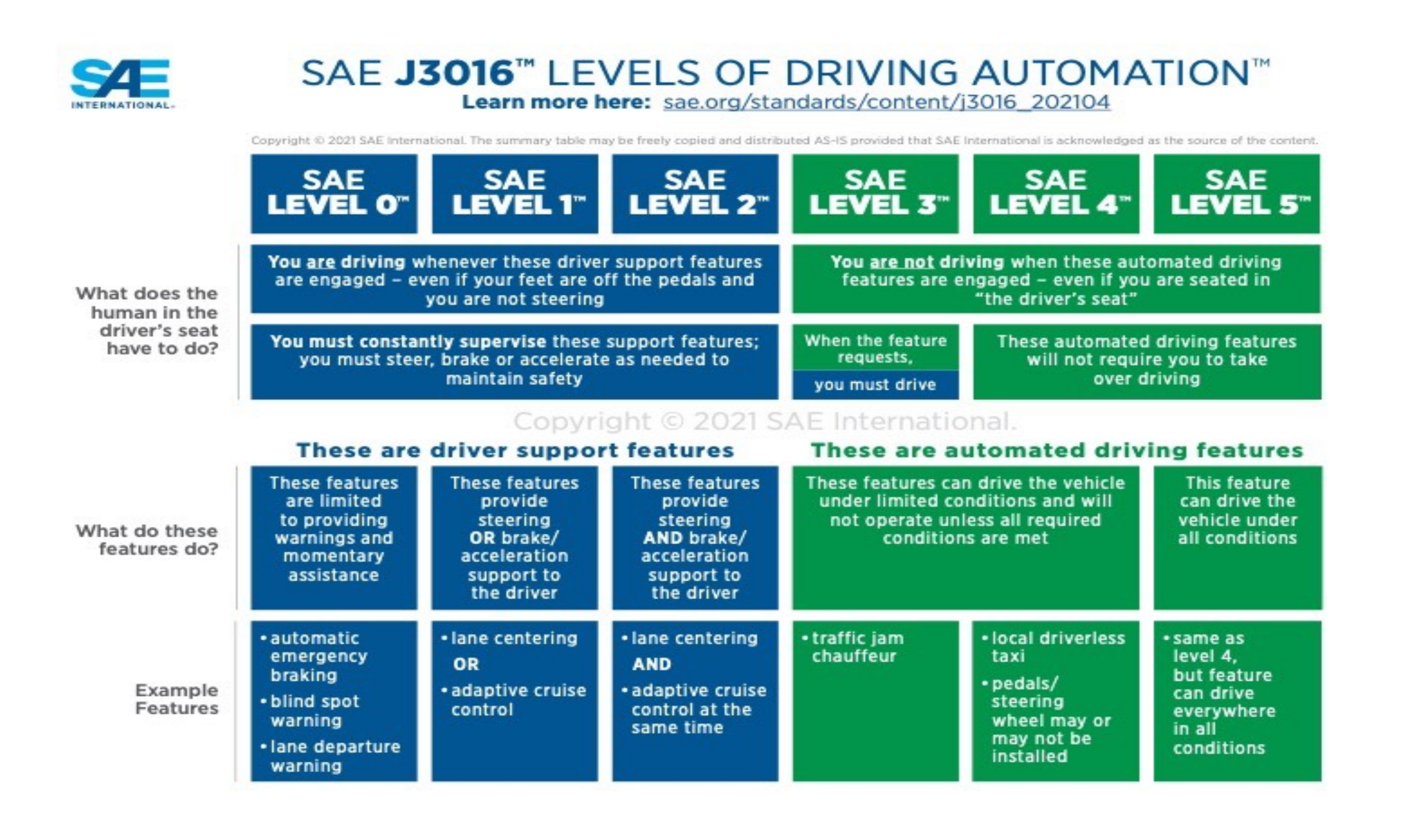
SICUREZZA INFORMATICA DEI CAMION A GUIDA AUTONOMA DI LIVELLO 4

GIANENRICO GRIFFINI – MEDIAPOINT & EXHIBITIONS

I DIVERSI LIVELLI DI AUTONOMIA



SAE INTERNATIONAL

SAE J3016™ LEVELS OF DRIVING AUTOMATION™

Learn more here: sae.org/standards/content/j3016_202104

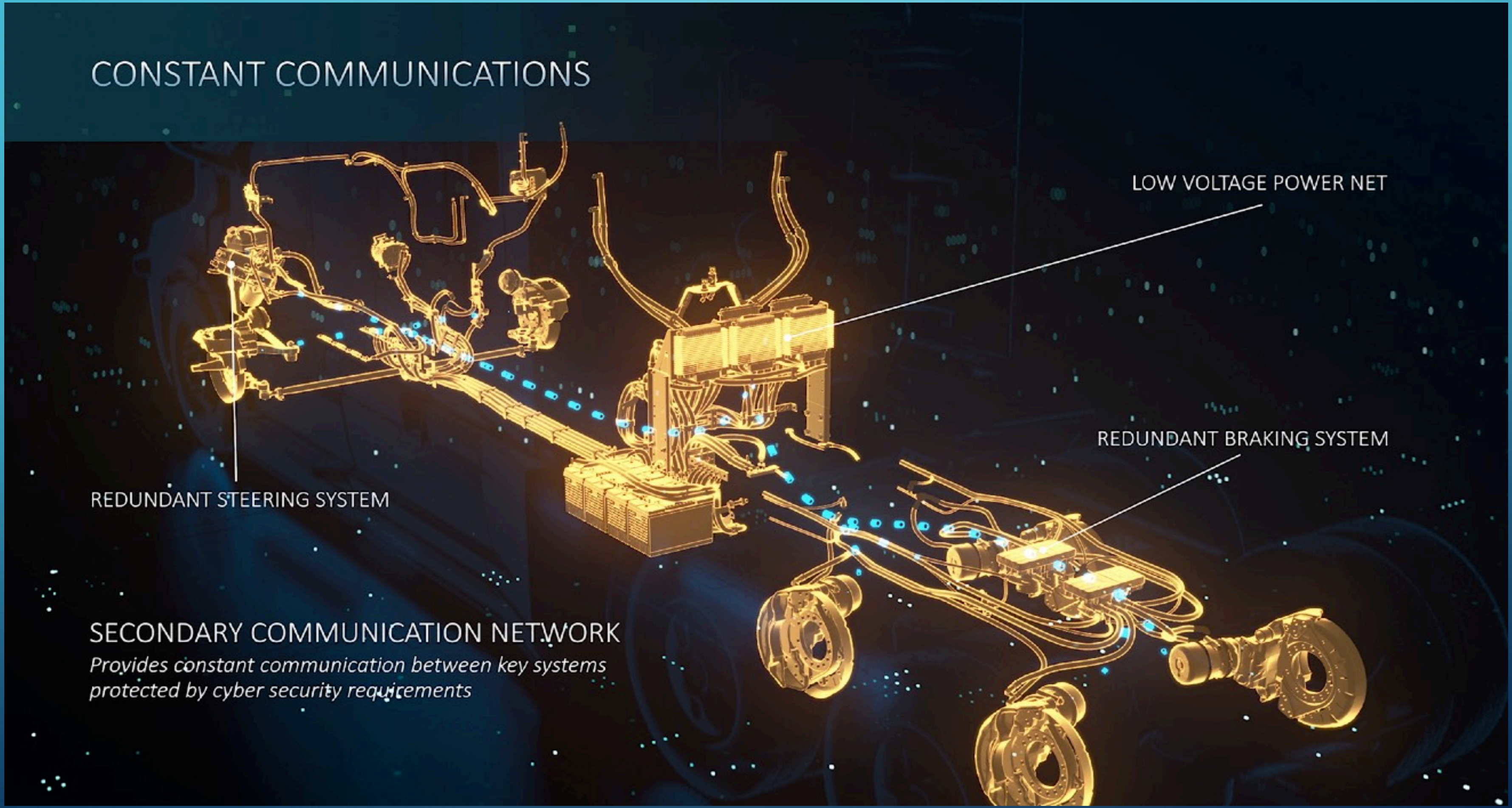
	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver's seat have to do?	**You are driving** whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			**You are not driving** when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			**These are automated driving features**		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering **OR** brake/ acceleration support to the driver	These features provide steering **AND** brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering **OR** • adaptive cruise control	• lane centering **AND** • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

I BUSINESS CASE PER I CAMION DI LIVELLO 4

- Cantieri / miniere
- Porti
- Hub-to-hub su strade pubbliche

LE SPERIMENTAZIONI HUB-TO-HUB NEGLI USA

I COMPONENTI DEL TRATTORE DI CLASSE 8



CONSTANT COMMUNICATIONS

SECONDARY COMMUNICATION NETWORK

Provides constant communication between key systems protected by cyber security requirements

