SECURE ELEMENTS
INTEGRATING SECURE MOBILITY SOLUTIONS

Securing Tomorrow's Mobility
with AI-Powered ✦ Cyber Intelligence

Automotive Cybersecurity Controls

Software Defined Vehicles - Ethernet Security

info@secureelements.co.uk | www.secureelements.co.uk

SDV Architecture

Software-Defined Vehicles (SDVs) are transforming the automotive industry by shifting from traditional, ECU-heavy architectures to centralized, software-driven platforms. This transition is powered by Ethernet-based communication, which offers the bandwidth and scalability needed to support data-intensive applications such as autonomous driving, ADAS, and over-the-air updates. Modern SDVs integrate zonal controllers, which consolidate functions from nearby ECUs and connect to a central High-Performance Compute (HPC) unit that manages key software services across the vehicle. Legacy ECUs are still supported via gateways, enabling hybrid networking during this transition phase. However, the expanded Ethernet topology introduces new cyber risks, including exposure to man-in-the-middle attacks, data tampering, and unauthorized access. As a result, Ethernet security mechanisms such as MACsec, IPsec, and SECOC are being deployed to protect in-vehicle networks. These safeguards ensure that the growing complexity of SDVs does not compromise safety, enabling secure and reliable operation in increasingly connected automotive environments.

Security is critical in SDVs due to the increasing attack surface introduced by Ethernet connectivity, cloud integration, and remote OTA update capabilities. A single vulnerability in zonal gateways or central compute platforms can compromise the entire vehicle system. This makes it essential to embed security from the ground up—ensuring confidentiality, integrity, and authenticity of data across all communication paths.

Secure Elements plays a pivotal role in supporting OEMs and Tier-1 suppliers by delivering tailored engineering services, proof-of-concepts (PoCs), and security consulting. Our offerings include secure Ethernet stack integration, implementation of MACsec/IPsec, SECOC validation, key management, and IDPS design. We help automotive clients align with global regulations such as AIS 189 (India), UNECE R155, and security standards like ISO/SAE 21434. By partnering with Secure Elements, automotive manufacturers gain access to domain expertise and ready-to-integrate security solutions, accelerating their journey toward compliant, secure, and resilient Software-Defined Vehicles.

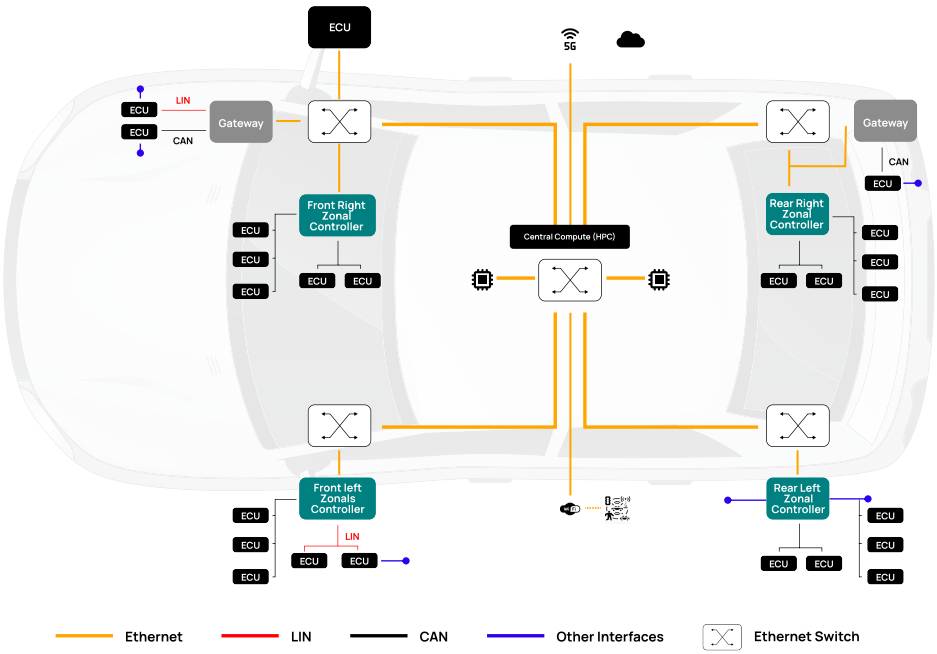
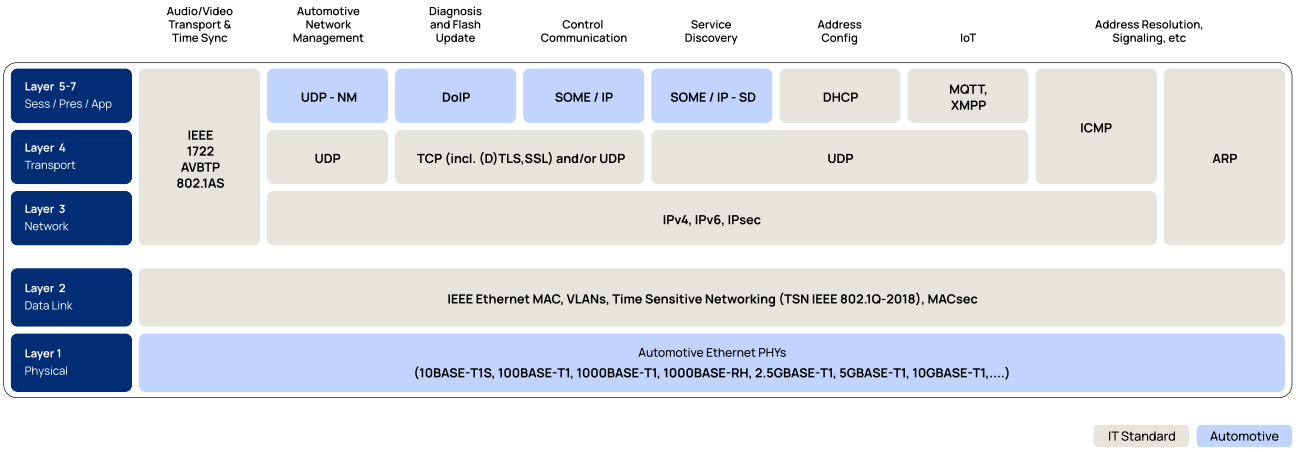


