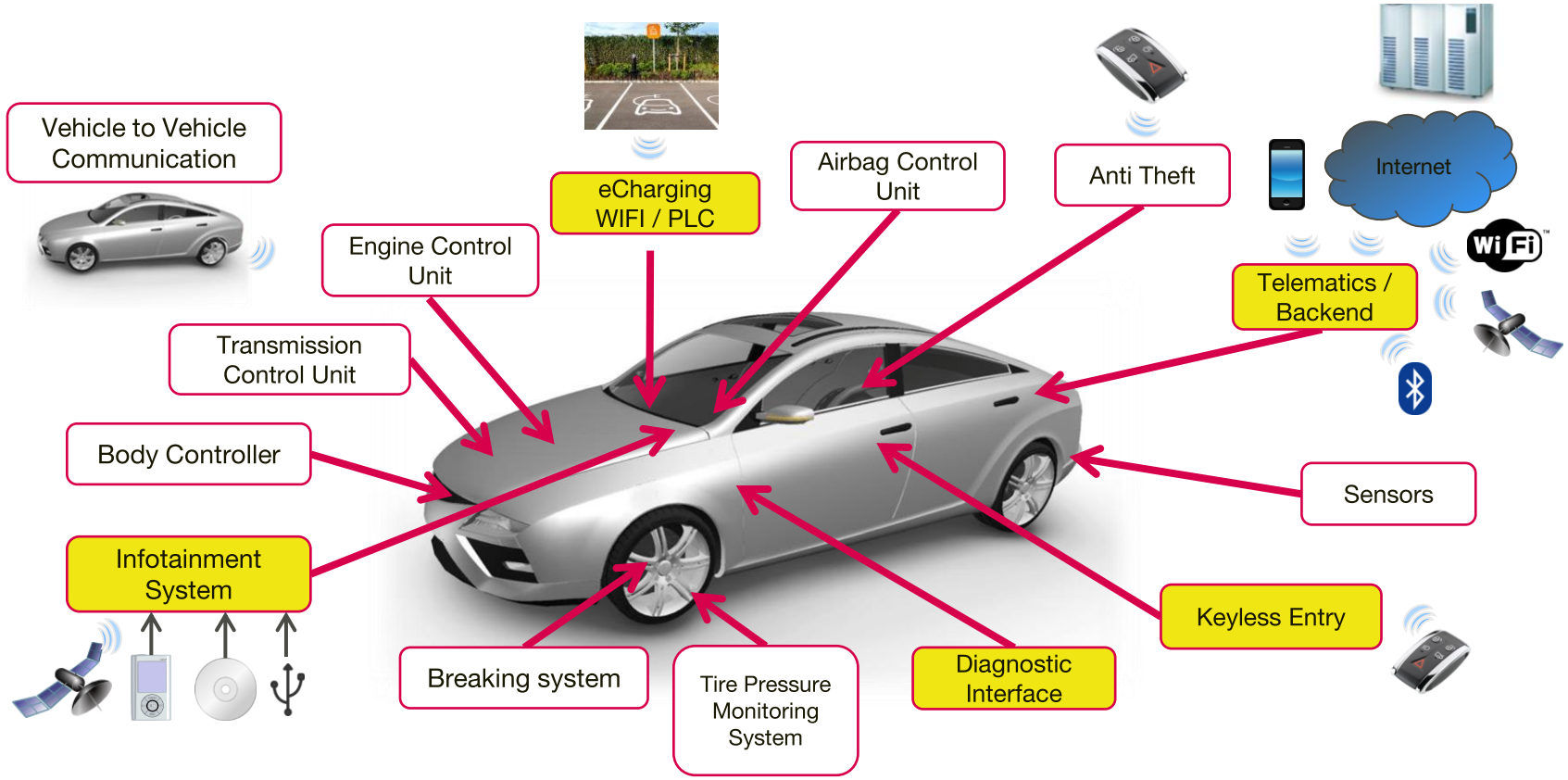


Fără siliciu, fără biți, fără octeți, în concluzie vulnerabilități puține

Sursa: Daimler view on Automotive Cyber Security, Lorenz Slansky 2018

TEHNOLOGIA DE AZI ȘI DE MÂINE

COMPLEXITATE ȘI CONECTIVITATE

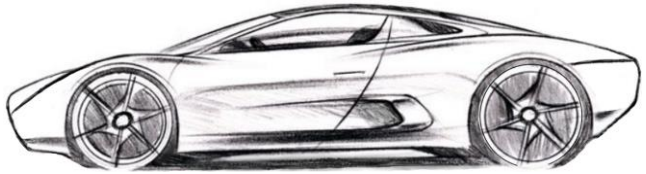


Complexitatea ridicată corelată cu conectivitatea oferă posibilități noi atacatorilor

vitesco TECHNOLOGIES

CE SE POATE ÎNTÂMPLA ?

DIFERITE SCENARII



Suprafață de atac crescută datorită noilor funcționalități și a conectivității

- Atacuri la nivelul infrastructurii
- Atacuri fără acces fizic asupra produsului
- Acces fizic la un protocol de comunicație
- Acces fizic la conectorul utilizat pentru diagnoză
- Acces fizic la nivel hardware

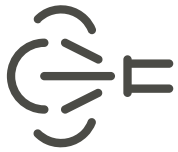
ÎN CONCLUZIE ...