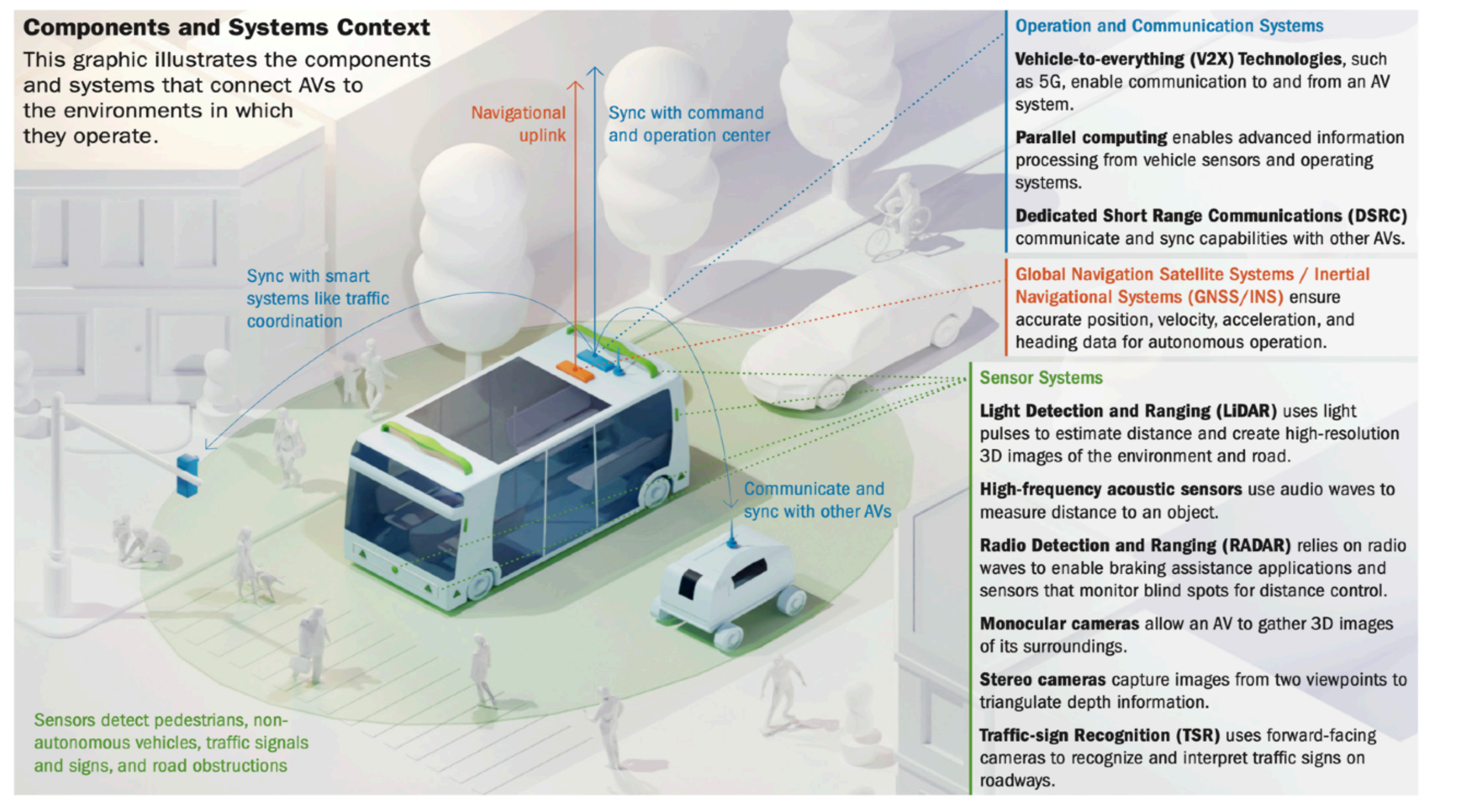
PERCHÉ HUB-TO-HUB PROPRIO NEGLI USA?

- Grandi distanze da costa a costa (5.000 km)
- Mancanza di autisti per il lunga distanza (162.000 nel 2030)
- Traffico autostradale regolare per file parallele
- Piccola differenza di velocità fra truck e auto (limite a 65 mph)
- Un solo interlocutore istituzionale (DOT)
- Ministero dei trasporti proattivo

E-CASCADIA: ELETTRICO & AUTONOMO

L'E-CASCADIA SPERIMENTALE IN AZIONE

COSA SERVE PER LA GUIDA AUTONOMA



Navigational uplink
Sync with command and operation center
Sync with smart systems like traffic coordination
Communicate and sync with other AVs
Sensors detect pedestrians, non-autonomous vehicles, traffic signals and signs, and road obstructions

Components and Systems Context

This graphic illustrates the components and systems that connect AVs to the environments in which they operate.

Operation and Communication Systems

Vehicle-to-everything (V2X) Technologies, such as 5G, enable communication to and from an AV system.

Parallel computing enables advanced information processing from vehicle sensors and operating systems.

Dedicated Short Range Communications (DSRC) communicate and sync capabilities with other AVs.

Global Navigation Satellite Systems / Inertial Navigational Systems (GNSS/INS) ensure accurate position, velocity, acceleration, and heading data for autonomous operation.

Sensor Systems

Light Detection and Ranging (LiDAR) uses light pulses to estimate distance and create high-resolution 3D images of the environment and road.

High-frequency acoustic sensors use audio waves to measure distance to an object.