Figure 1: Next generation automotive architecture

1. OSI Layer - Automotive Ethernet

The OSI (Open Systems Interconnection) model defines a standardized framework of seven layers to enable interoperable communication between systems. In automotive Ethernet, protocols like SOME/IP operate at the application layer to handle service-oriented communication, while its companion SOME/IP-SD provides service discovery capabilities for ECUs. DoIP functions over IP at the application layer to enable diagnostics over Ethernet.



MACsec ensures secure data at the data link layer by providing Layer 2 encryption and integrity, while IPsec operates at the network layer to secure IP packets via encryption and authentication. Together, these protocols enhance security, diagnostics, and service communication in connected vehicles.

2. Media Access Control Security (MACsec)

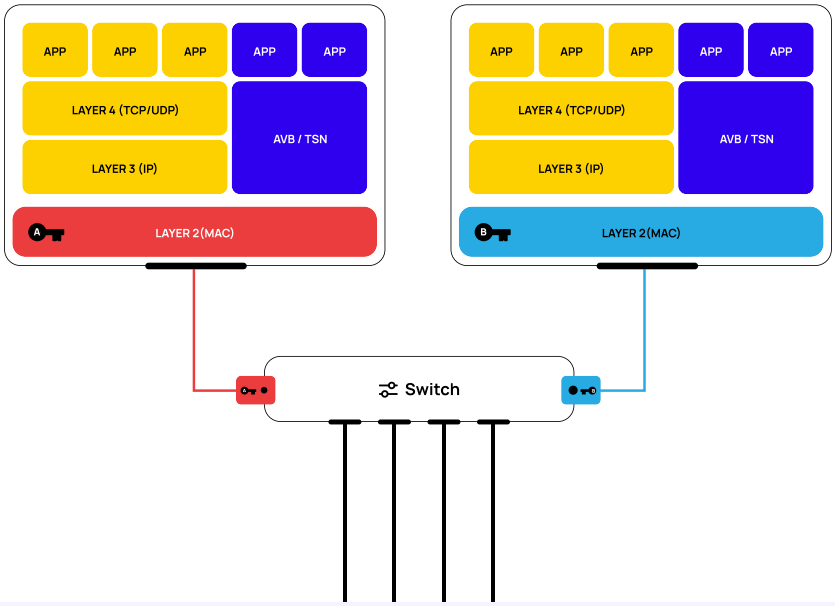
MACsec is the state-of-the-art security solution on Ethernet. It provides integrity protection, replay protection, and optional confidentiality protection for nearly all frames transported on Ethernet. In contrast to other available solutions, this includes Unicast, Multicast, and Broadcast messages as well as all protocols running over Layer 2.