CÂTEVA EFECTE

Hackerii există și în automotive

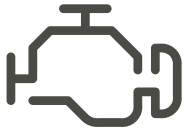
Conectivitate ⇨ scalabilitate

Furt



Manipularea valorilor raportate pentru noxe

Provocarea unor accidente



Creșterea puterii motorului

Furtul proprietății intelectuale

Încălcarea legislației din domeniu

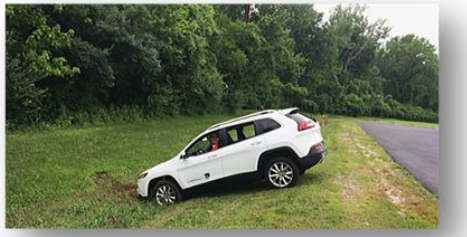
Prejudicii imense de imagine pentru producătorii auto

vitesco TECHNOLOGIES

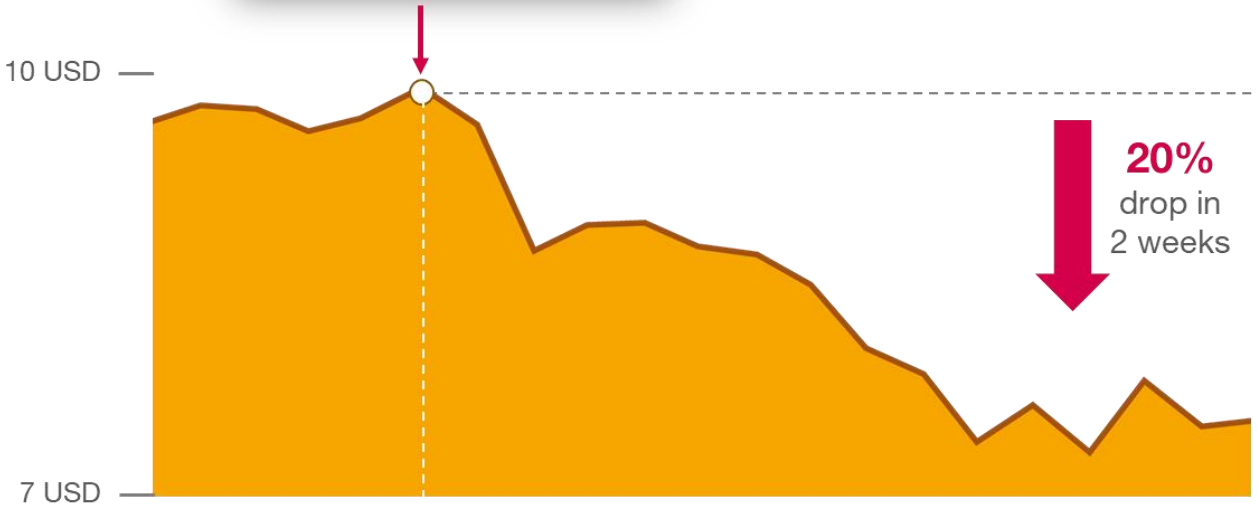
INCIDENTE DIN ACEASTĂ ARIE

STUDIU DE CAZ – IMPACTUL FINANCIAR

Valoarea acțiunilor la bursă a Fiat Chrysler - August 2015



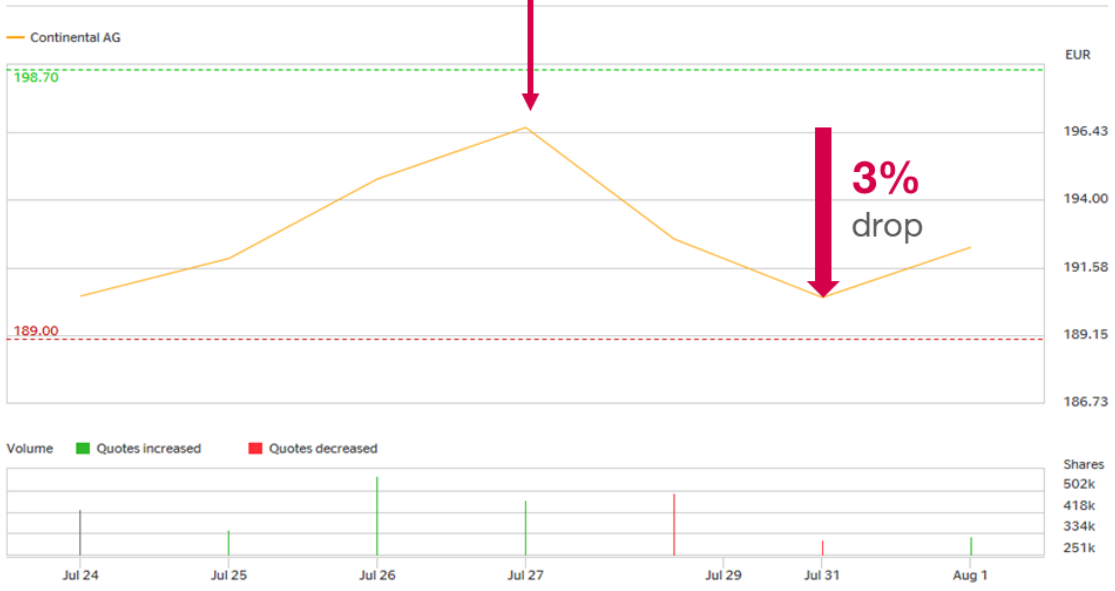
„After this jeep hack, **Chrysler recalled 1.4 Mill. vehicles for a security bug fix.**"