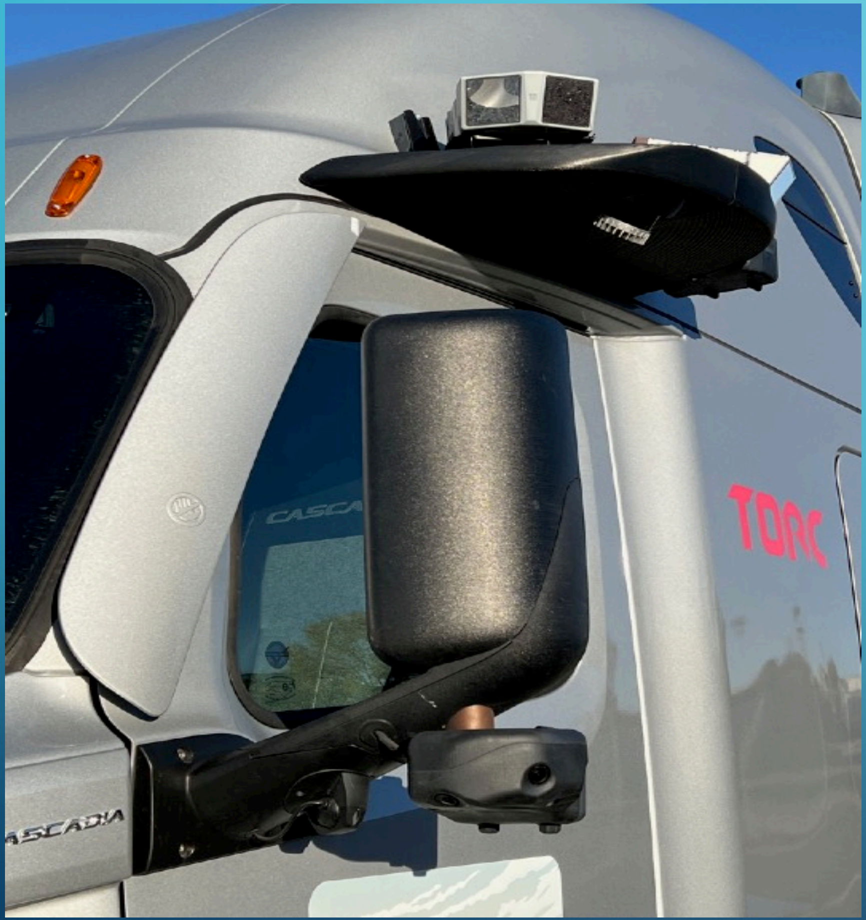
Radio Detection and Ranging (RADAR) relies on radio waves to enable braking assistance applications and sensors that monitor blind spots for distance control.

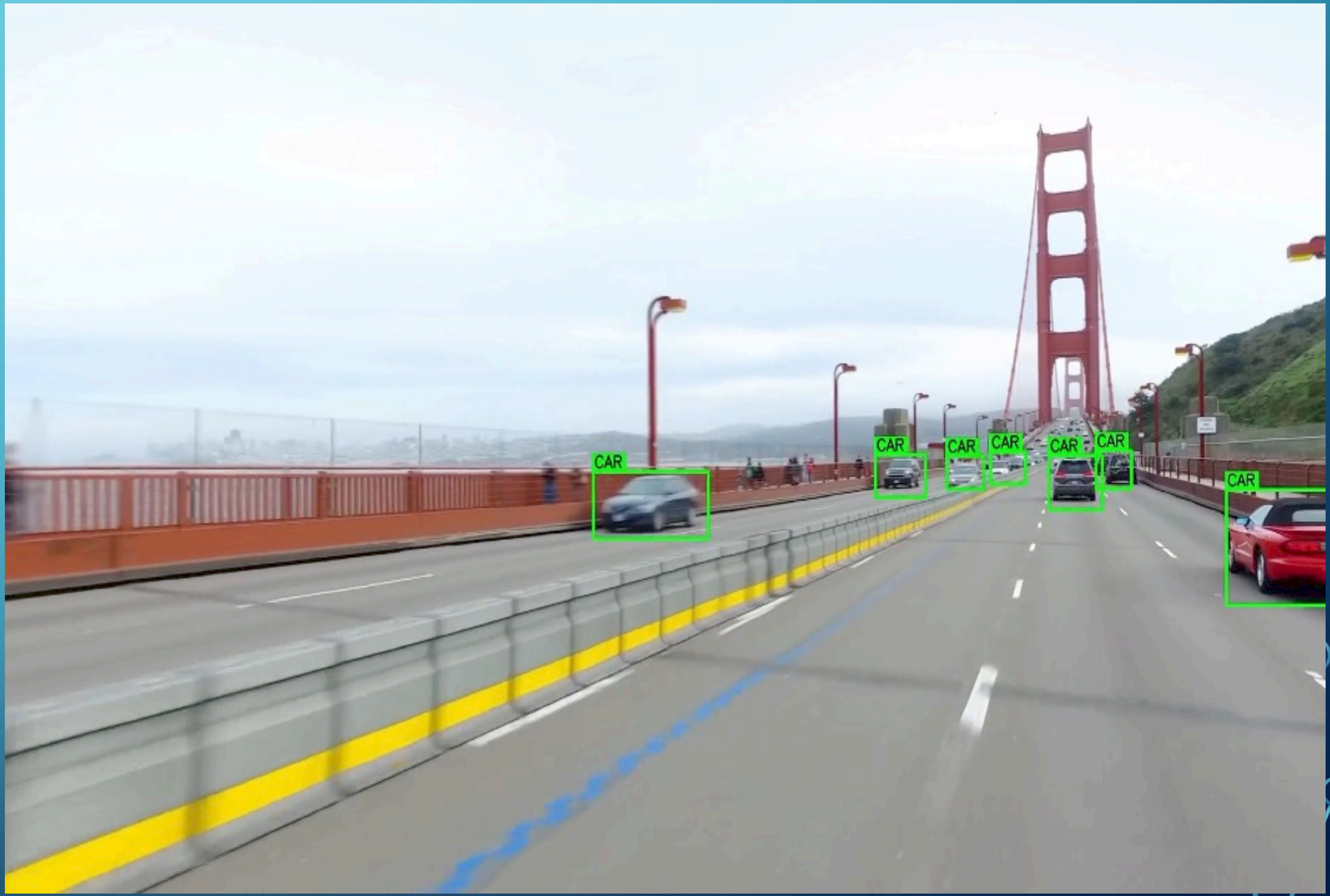
Monocular cameras allow an AV to gather 3D images of its surroundings.