There are multiple attack surfaces on the vehicle like OBD connector, WiFi network, Head unit, and infotainment system, USB ports etc... As the automotive ethernet vehicle network communication is based on the OSI 7-layer model, each layer requires its own protection mechanisms. Some of the widely used approaches are:

- TLS/DTLS is an End-to-End protection that works between 2 applications and is developed for TCP and UDP protocols.
- SecOC (Secure onboard Communication) was developed to protect specifically CAN communication which is not related to any ethernet protocols.
- IPsec is also an End-to-End protection and is dedicated to the IP protocol only.
- MACsec on PHY level in Automotive Ethernet is a recent security approach. It is a Point-to-Point protection. It protects all Ethernet traffic on OSI LAYER 2. The advantage of MACsec for Automotive Ethernet is, that MACsec protects many protocols beyond the IP-protocol family, which are used by Automotive Ethernet.

Point-to-Point Protection

Example: MACsec (Layer 2)



2.1 MACsec Features for Automotive Ethernet

Media Access Control Security (MACsec), specified in the IEEE 802.1AE standard, is designed to provide authentication, confidentiality and integrity for data transportedon point-to-point links in Local Area Network(LAN) using the Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) data cryptography algorithm.

MACsec provides authentication by ensuring that only known nodes / devices are allowed to communicate on the LAN. It provides confidentiality through encryption of the data so only end-points with the correct encryption key can see the contents. Integrity is provided through acryptographic mechanism ensuring that data has not been tampered with while in motion.

2.2 How MACsec works

MACsec operates at the Data Link Layer acting as a client of the Ethernet Media Access Control (MAC) layer. It encapsulates packets with a16-byte MACsec SecTAG header and 16-byte Integrity Check Value(ICV)tail and uses the EtherType (0x88E5) as shown in Figure 3. In the MAC layer, the preamble and Frame Check Sequence (FCS) are added to the Ethernet frame before transmission.

The SecTAG includes a TAG Control Information/Association Number (TCI/AN) field that provides information on whether encryption is used or not, if the optional Secure Channel Identifier (SCI) is used and the SA that is in use.

The SCI specifies the Secure Channel (SC) and is a concatenation of the 48-bit source MAC address and16-bit port identifier. The Short Length (SL) field is only used for short frames, while the Packet Number (PN) can be used to keep track of packet order and detect if packets are missing or delayed.

The TAG Control Information/ Association Number (TCI/AN) specifies if encryption is used.

The Short Length (SL) field specifies the length of the encrypted data if it is a short frame.

The Packet Number (PN) is typically 32bits long, but canbe up to64 bits long when eXtendedPacket Number (XPN) versions areused for higher speedinterfaces.

The Secure Channelldentifier (SCI) specifies the Secure Channel (SC) andis a concatenation of the 48 bit source MACaddress anda16-bit port ID.

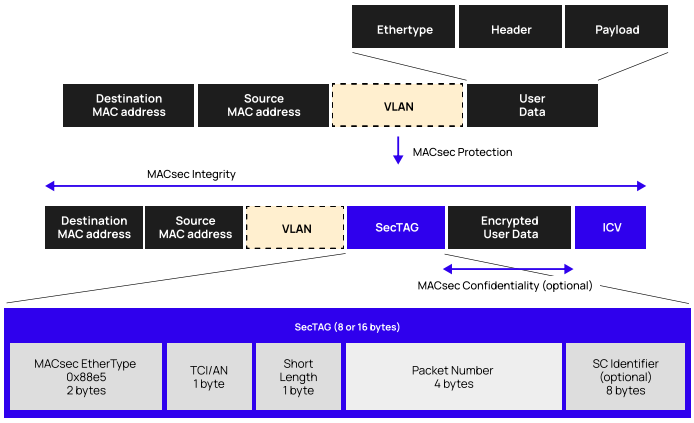


Figure 3: MACsec frame format

2.3 MACsec Authentication

In order for Ethernet-enabled devices to send MACsec frames over the in-vehicle network, they must be authenticated. Authenticated MACsec peers, such as end stations, gateways, or bridges, belong to a Connectivity Association (CA). This basically means that these MACsec peers are connected and are allowed to communicate with each other. Members of the CA identify themselves using a long-lived Connectivity AssociationKey(CAK)with a corresponding Connectivity Association Key Name (CKN).