Atacul asupra Nissan Leaf – Iulie 2017

Nissan Leaf Hack
Advisory (ICSA-17-208-01)
Continental AG Infineon S-Gold 2
(PMB 8876)

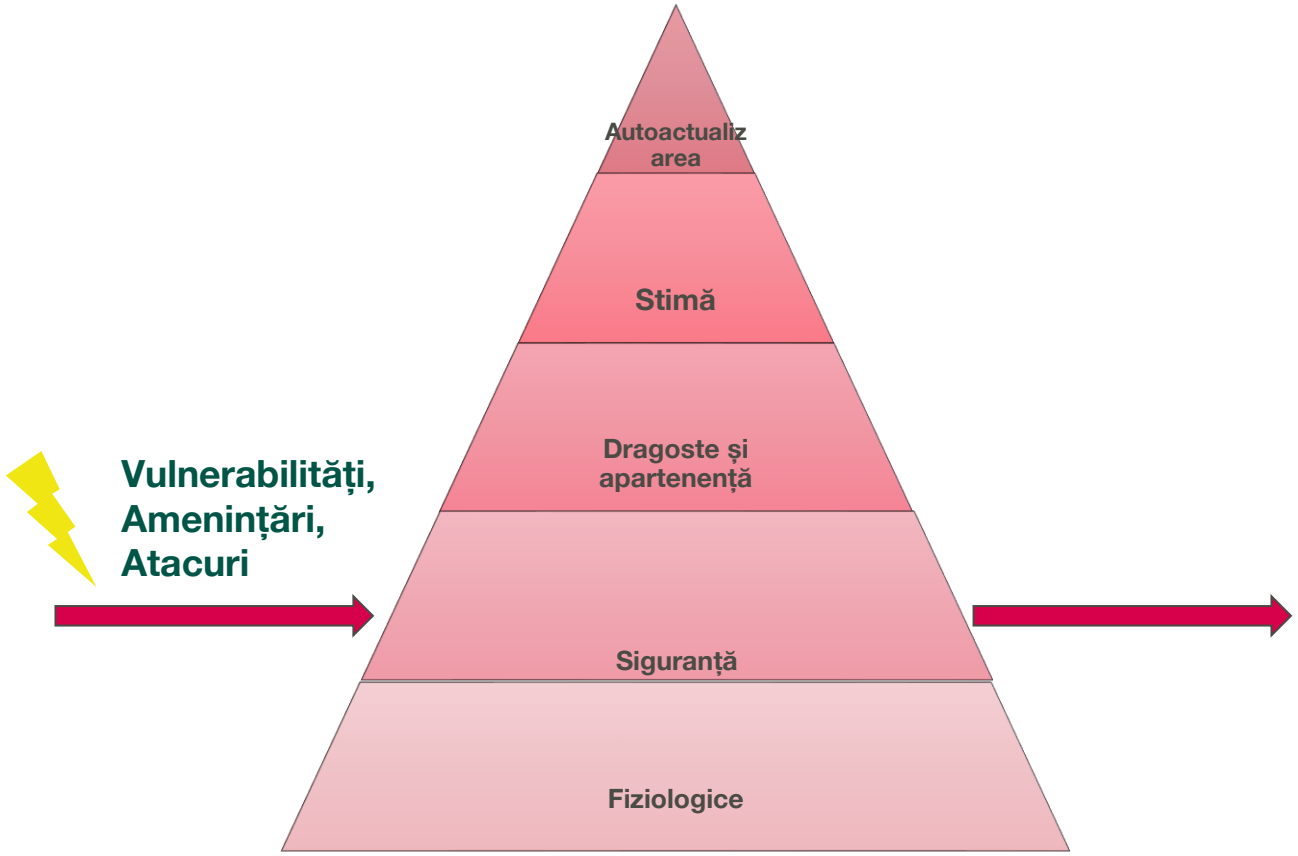
https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01
27.07.2017



vitesco TECHNOLOGIES

INCIDENTE DIN ARIA SECURITĂȚII CIBERNETICE

IMPACTUL LA NIVEL UMAN



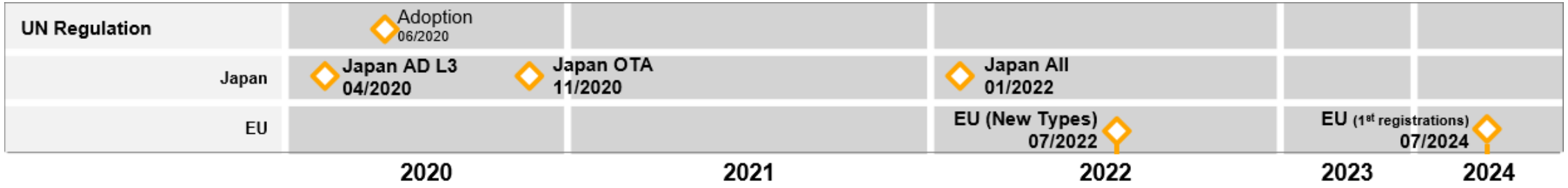
Piramida nevoilor - Maslow

- Autoritățile vor reglementa aceste aspecte
- Standardul ISO 21434 va intra in vigoare
- Producătorii auto își înăspresc cerințele din această arie
- Furnizorii accelerează implementarea proceselor interne

vitesco TECHNOLOGIES

CYBERSECURITY ÎN AUTOMOTIVE

PE CÂND ?

