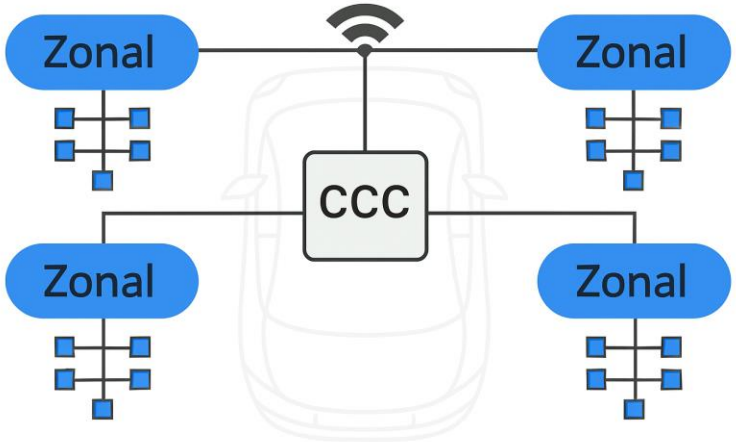
15 May 2025

面向下一代网联汽车的全车网络安全平台化框架

Platform-Based Full-Vehicle Cybersecurity Framework for Next-Gen Connected Vehicles

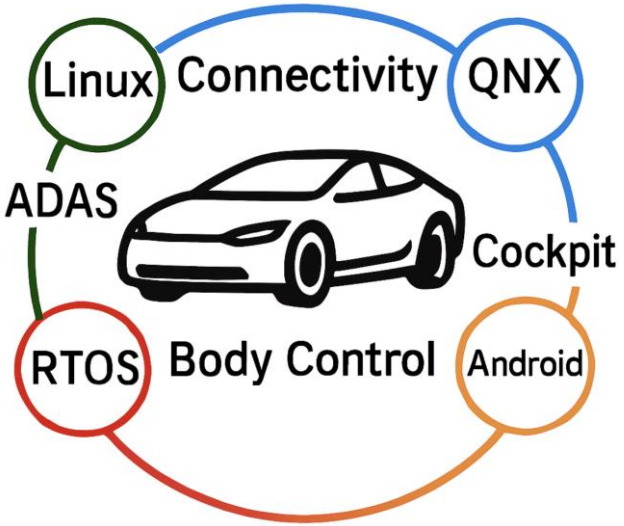
Cybersecurity Challenges for Next-Gen Connected Vehicles

- The E/E architecture is rapidly transforming toward a centralized architecture with the Center Computing Cluster + Zonal controller.
- The 'Strong central + zonal distribution' model has become the mainstream development direction for intelligent vehicle E/E architecture.



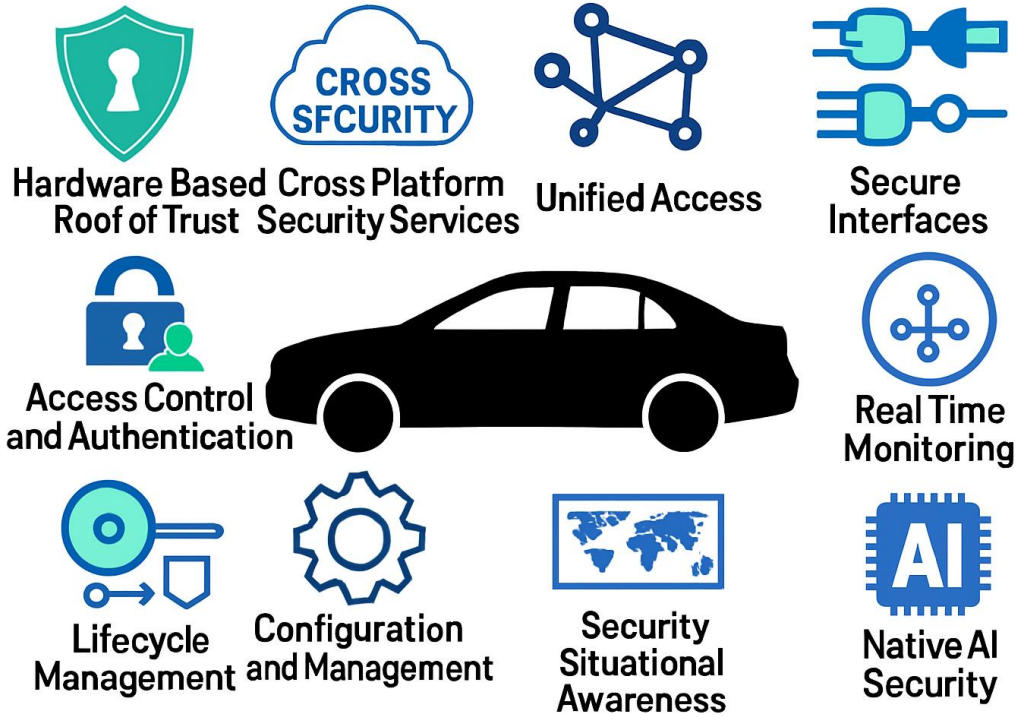
Cybersecurity Challenges for Next-Gen Connected Vehicles

- Modern intelligent vehicles integrate Linux, QNX, AUTOSAR, and Android, creating complex computing platforms. Frequent system interactions and network connectivity expand the attack surface.
- Traditional siloed security approaches are inadequate, with subsystems lacking coordinated protection and unified management.
- Platform-based security frameworks offer the solution through cross-system governance and unified threat response, enabling complete lifecycle security management.