2.4 Confidentiality

The MACsec frames are transported over virtual, unidirectional, point-to-multipoint Secure Channels (SCs), which are supported by Secure Associations (SAs). As defined by the 802.1AE standard, a “SecY “is the entity that operates the MACsec protocol on a network port. There can be one or more SecY instances on any physical port, but the SecY instance is associated with a specific virtual port. Each SecY and virtual port will have one transmit-SC, and can have multiple receive-SCs. Each receive-SC corresponds to each peer associated with the SecY. Each transmit-SC and receive-SC can have up to four SA. Each SA uses a separate SAK to encrypt and authenticate frames.

2.5 Integrity

MACsec not only encrypts data, but also provides integrity through an Integrity Check Value (ICV)whichis a cryptographic digest function dependent on the data and the SAK. Because of this, an attacker cannot tamper with the data without the encryption key.

3. SecOC Features for Automotive

AutoSAR (Automotive Open System Architecture) SecOC (Security On-board Communication) is a security architecture that aims to protect the communication between the various electronic control units (ECUs) within a vehicle against cyber-attacks.

- SecOC is an AUTOSAR module
- Provides integrity and authentication for messages (PDUs)
- Freshness protects against replay attacks
- Generic specification which can operate with asymmetric or symmetric cryptography
- Key distribution is not specified
- Every PDU has a unique identifier (SecOCDataID).

- On CAN networks, the CAN identifier is used.
- On Ethernet networks, the PDU identifier or internal mappings for PDU identifier to SecOCDataIDs are used.