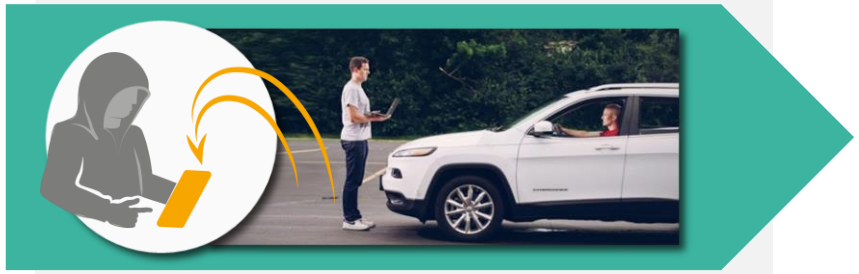


vitesco TECHNOLOGIES

RECAPITULARE

MOTIVAȚIA: SIGURANȚA PASAGERILOR

CyberSecurity



UNECE Type Approval Regulations

Cyber Security Management System (CSMS)

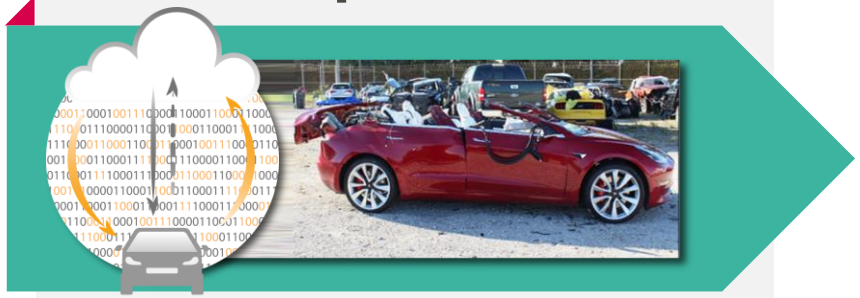
Prerequisite for

Vehicle Type A | **Vehicle Type B** | ... | **Vehicle Type N**

Cerințe

- Procese ce tratează:
  - (1) Faza de dezvoltare,
  - (2) Faza de producție,
  - (3) Faza de post-producție
- Cerințe tehnice pentru soluții de prevenție și detecție

SW Updates



Software Updates Management System (SUMS) + *RxSWIN*

Prerequisite for

Vehicle Type A | **Vehicle Type B** | ... | **Vehicle Type N**

Cerințe

- Procesul de dezvoltare
- Gestionarea actualizărilor:
  - Instalarea
  - Verificarea compatibilității
  - Capacitatea de a reveni la starea anterioară

SIGURANȚĂ FUNCȚIONALĂ VS SECURITATE CIBERNETICĂ

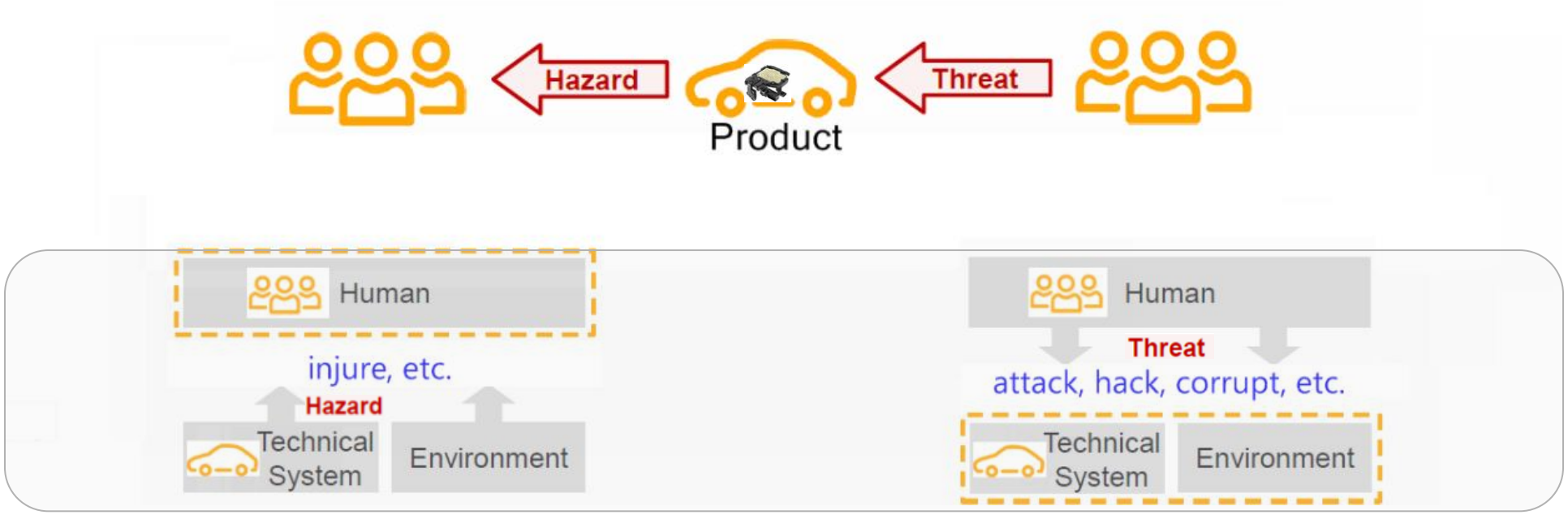
INFLUENȚE

Functional Safety

- Protect humans by limiting the risk of hazards emanating from (known) technical systems and the environment.