Stereo cameras capture images from two viewpoints to triangulate depth information.

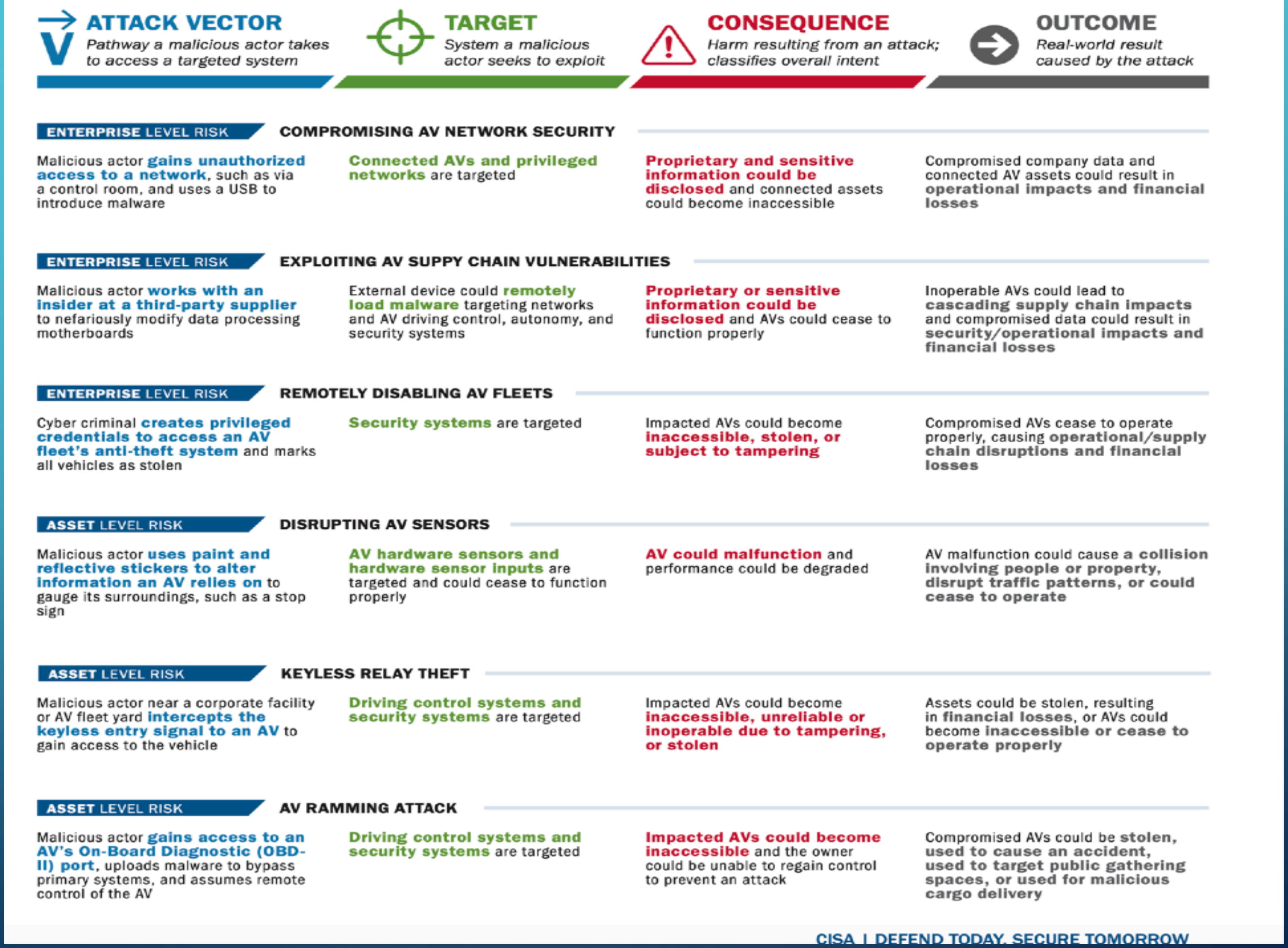
Traffic-sign Recognition (TSR) uses forward-facing cameras to recognize and interpret traffic signs on roadways.