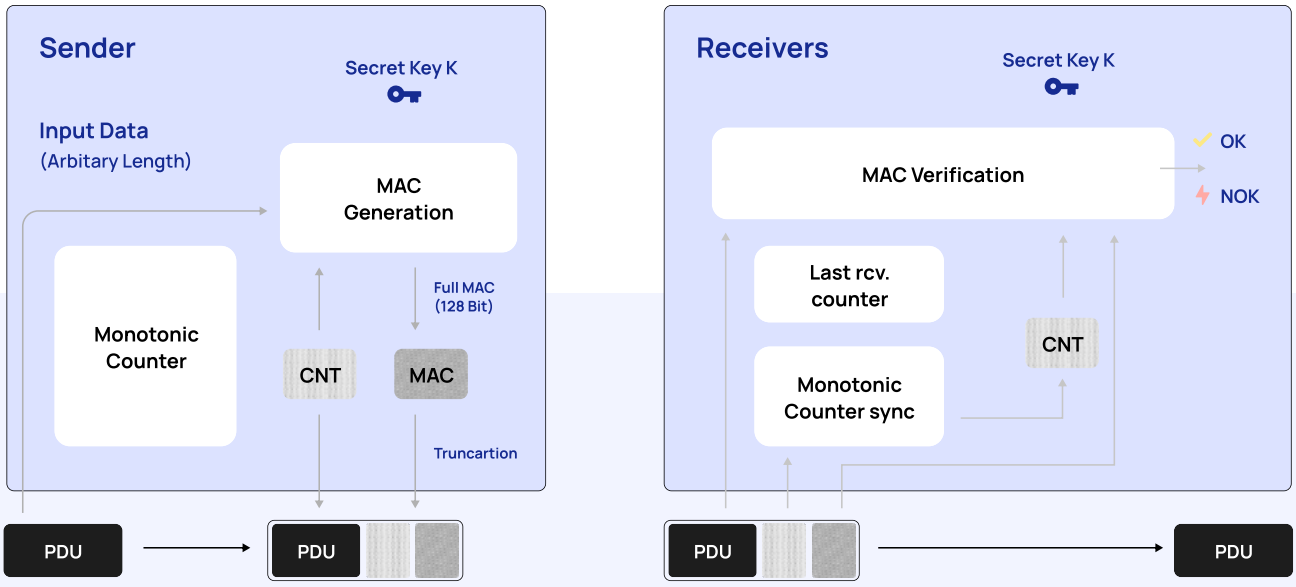


Figure 4: SecOC Communication

4. Internet Protocol Security (IPsec)

IPsec is a network layer protocol suite

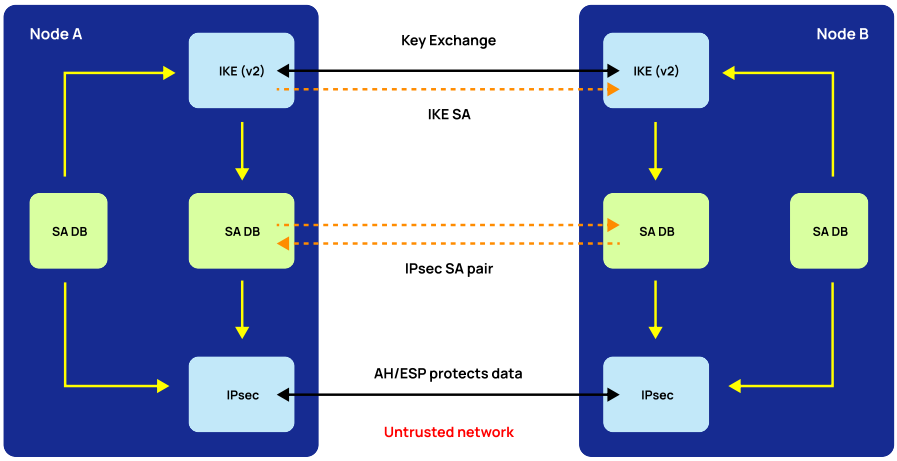


Figure 5: IPSEC

that secures network connections by encrypting or authenticating IP packets. It constitutes a part of IP protocol suite. IPsec consists of three elementary components: Internet Key Exchange- most widely used module for key management Authentication Header- (IP protocol 51) for integrity Encapsulating Security Payload- (IP protocol 50) for integrity and confidentiality.

5. vSOME/IP for Automotive

SOME/IP is an abbreviation for "Scalable service-Oriented middlewarE over IP". This middleware was designed for typical automotive use cases and for being compatible with AUTOSAR (at least on the wire-format level).

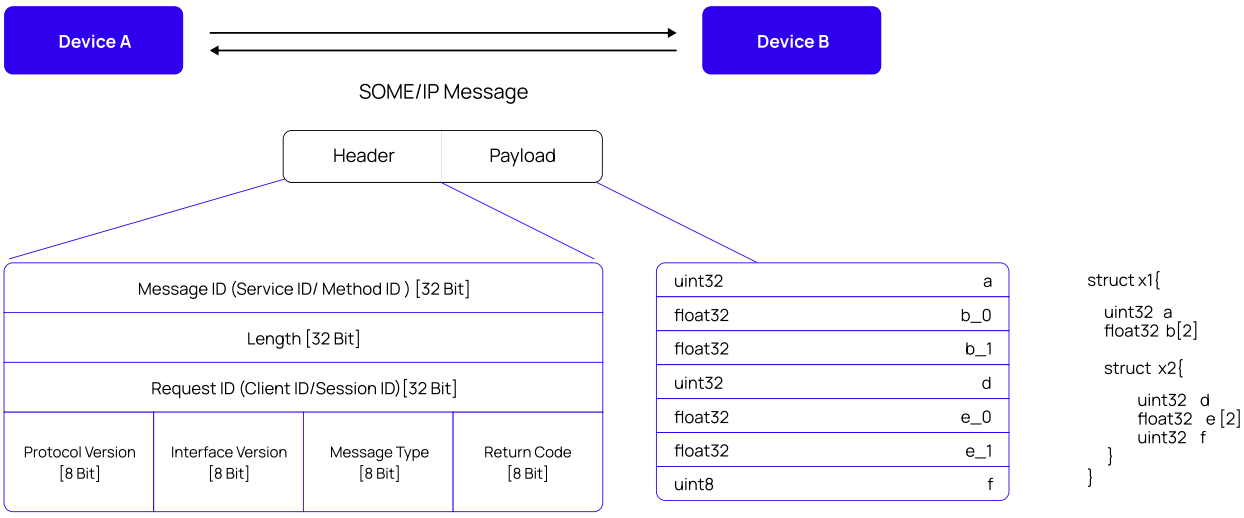


Figure 6: Automotive vSOME/IP Format

Comparison of IVN Communication Protocols

Automotive Protocols & Parameters	CAN-FD	LIN	FlexRay	MOST	Ethernet
Media	Unshielded Twisted Pair	1 Wire	2 or 4 Wires	Fibre Optic, UTP, cables, coax, cables.	UTP
Topology	Bus	Bus	Star, bus	Ring	Star
Access	Priority Based Messages	Master-slave with schedule tables	TDMA	Slave, controller and HMI (Human Machine Interface)	Switched point-to-point link
Data Transfer Rate (Mbps)	1 Mbps/16 Mbps	0.02	2.5-10	14-25	1000
Noise Immunity (dB)	20-25	20-25	>25	>70	>70
Cable length (m)	40-1000	40	40-200	50-1500	15-40
Maximum Power Consumption (mA)	50	20	200	500	1000
Max. Nodes	16 (at 500 kbps)	16 (1 Master 15 Slaves)I	22 (bus), 22/64(star), 64 (mixed)	Upto 64	256 to theoretically unlimited
Implementation cost	Low	Low	Low	High	High
Communication	Signal-based	Signal-based	Signal-based	Signal-based	Service-oriented based
Scalability	Low	Low	Medium	High	High
Security Modules	SecOC (Secure Onboard Communication)	--	SecOS	No information	Media Access Control security (MACised), IPsec, TIS/ DTLS, SecOC
Application	Transmitting critical information, such as engine data, safety information, and diagnostic	Door locks, mirrors, and seat controls	Safety-critical applications such as steering and braking	Connecting multimedia devices such , rear-seat entertainment systems, and other infotainment components.	Multimedia applications, autonomous driving and safety, such as the ADAS.