Security

- Protect a technical system and the environment by limiting the risk of attacks (basically unknown) caused by humans.



Siguranța funcțională este pusă în pericol în lipsa securității cibernetice

vitesco TECHNOLOGIES

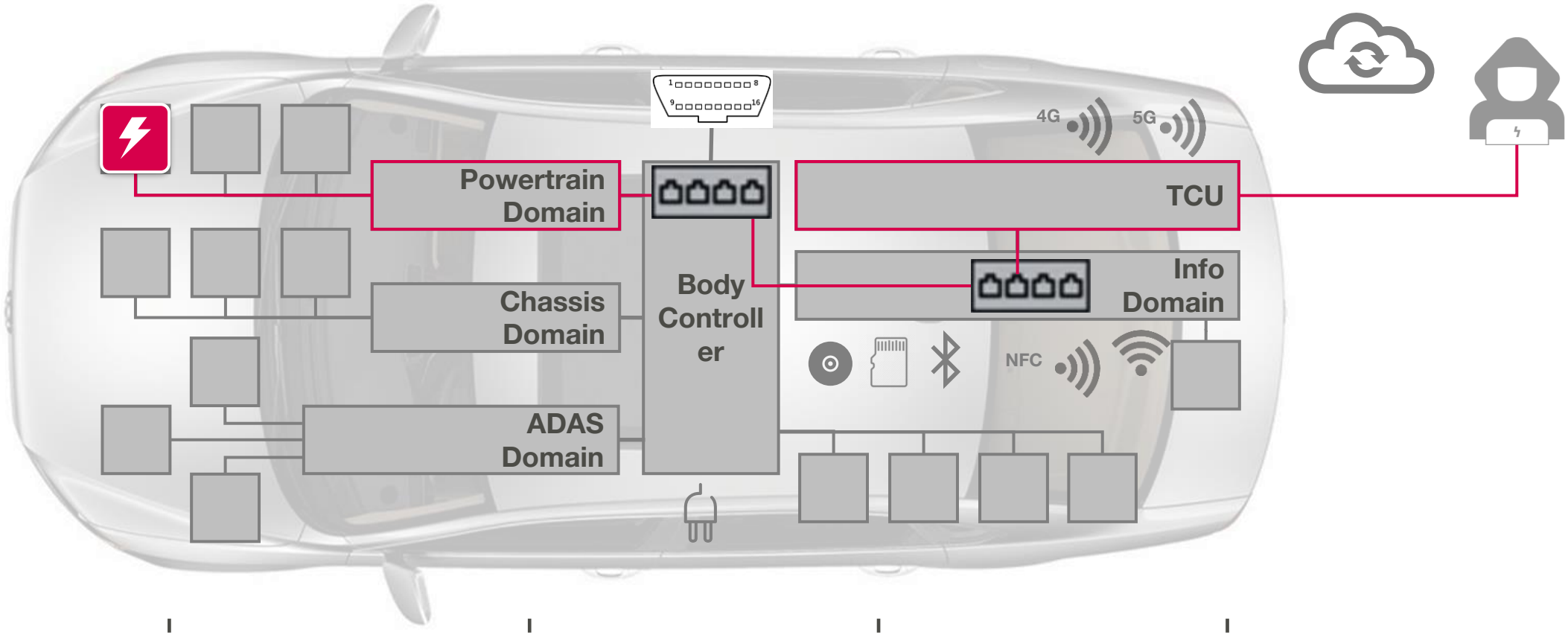
CE URMEAZĂ ?

	Conectivitate si noi canale de comunicatie	Vulnerabilitati stiute si activitati de cercetare	Atacuri	Prejudicii de imagine si financiare
Automotive	2005	2015	Astazi	
Telecom	2000	2005	Astazi	
IT-Infrastructure	1985	1990	1995	Astazi

› **Industria automotive a învățat din lecțiile altor industrii și este pregatită să reacționeze**