COSA VEDONO GLI OCCHI DEL CAMION





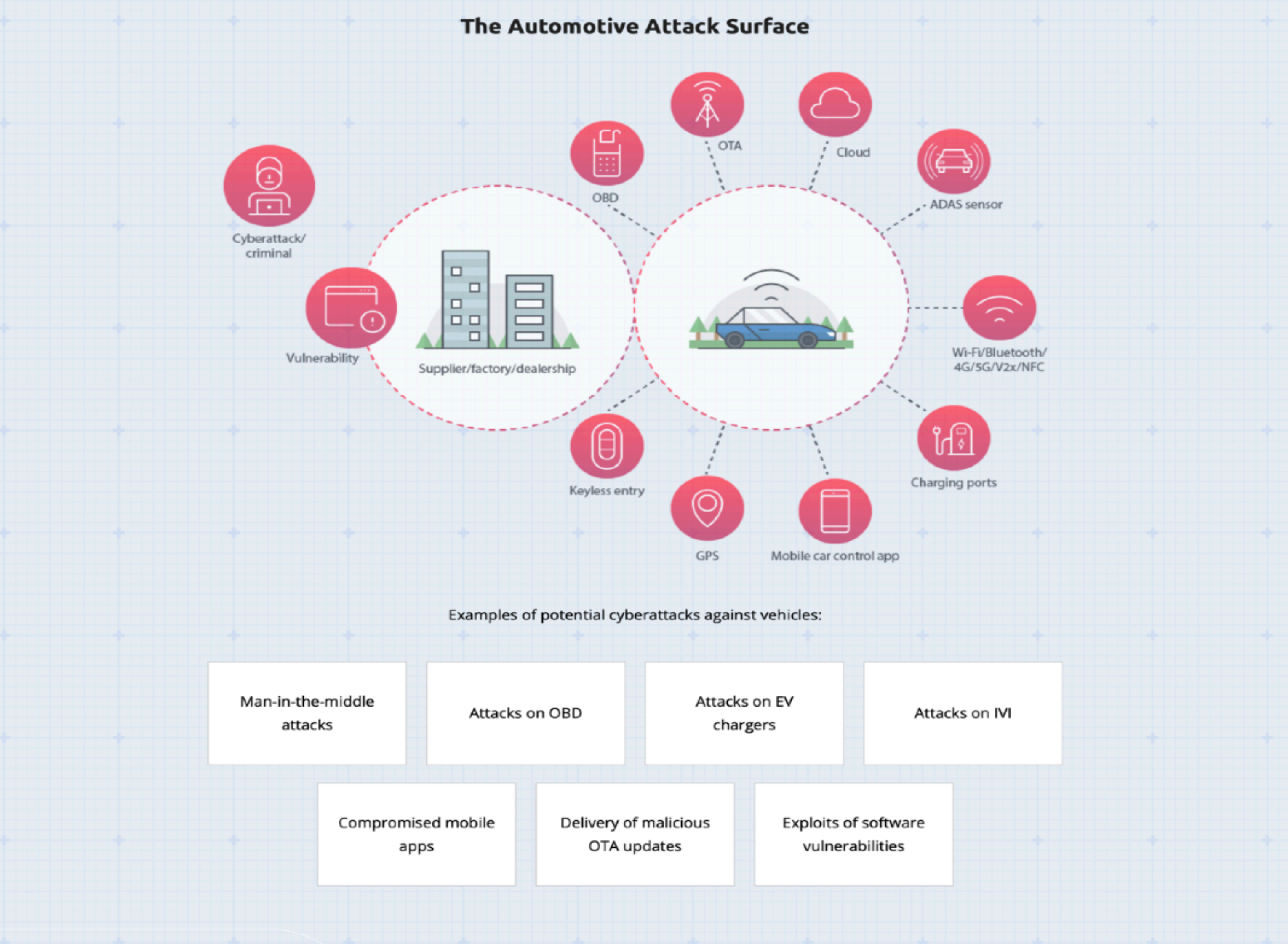
LE MINACCE INFORMATICHE



ATTACK VECTOR *Pathway a malicious actor takes to access a targeted system*	**TARGET** *System a malicious actor seeks to exploit*	**CONSEQUENCE** *Harm resulting from an attack; classifies overall intent*	**OUTCOME** *Real-world result caused by the attack*
ENTERPRISE LEVEL RISK	**COMPROMISING AV NETWORK SECURITY**		
Malicious actor **gains unauthorized access to a network**, such as via a control room, and uses a USB to introduce malware	**Connected AVs and privileged networks** are targeted	**Proprietary and sensitive information could be disclosed** and connected assets could become inaccessible	Compromised company data and connected AV assets could result in **operational impacts and financial losses**
ENTERPRISE LEVEL RISK	**EXPLOITING AV SUPPY CHAIN VULNERABILITIES**		
Malicious actor **works with an insider at a third-party supplier** to nefariously modify data processing motherboards	External device could **remotely load malware** targeting networks and AV driving control, autonomy, and security systems	**Proprietary or sensitive information could be disclosed** and AVs could cease to function properly	Inoperable AVs could lead to **cascading supply chain impacts** and compromised data could result in **security/operational impacts and financial losses**
ENTERPRISE LEVEL RISK	**REMOTELY DISABLING AV FLEETS**		
Cyber criminal **creates privileged credentials to access an AV fleet's anti-theft system** and marks all vehicles as stolen	**Security systems** are targeted	Impacted AVs could become **inaccessible, stolen, or subject to tampering**	Compromised AVs cease to operate properly, causing **operational/supply chain disruptions and financial losses**
ASSET LEVEL RISK	**DISRUPTING AV SENSORS**		
Malicious actor **uses paint and reflective stickers to alter information an AV relies on** to gauge its surroundings, such as a stop sign	**AV hardware sensors and hardware sensor inputs** are targeted and could cease to function properly	**AV could malfunction** and performance could be degraded	AV malfunction could cause **a collision involving people or property, disrupt traffic patterns, or could cease to operate**
ASSET LEVEL RISK	**KEYLESS RELAY THEFT**		
Malicious actor near a corporate facility or AV fleet yard **intercepts the keyless entry signal to an AV** to gain access to the vehicle	**Driving control systems and security systems** are targeted	Impacted AVs could become **inaccessible, unreliable or inoperable due to tampering, or stolen**	Assets could be stolen, resulting **in financial losses**, or AVs could **become inaccessible or cease to operate properly**
ASSET LEVEL RISK	**AV RAMMING ATTACK**		
Malicious actor **gains access to an AV's On-Board Diagnostic (OBD-II) port**, uploads malware to bypass primary systems, and assumes remote control of the AV	**Driving control systems and security systems** are targeted	**Impacted AVs could become inaccessible** and the owner could be unable to regain control to prevent an attack	Compromised AVs could be **stolen, used to cause an accident, used to target public gathering spaces, or used for malicious cargo delivery**