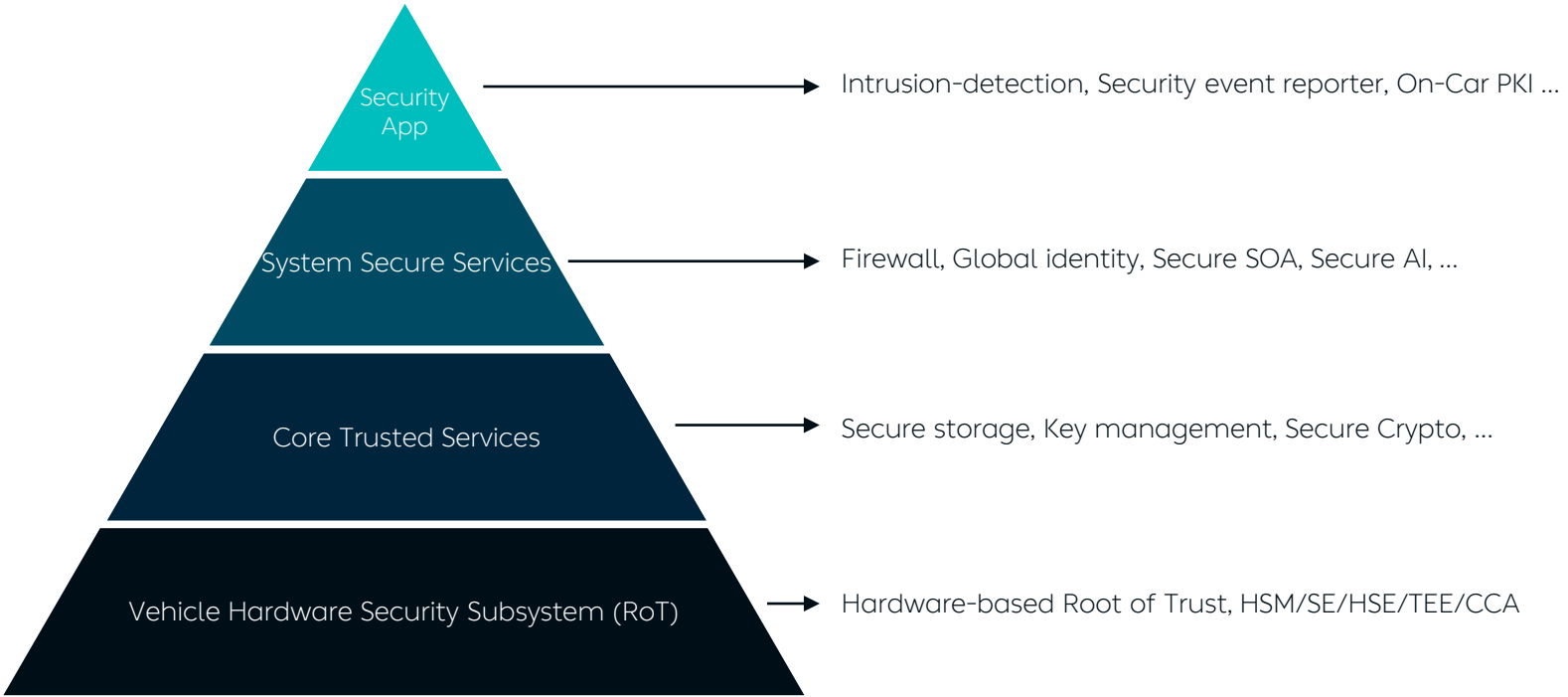


Full-Vehicle Security Framework

- Hardware-based Root of Trust for all vehicle domains
- Cross-platform/system trusted service deployment capability
- Stable and unified security interfaces for vehicle-wide services and applications
- Global access control, identification and authentication
- Security protection for multiple communication interfaces
- Full lifecycle key and certificate management from factory to after-market service
- Real-time monitoring, defense, recording and analysis of security events and abnormal behaviors across all domains
- Providing global configuration and baseline management capabilities for vehicle level security
- Security situational awareness in intelligent connected vehicle scenarios
- Native AI security capabilities



NIO Full-Vehicle Security Framework - SkyShield



Cybersecurity in the AI Era

Model Security

Identity & Access Control

Data Security

Standard & Regulation

Thank You