CONCEPTE PRACTICE

MECANISME DE APĂRARE ÎN FAȚA ATACATORILOR



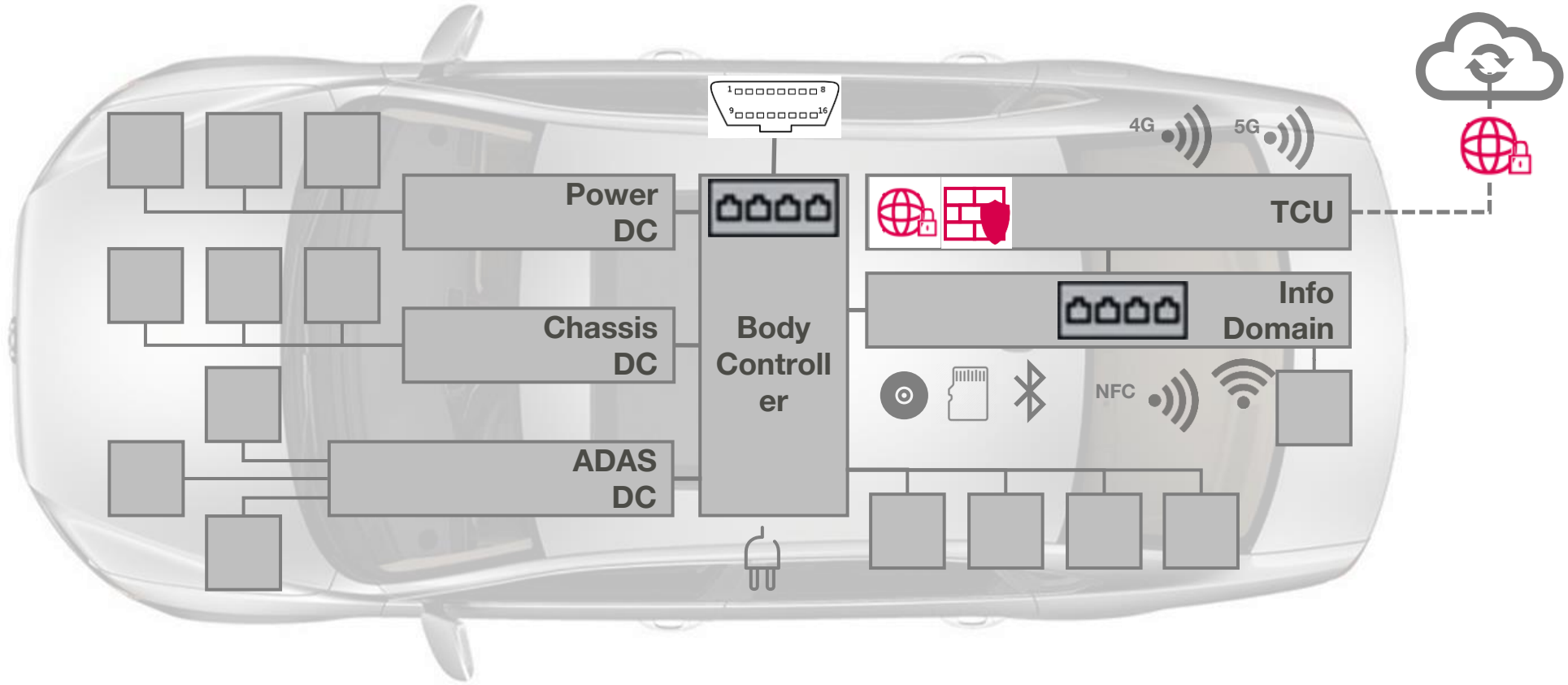
Linii de aparare

1. Access wireless
2. Acces fizic la rețeaua internă
3. Acces fizic între domenii
4. Acces fizic la nivelul unui produs
5. Manipularea comportamentului la nivel de produs sau vehicul

vitesco TECHNOLOGIES

CONCEPTE PRACTICE

PRIMUL NIVEL DE APĂRARE



Blocarea traficului nelegitim

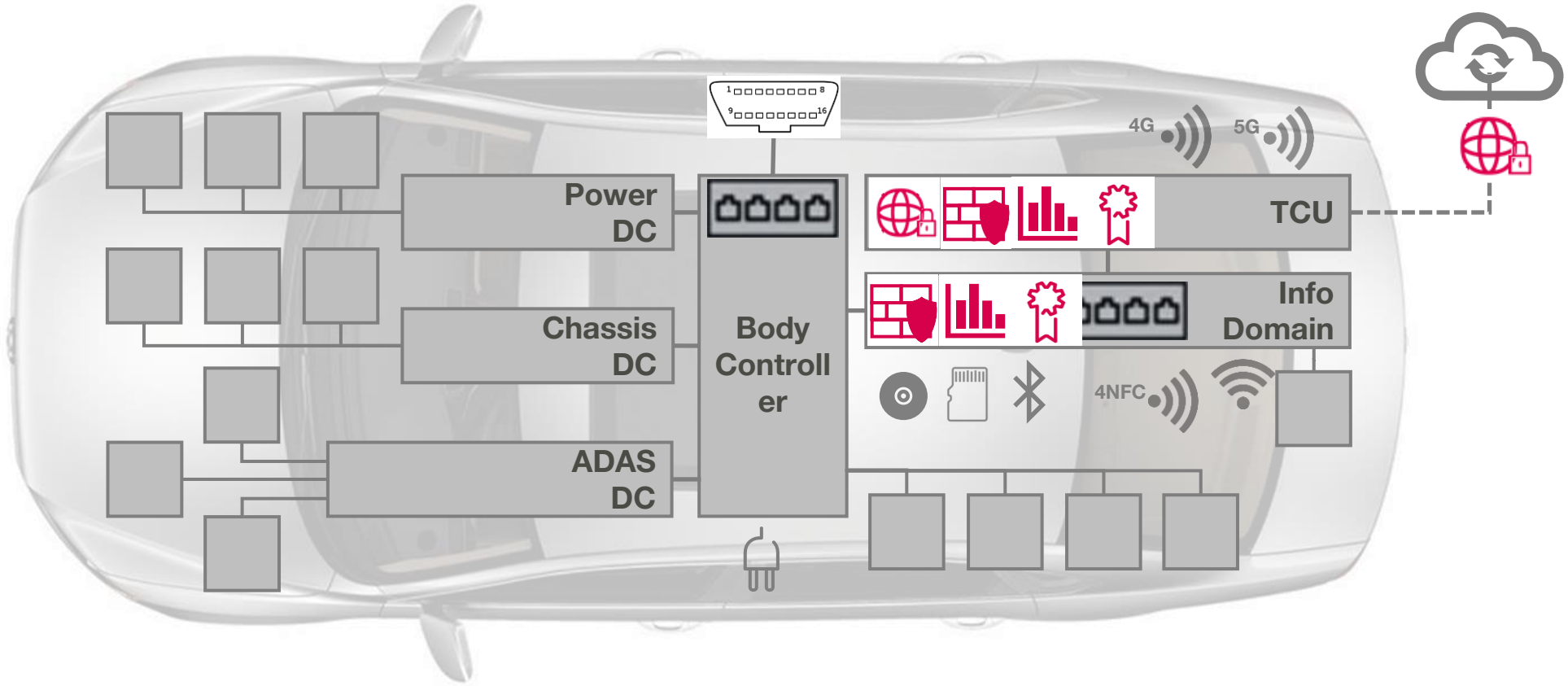
> Securizarea interfețelor ce comunică cu exteriorul

> Implementarea mecanismelor de tip Firewall

vitesco TECHNOLOGIES

CONCEPTE PRACTICE

AL DOILEA NIVEL DE APĂRARE



> Izolarea componentelor relevante din perspectiva securității

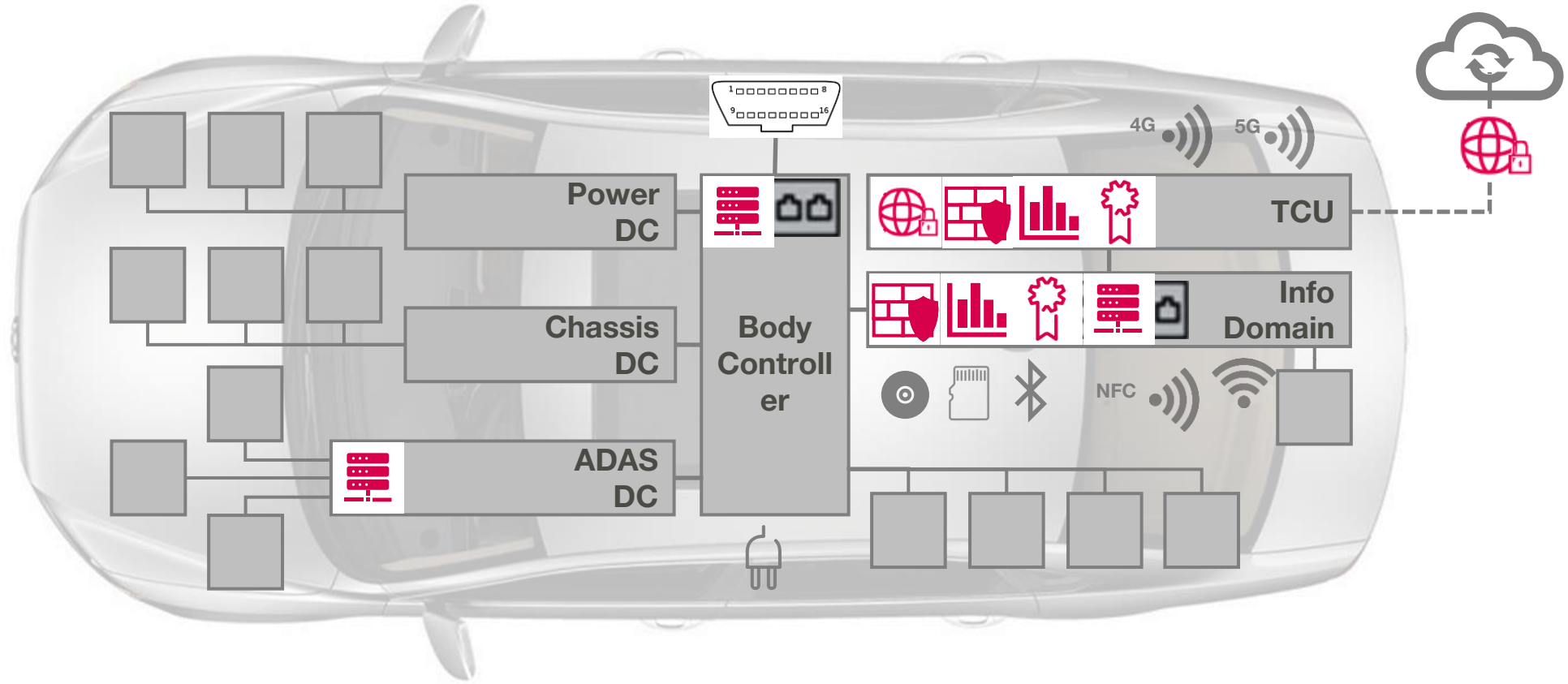
> Extinderea prezenței firewall-urilor

> Limitarea accesului pentru unele functionalități

vitesco TECHNOLOGIES

CONCEPTE PRACTICE

AL TREILEA NIVEL DE APĂRARE



Arhitectură bazatăd pe domenii

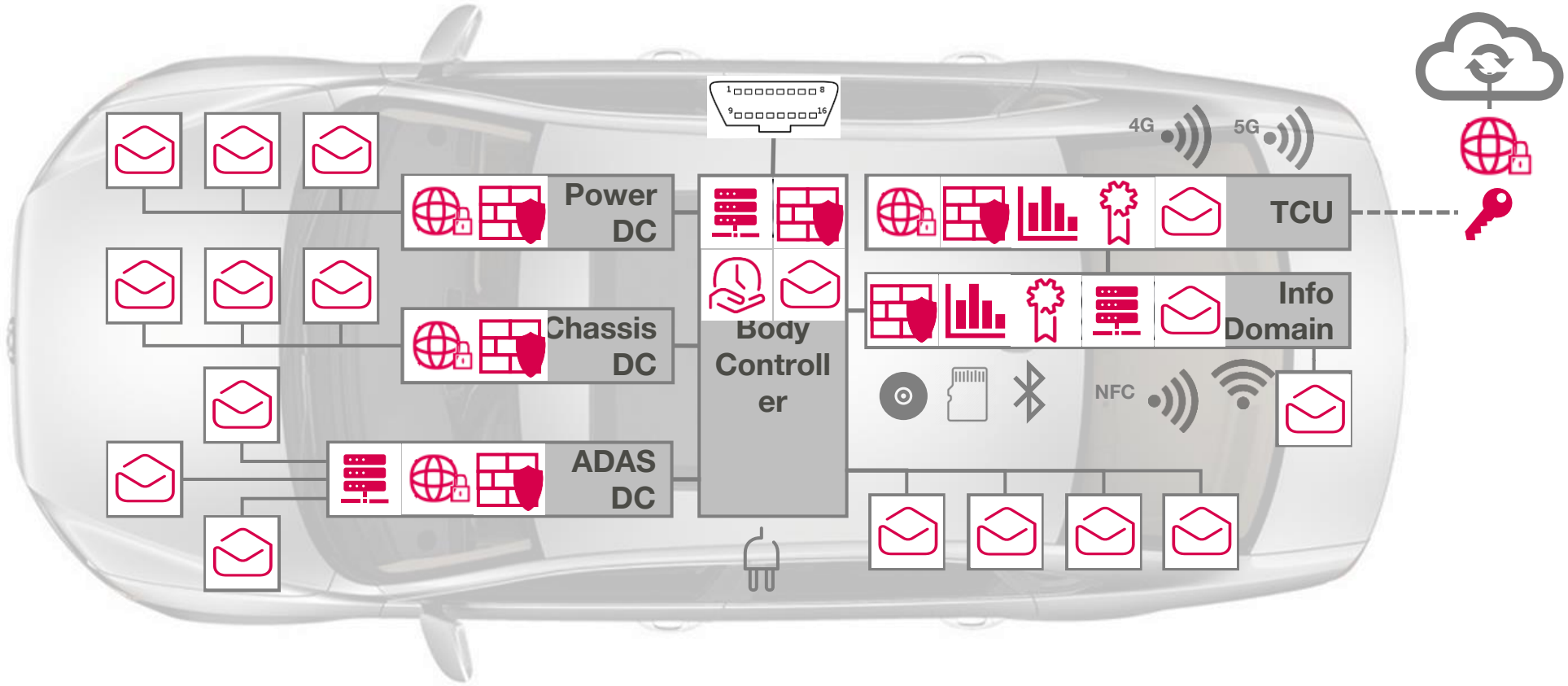
> Arhitectura vehiculului

> Rutarea comunicației prin canale securizate

vitesco TECHNOLOGIES

CONCEPTE PRACTICE

ÎN CELE DIN URMĂ



Securizarea la nivel de produs

- > Securizarea actualizărilor de software
- > Securizarea serviciilor de diagnoză utilizând mecanisme de autentificare
- > Managementul drepturilor de acces
- > Activarea funcționalităților de securitate din hardware

vitesco TECHNOLOGIES

CYBERSECURITY ÎN VT IAȘI

CYBERSECURITY

ACTIVITĂȚI ÎN DESFĂȘURARE ÎN IAȘI

> **Security Penetration Testing**
  > Centru de competență in Iași
  > Deservește toate produsele Vitesco Technologies la nivel global
  > “White-Hat Hackers”

> **Software Development for Security Solutions**
  > Activități de implementare a soluțiilor de securitate pentru produsele destinate producatorilor de autovehicule

> **Project Security & Privacy Manager**
  > Activități de coordonare a activităților din zona CyberSecurity în proiecte

> **Incident Response Management**
  > Activități de gestionare a incidentelor de securitate pentru produsele Vitesco Technologies
  > Parte a Vitesco Security Competence Center

Activitate nouă

> **Vulnerability Management**
  > Activități de identificare, evaluare și gestionare a vulnerabilităților
  > Parte a Vitesco Security Competence Center

Activitate nouă

vitesco TECHNOLOGIES

VĂ MULȚUMESC !