CISA | DEFEND TODAY, SECURE TOMORROW

L’AMBIENTE CIRCOSTANTE

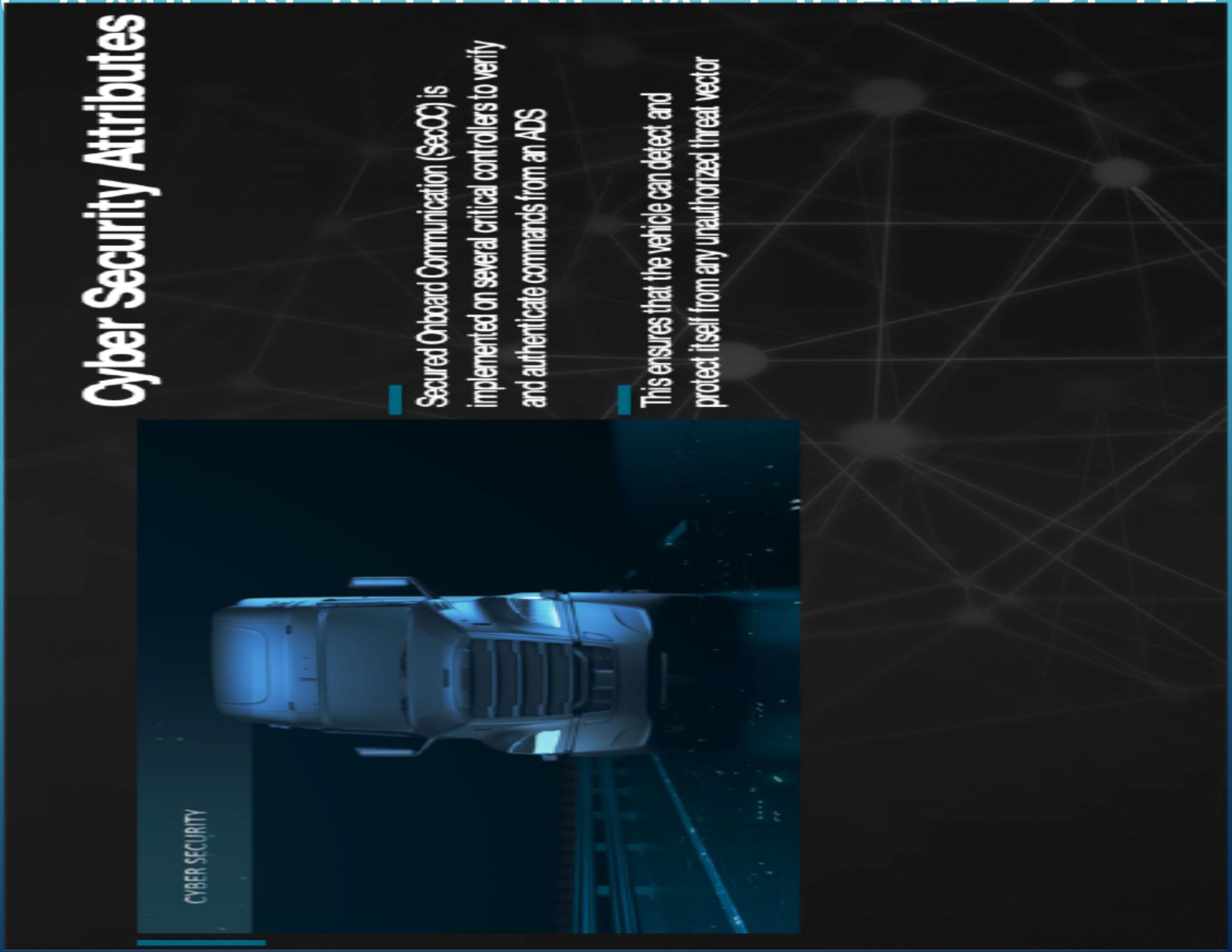


The Automotive Attack Surface

Examples of potential cyberattacks against vehicles:

- Man-in-the-middle attacks
- Attacks on OBD
- Attacks on EV chargers
- Attacks on IVI
- Compromised mobile apps
- Delivery of malicious OTA updates
- Exploits of software vulnerabilities