Conclusion

Secure Elements is a trusted cybersecurity engineering company dedicated to supporting automotive OEMs and Tier-1 suppliers in building secure-by-design vehicles. With deep domain expertise in automotive CAN and Ethernet protocols and security architectures, Secure Elements offers specialized engineering services and proof-of-concept (PoC) delivery to integrate and validate technologies such as vSOME/IP, SECOC, IPsec, and MACsec within automotive E/E architectures.

vSOME/IP (vehicle Scalable service-Oriented MiddlewarE over IP) is rapidly becoming the backbone of service-based communication in next-generation vehicle networks. Secure Elements provides full-stack integration support for vSOME/IP and its Service Discovery (SD) features, ensuring interoperability, scalability, and robustness in service communication between Electronic Control Units (ECUs).

To protect this communication, SECOC (Secure Onboard Communication) adds message authentication and freshness counters. Secure Elements has hands-on experience integrating SECOC modules with AUTOSAR Classic and Adaptive stacks, ensuring seamless end-to-end security for safety-critical applications like ADAS, powertrain, Phone as a Key Module etc.

Beyond ECU-level security, IPsec and MACsec offer layered protection across IP and Ethernet respectively. Secure Elements supports automotive cybersecurity teams in implementing IPsec for encrypted and authenticated IP communications, particularly for over-the-air updates, diagnostics, and V2X scenarios. Similarly, MACsec ensures secure Ethernet frame transmission, helping OEMs comply with ISO/SAE 21434 and AIS 189 by preventing man-in-the-middle and eavesdropping attacks on in-vehicle networks.

Secure Elements delivers tailored PoCs to evaluate performance, integration overhead, and security impact of these technologies. In parallel, our engineering services extend to Key Management Systems and Intrusion Detection Systems (IDS) for CAN and Ethernet-based networks.

With a proven track record, Secure Elements empowers automotive companies to accelerate secure product development, meet compliance requirements, and future-proof their platforms against evolving cyber threats. Our mission is to deliver embedded security excellence—by design, by default, and by deployment.

To get more technical details and insights write to info@secureelements.co.uk or visit www.secureelements.co.uk

Threats Evolve. So Do We

CRISKLE©

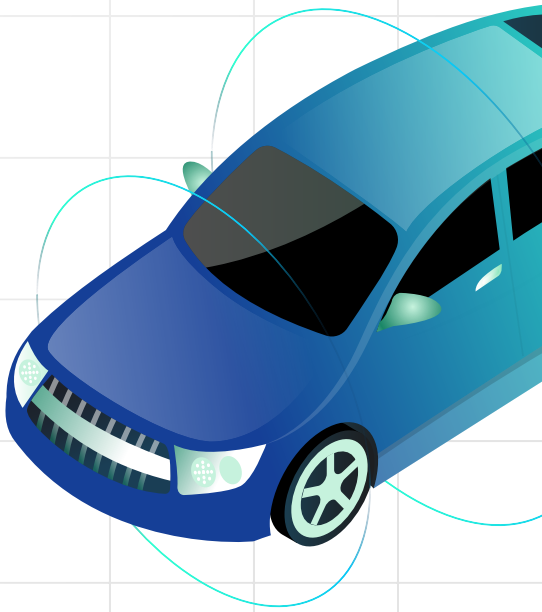
A GenAI Powered, Integrated Safety and Security Engineering Application

CRISKLE© MSOC

An Integrated Mobility Security Operations Centre

The **Smart Choice** for Software Defined Vehicles Cybersecurity!

www.secureelements.co.uk



SECURE ELEMENTS
INTEGRATING SECURE MOBILITY SOLUTIONS

info@secureelements.co.uk
www.secureelements.co.uk

Bengaluru, India
Coventry, UK