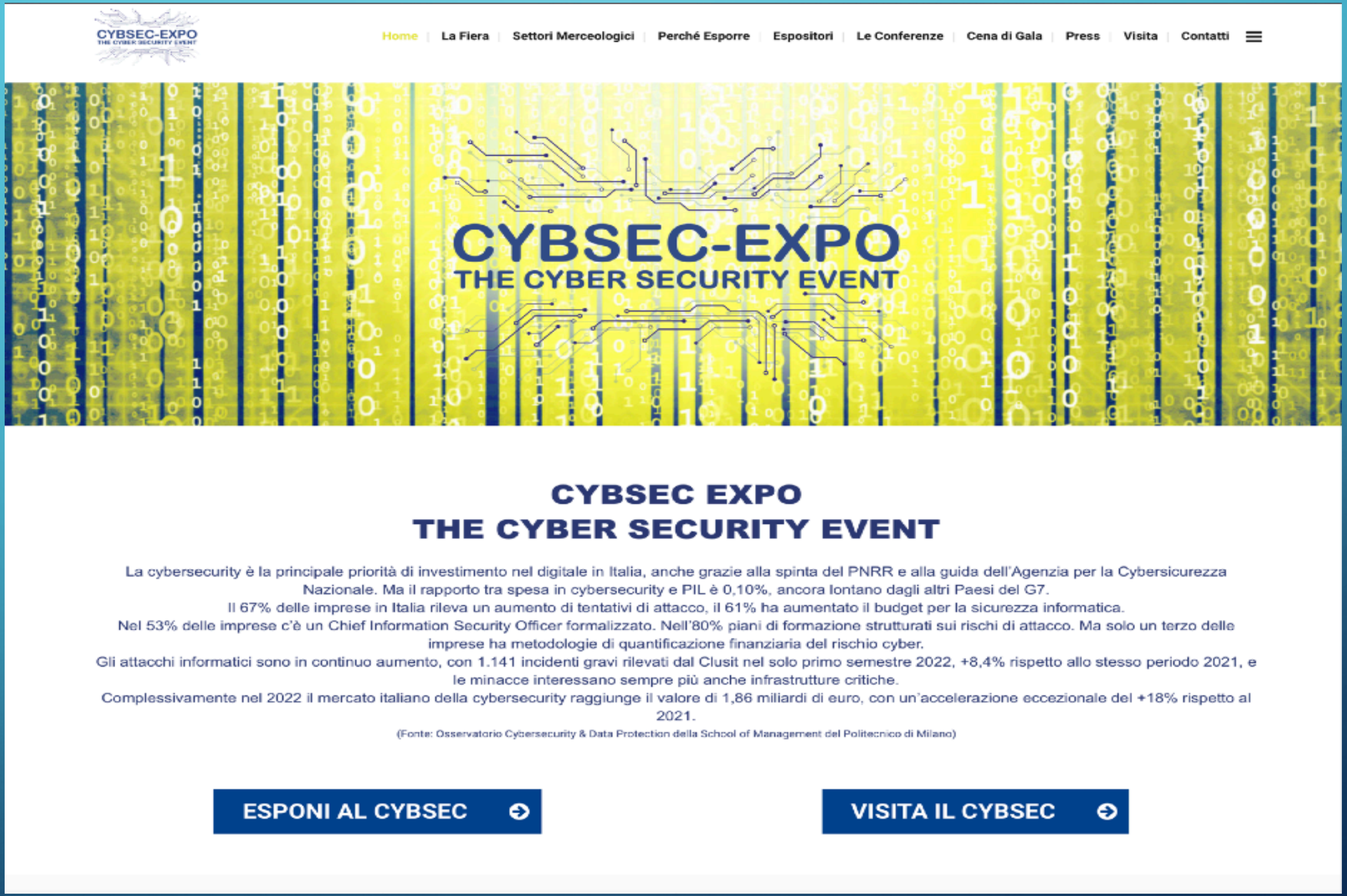
COME IL CAMION AUTONOMO VIENE PROTETTO



Cyber Security Attributes

- Secured Onboard Communication (SecOC) is implemented on several critical controllers to verify and authenticate commands from an ADS
- This ensures that the vehicle can detect and protect itself from any unauthorized threat vector

GRAZIE DELL'ATTENZIONE E BUON CYBSEC-EXPO



CYBSEC EXPO
THE CYBER SECURITY EVENT

La cybersecurity è la principale priorità di investimento nel digitale in Italia, anche grazie alla spinta del PNRR e alla guida dell'Agenzia per la Cybersicurezza Nazionale. Ma il rapporto tra spesa in cybersecurity e PIL è 0,10%, ancora lontano dagli altri Paesi del G7.

Il 67% delle imprese in Italia rileva un aumento di tentativi di attacco, il 61% ha aumentato il budget per la sicurezza informatica.

Nel 53% delle imprese c'è un Chief Information Security Officer formalizzato. Nell'80% piani di formazione strutturati sui rischi di attacco. Ma solo un terzo delle imprese ha metodologie di quantificazione finanziaria del rischio cyber.

Gli attacchi informatici sono in continuo aumento, con 1.141 incidenti gravi rilevati dal Clusit nel solo primo semestre 2022, +8,4% rispetto allo stesso periodo 2021, e le minacce interessano sempre più anche infrastrutture critiche.

Complessivamente nel 2022 il mercato italiano della cybersecurity raggiunge il valore di 1,86 miliardi di euro, con un'accelerazione eccezionale del +18% rispetto al 2021.

(Fonte: Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano)