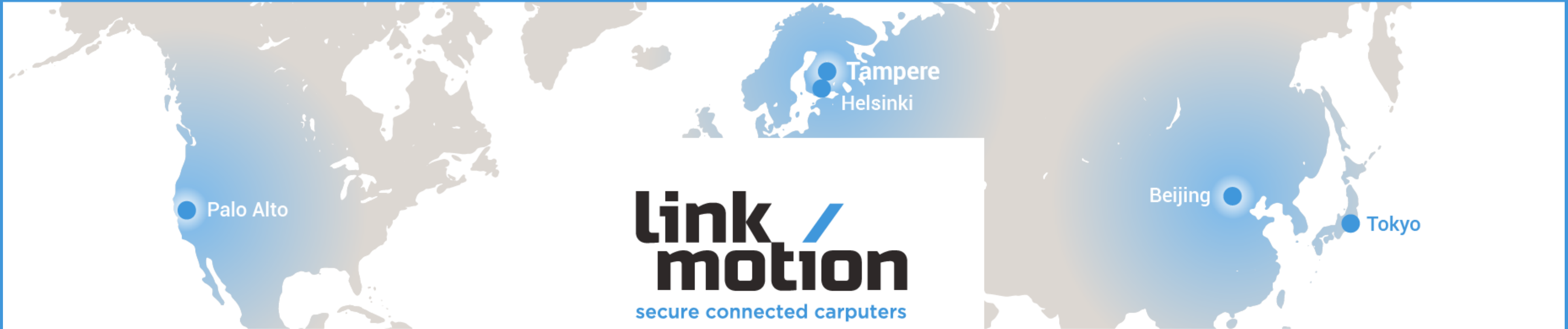
HOW TO CONNECT VEHICLE IN SAFE AND SECURE WAY

MIKKO HURSKAINEN
TECHNOLOGIST

NOMOVOK

link motion



link motion

secure connected carputers

NOMOVOK

17+

YEARS IN EMBEDDED SOFTWARE BUSINESS

200+

AUTOMOTIVE SOFTWARE PROJECTS DELIVERED

70+

TOP NOTCH PROFESSIONALS BUILDING THE PRODUCTS

5

LOCATIONS AROUND THE GLOBE

SHANGHAI OFFICE IN 2017 H2
SHENZHEN OFFICE IN 2017 H2

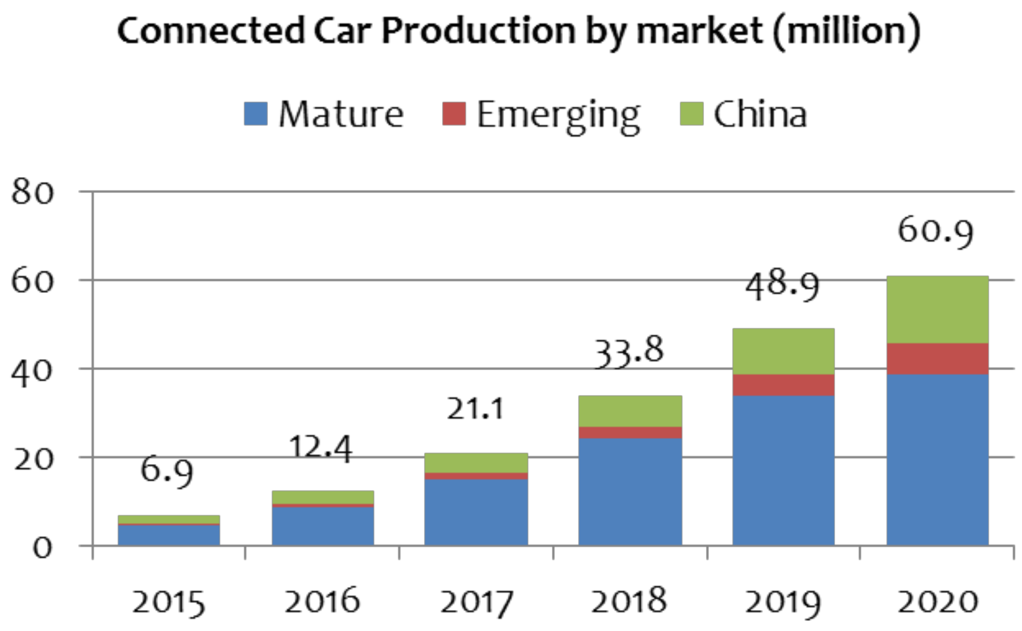
CONTENTS

- Connected vehicles
- What is security?
- Security solutions
- What’s next?

CONNECTED VEHICLES

link motion

CONNECTED VEHICLES

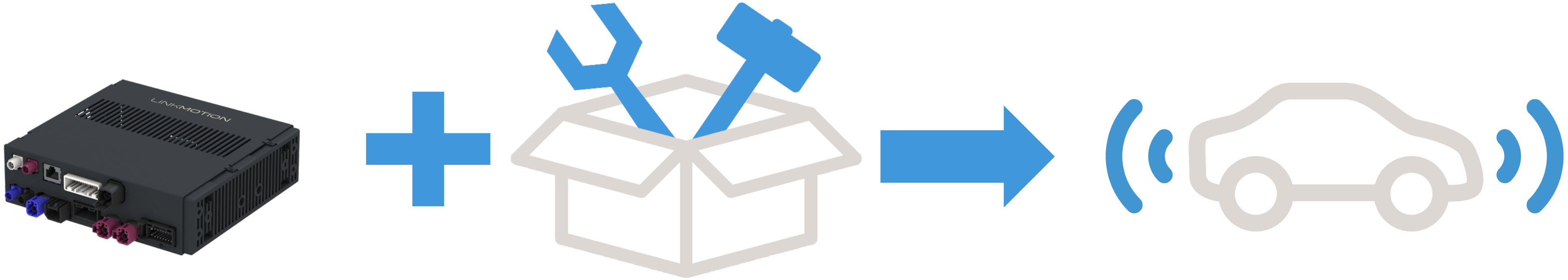


Source: Gartner

- Connected car market is experiencing rapid growth
- There’s a need for secure and safe solutions

link motion

CONNECTED VEHICLE DEVELOPMENT MODEL



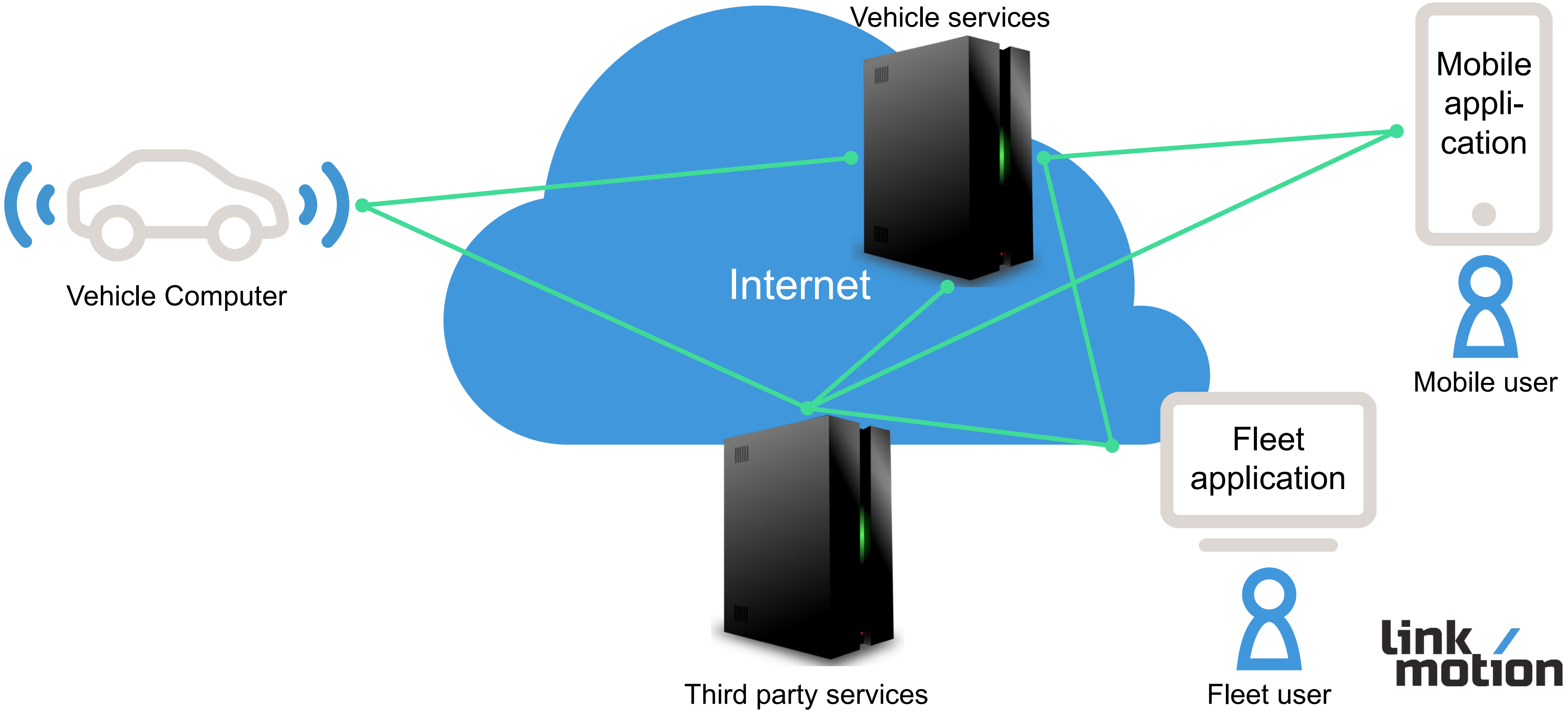
Vehicle Computer and Platform

SDK

Connected Vehicle

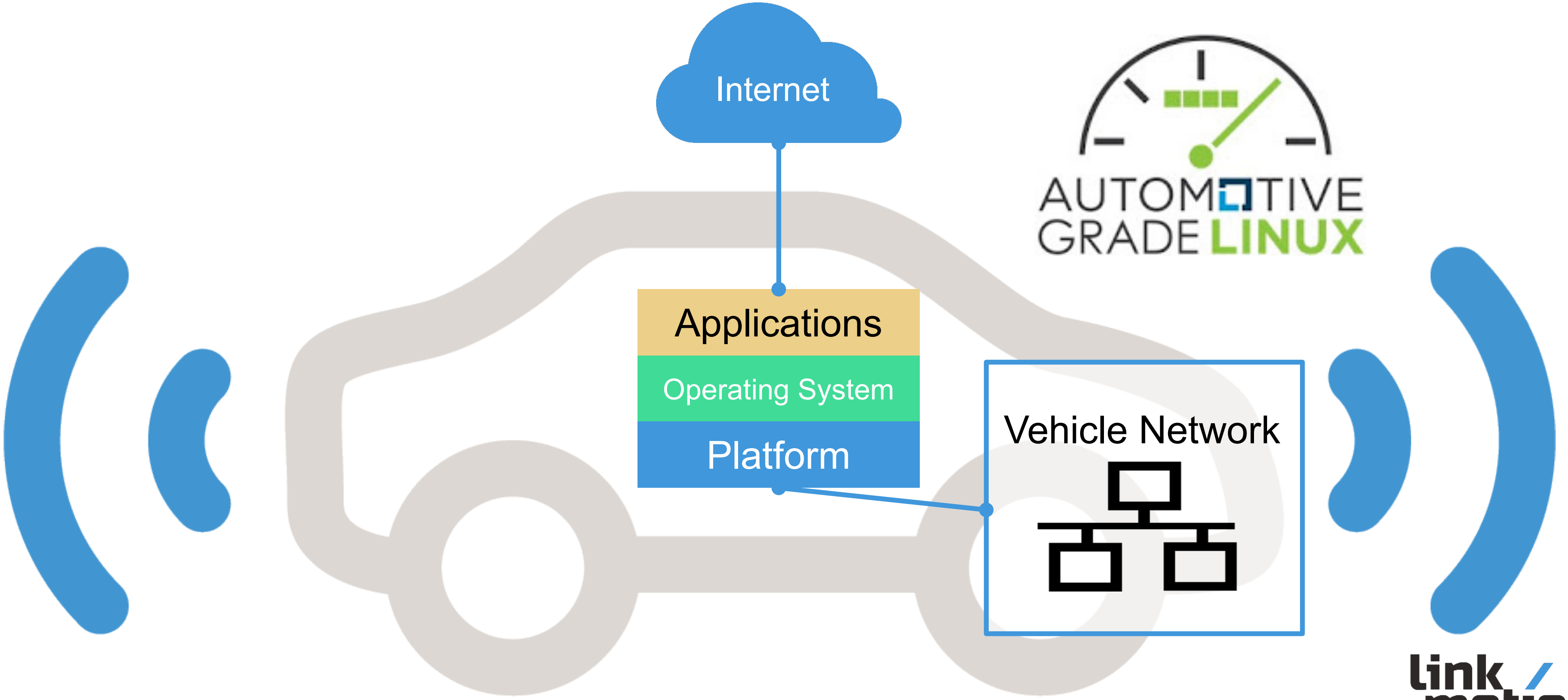
link motion

CONNECTED VEHICLES



link motion

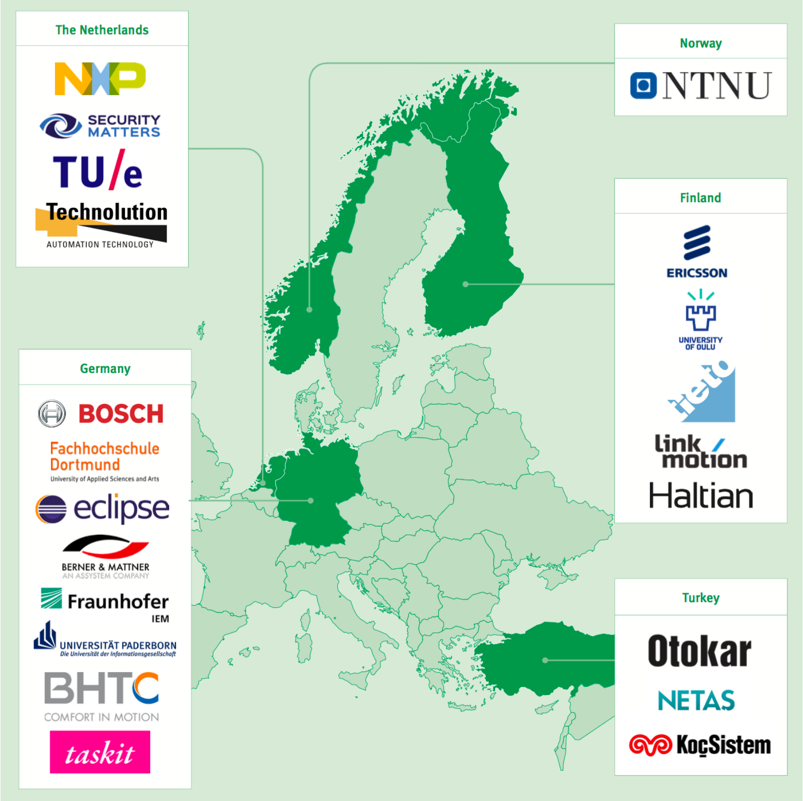
ARCHITECTURE



AUTOMOTIVE GRADE LINUX

link motion

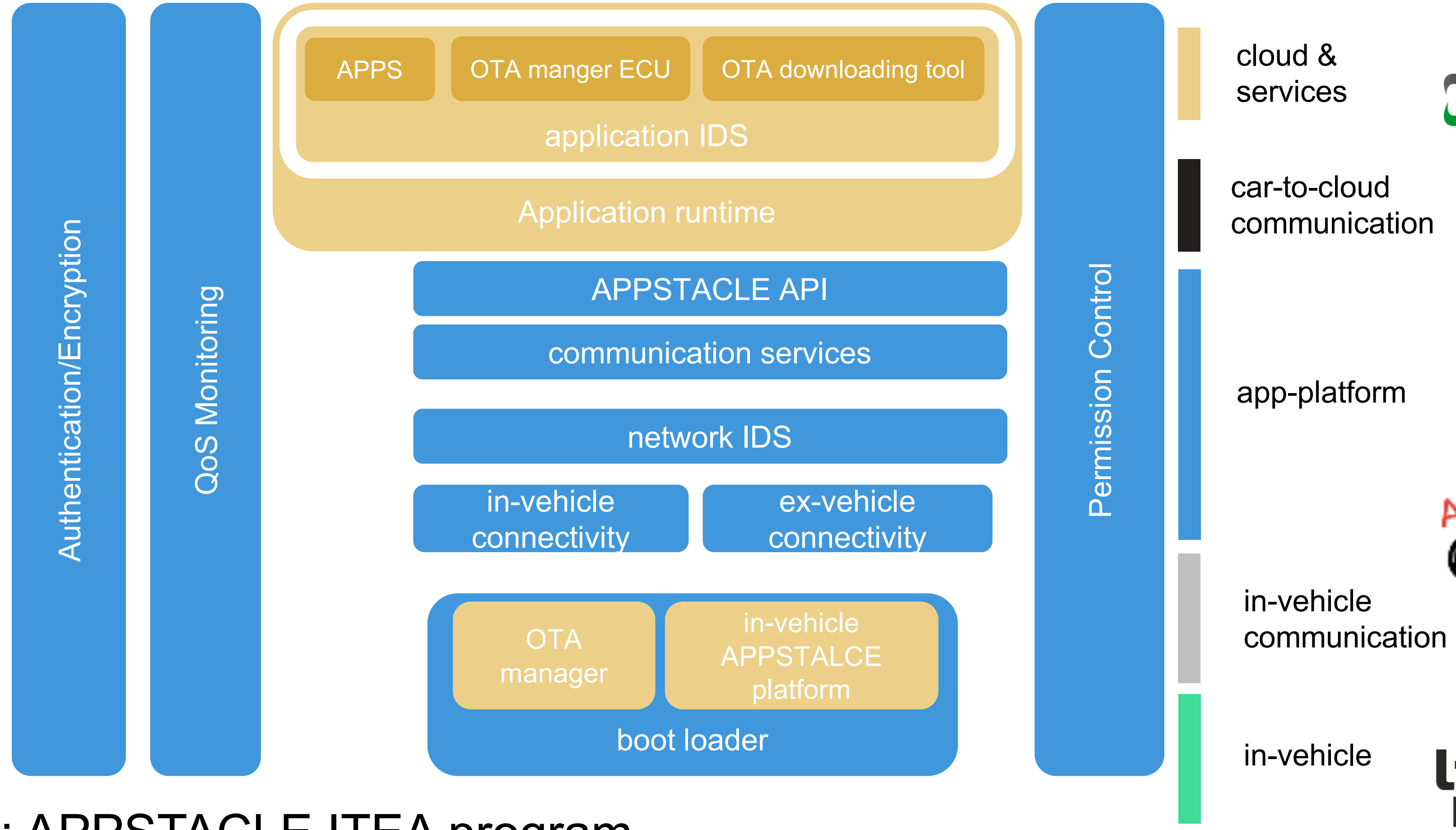
APPSTACLE PLATFORM



- European collaboration project for open connected car architecture
- Link Motion is promoting AGL

link motion

APPSTACLE ARCHITECTURE



Authentication/Encryption

QoS Monitoring

APPS

OTA manger ECU

OTA downloading tool

application IDS

Application runtime

APPSTACLE API

communication services

network IDS

in-vehicle connectivity

ex-vehicle connectivity

OTA manager

in-vehicle APPSTALCE platform

boot loader

Permission Control

cloud & services

car-to-cloud communication

app-platform

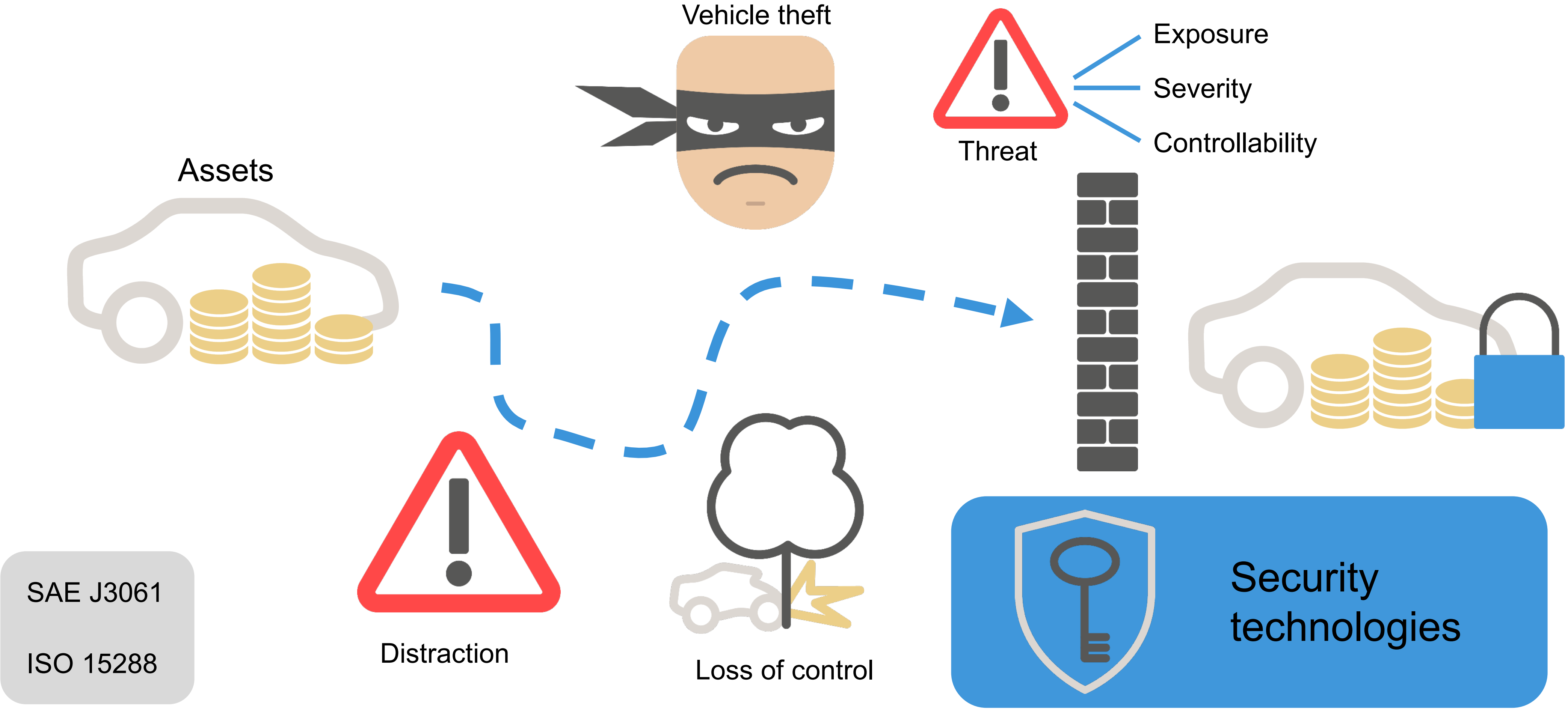
in-vehicle communication

in-vehicle

Source: APPSTACLE ITEA program

WHAT IS SECURITY?

PROTECTION OF ASSETS



Vehicle theft

Threat

Exposure

Severity

Controllability

Assets

Distraction

Loss of control

Security technologies

SAE J3061

ISO 15288

ASSETS

Assets in connected vehicle

- **Data.** If data has been compromised, it can lead to hijacking of vehicle, lost property or manipulation of operation. Examples of data include remote control keys, maintenance data, routing information
- **Privacy.** Lack of privacy can lead to uncomfortable situation or expose user to greater security risks. Examples of privacy assets include location information, route history and consumer habits
- **Control.** Loss of control can lead to unwanted behaviour of vehicle during driving or even hijacking of passengers inside the vehicle. Loss of control also compromises owner’s ability to use car

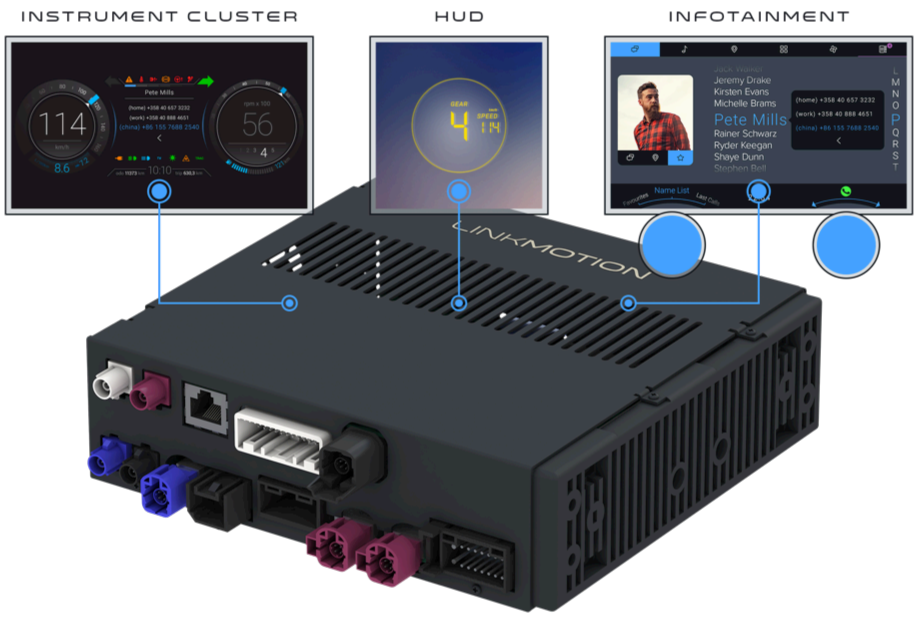
Tangible and intangible

link motion

THREATS

- Ransomware
- Publicized vulnerability
- Leakage of privacy data
- Blocking use of system

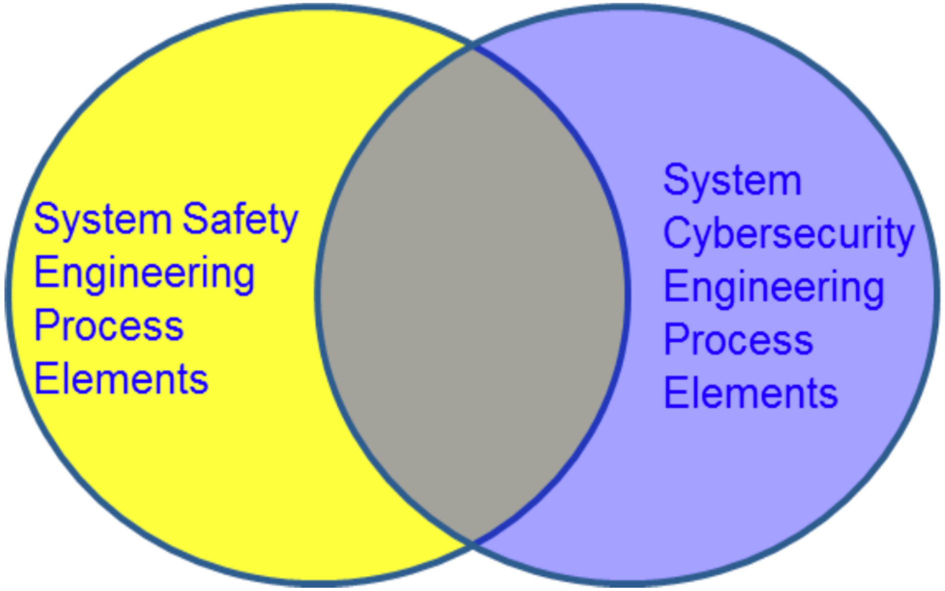
=> Remotely attack fleet



SECURE & CONNECTED

link motion

SAFETY AND SECURITY



System Safety Engineering Process Elements

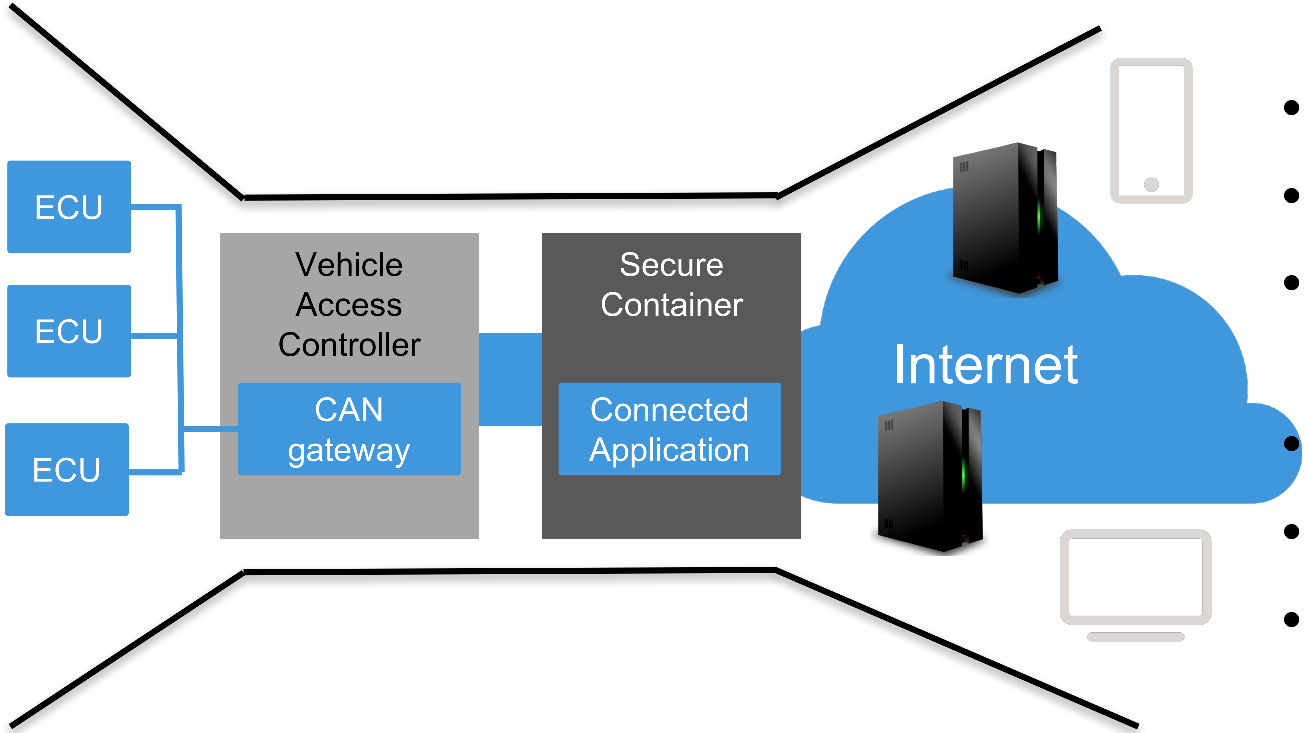
System Cybersecurity Engineering Process Elements

Source: SAE J3061

SECURITY SOLUTIONS

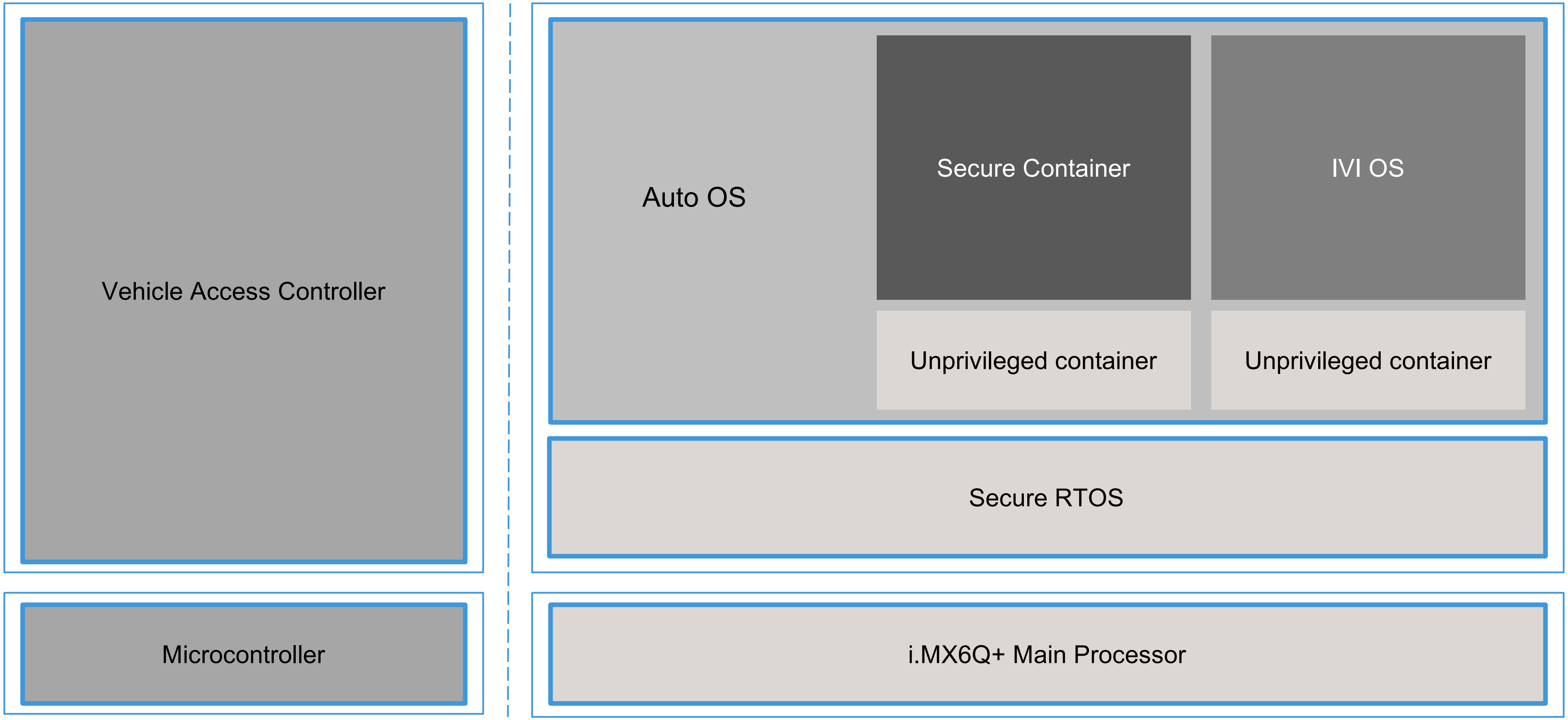
link motion

SECURITY FEATURES



- Modularity and layering
- Hierarchical protection
- Attack surface minimization
- Least privilege principle
- Predicate permission
- Defense-in-depth

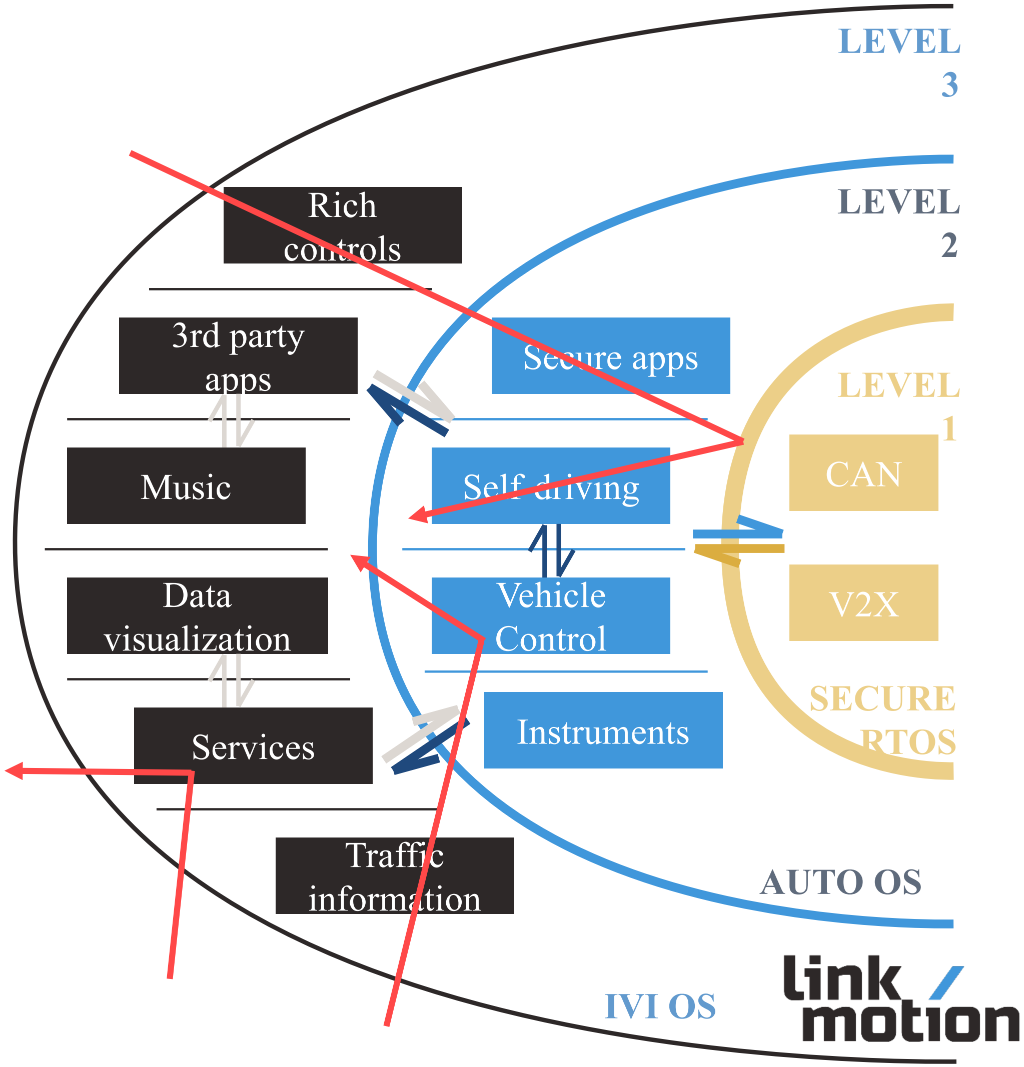
SANDBOXING OF THE SYSTEM



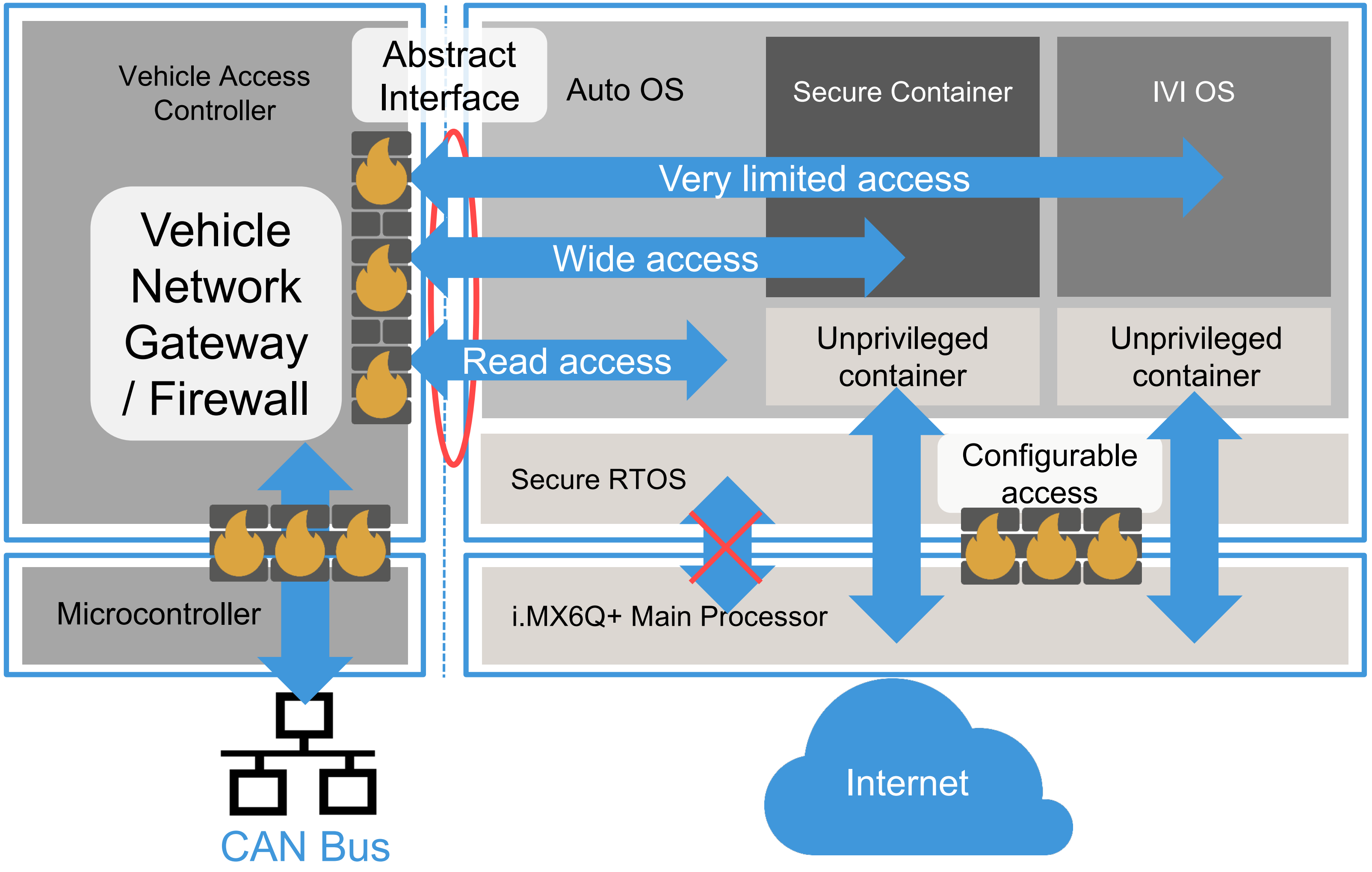
link motion

DEFENSE IN DEPTH

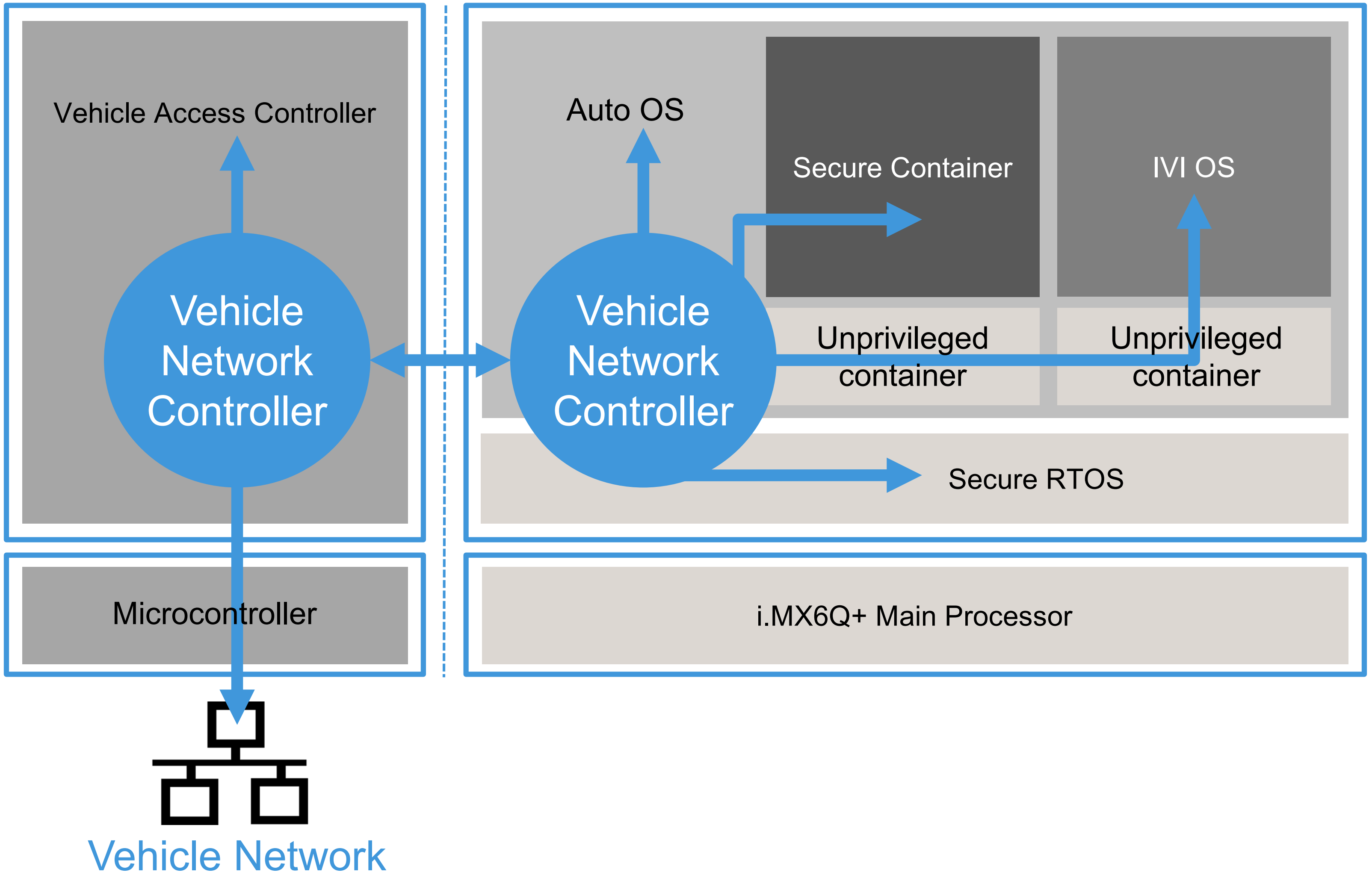
- Minimizes impact of successful attacks
- Allows protection according to needs
- Innermost layer (TCB) is compact and most secure



VEHICLE NETWORK DATAFLOWS



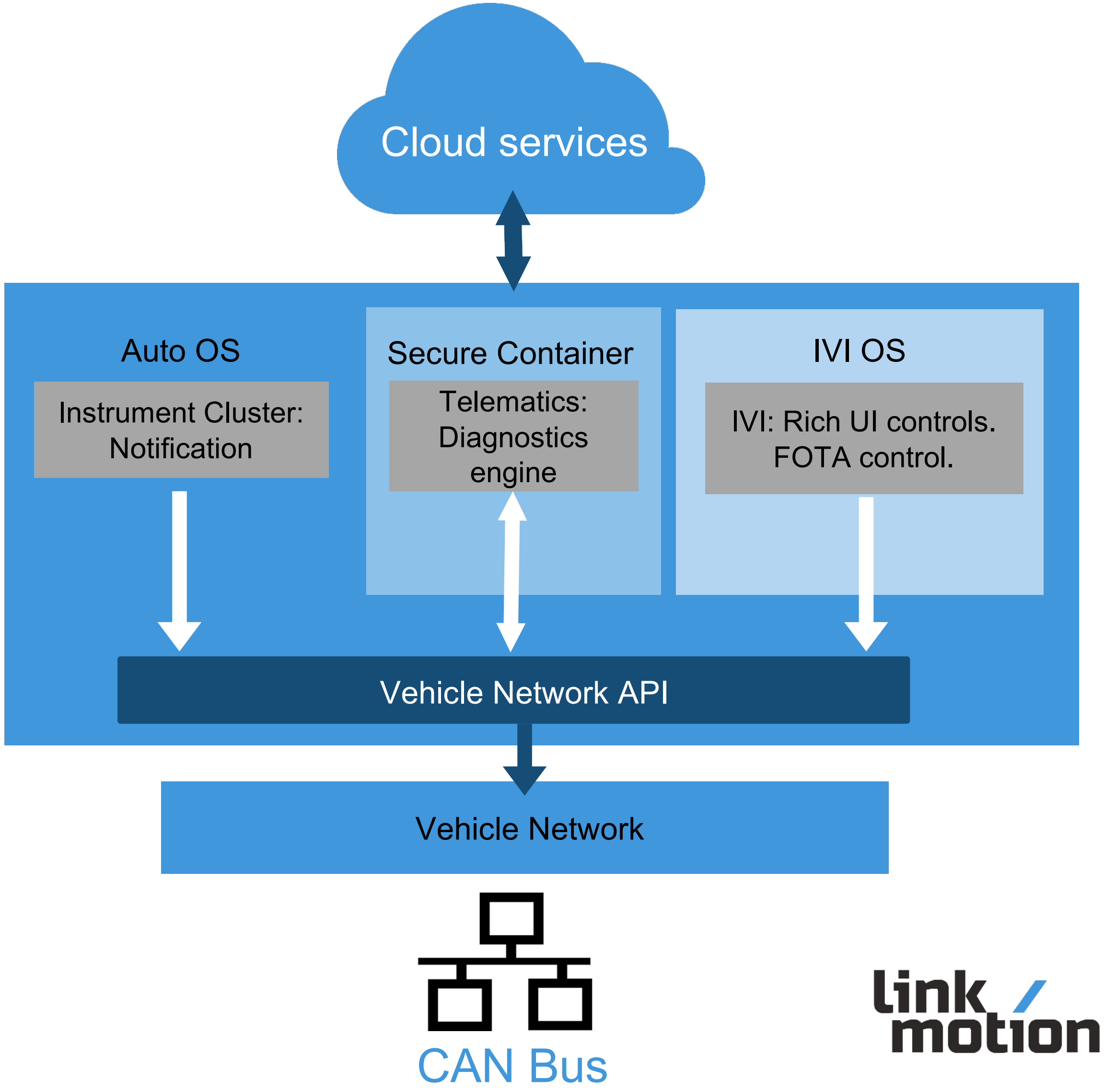
VEHICLE NETWORK CONTROLLED ACCESS



link motion

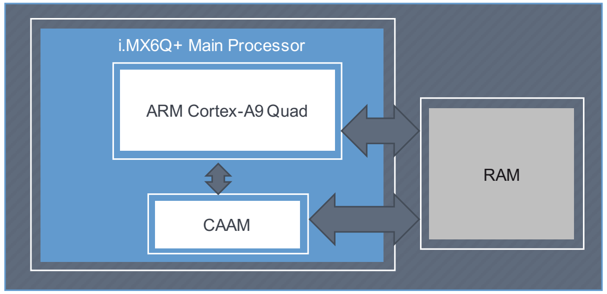
SECURITY MINDED DESIGN PATTERN

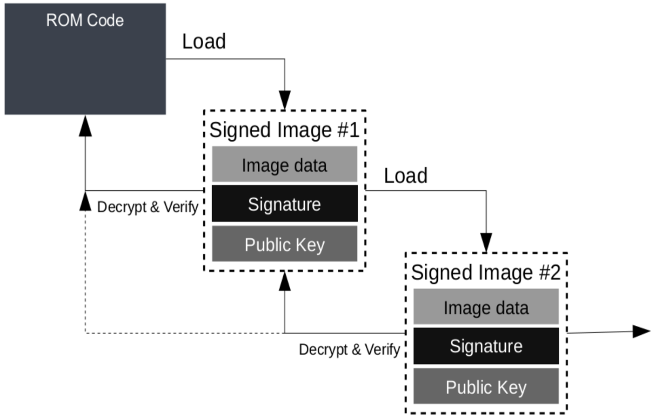
- Follows automotive design patterns
- Separation of control, critical control and rich control
- Example: Diagnostics vECU


Cloud services
Auto OS
Instrument Cluster: Notification
Secure Container
Telematics: Diagnostics engine
IVI OS
IVI: Rich UI controls. FOTA control.
Vehicle Network API
Vehicle Network
CAN Bus

HARDWARE SECURITY TECHNOLOGIES

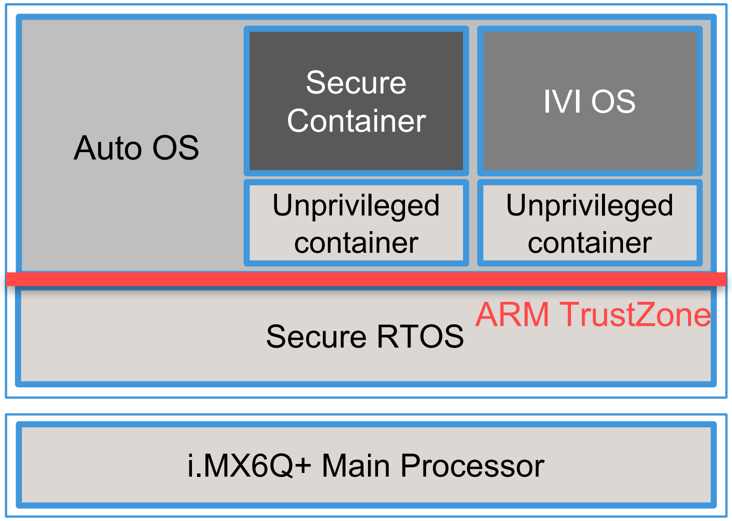
Secure Key Storage



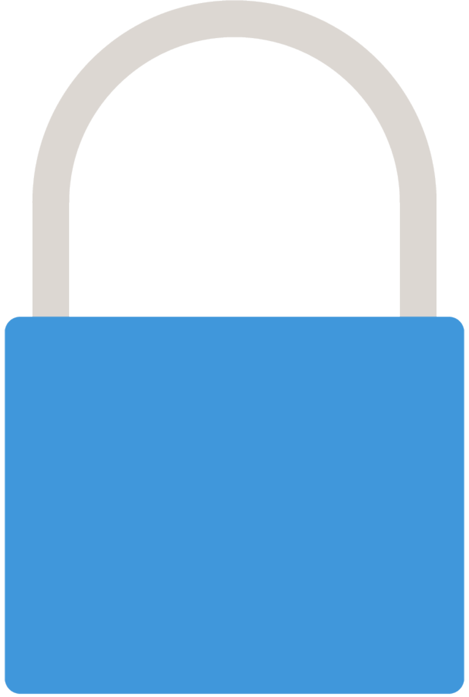


High Assurance Boot and Chain of Trust

ARM TrustZone



MORE SECURITY SOLUTIONS

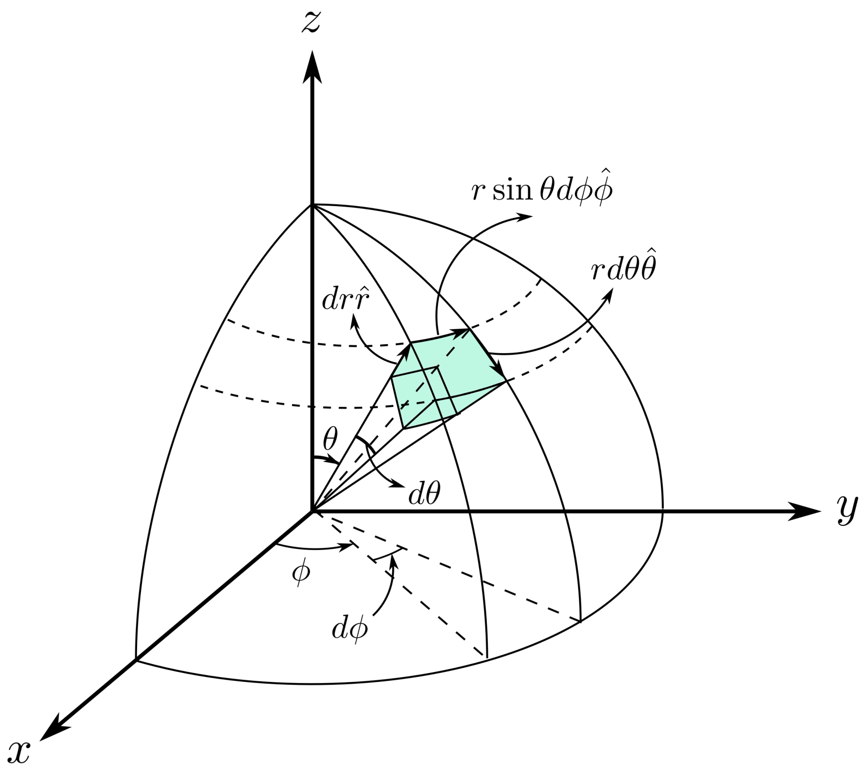


- Vehicle network protection
- Cryptography
- Intrusion detection system
- Open source development model
- External partners
- Research
- Training

WHAT’S NEXT

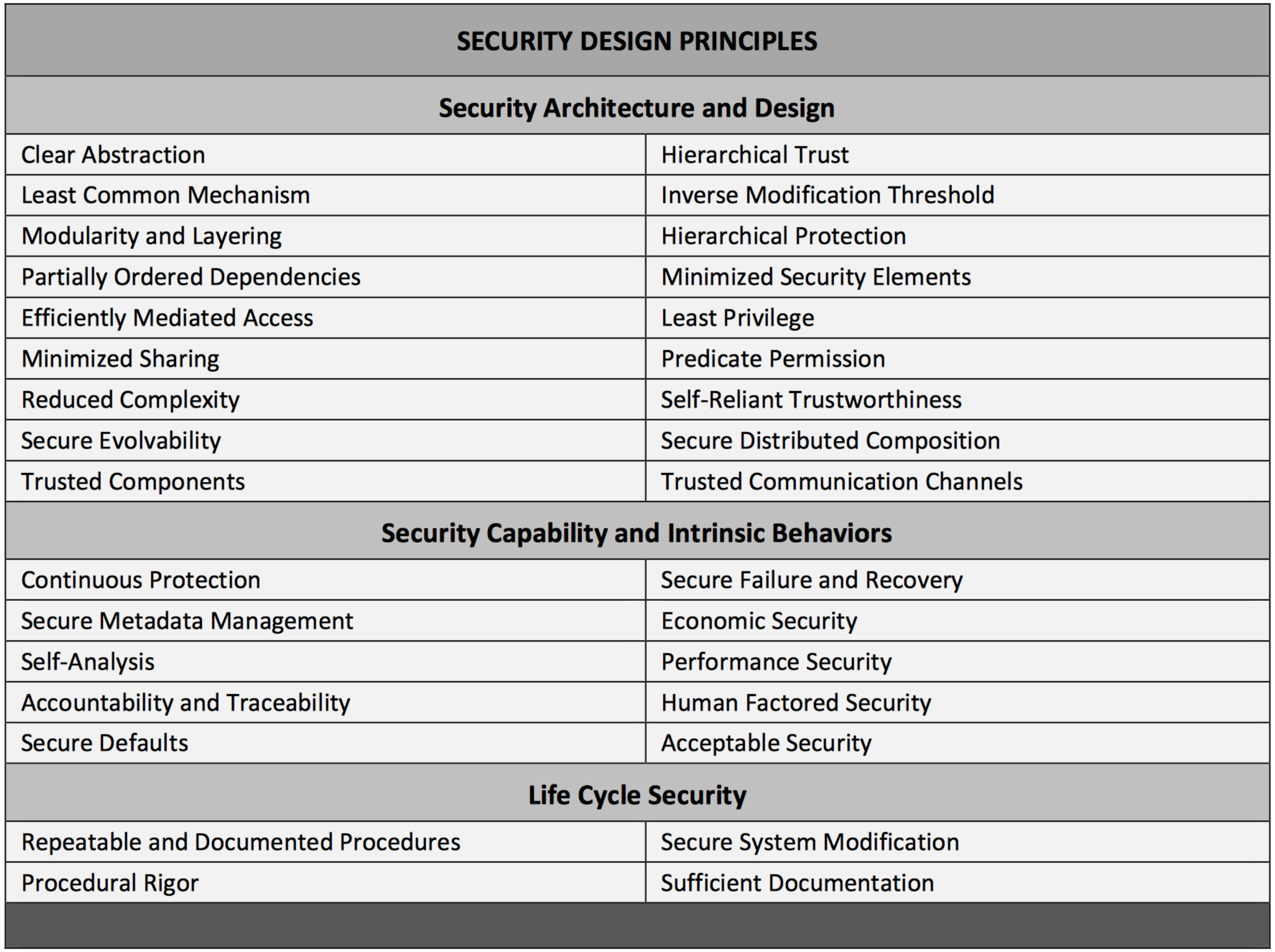
link motion

SECURITY FORMALIZATION



- Broader analysis
- NIST SP-800, SAE J3061, ISO 15288
- Privacy standards
- Integration to processes
- Secure System State
- Security Taxonomy
- Mathematical proofs

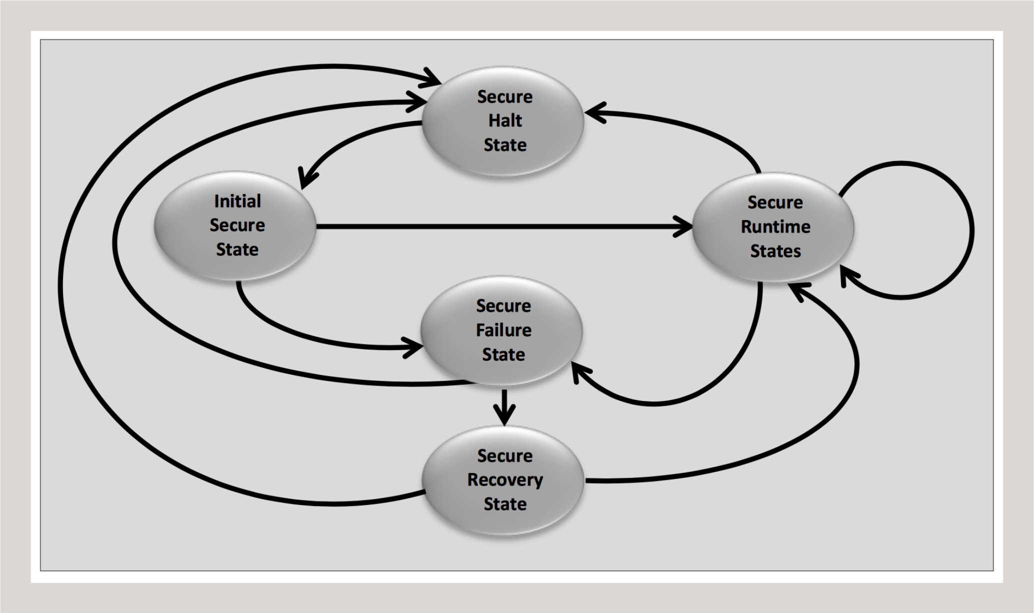
SECURITY TAXONOMY



SECURITY DESIGN PRINCIPLES	
Security Architecture and Design	
Clear Abstraction	Hierarchical Trust
Least Common Mechanism	Inverse Modification Threshold
Modularity and Layering	Hierarchical Protection
Partially Ordered Dependencies	Minimized Security Elements
Efficiently Mediated Access	Least Privilege
Minimized Sharing	Predicate Permission
Reduced Complexity	Self-Reliant Trustworthiness
Secure Evolvability	Secure Distributed Composition
Trusted Components	Trusted Communication Channels
Security Capability and Intrinsic Behaviors	
Continuous Protection	Secure Failure and Recovery
Secure Metadata Management	Economic Security
Self-Analysis	Performance Security
Accountability and Traceability	Human Factored Security
Secure Defaults	Acceptable Security
Life Cycle Security	
Repeatable and Documented Procedures	Secure System Modification
Procedural Rigor	Sufficient Documentation

Source: NIST SP 800-160

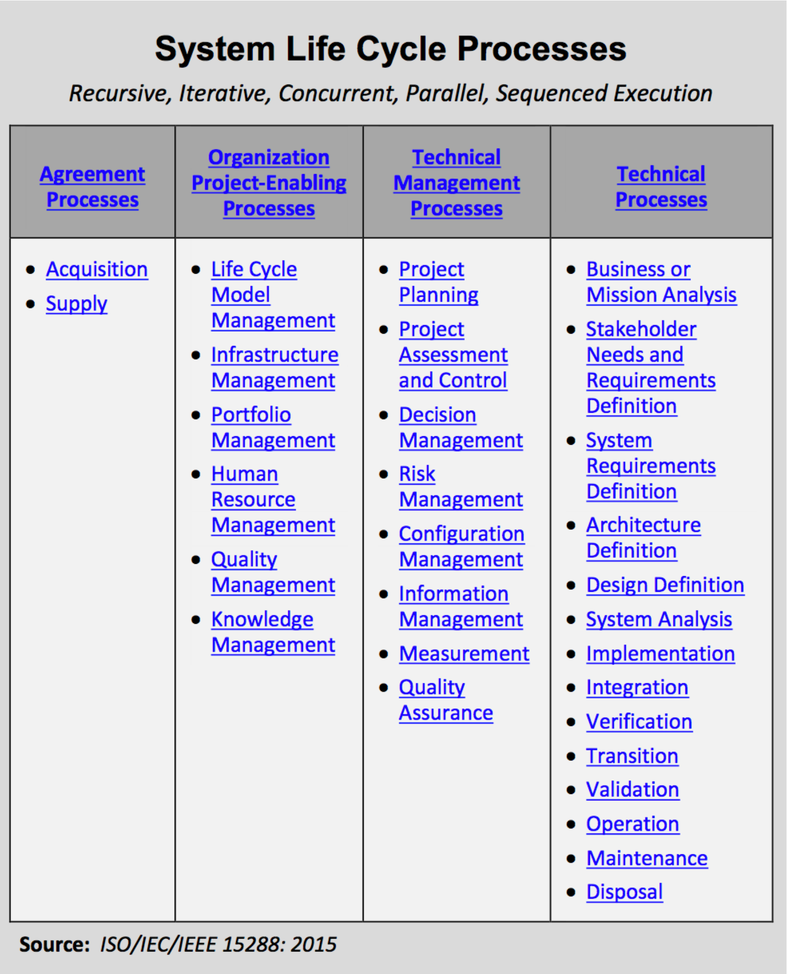
SECURE SYSTEM STATE



Source: NIST SP 800-160

- Design with safe state (ISO 26262)
- Example implementation:
  - Reference monitor (IDS)
  - Re-flash from ROM

INTEGRATION TO PROCESSES



System Life Cycle Processes

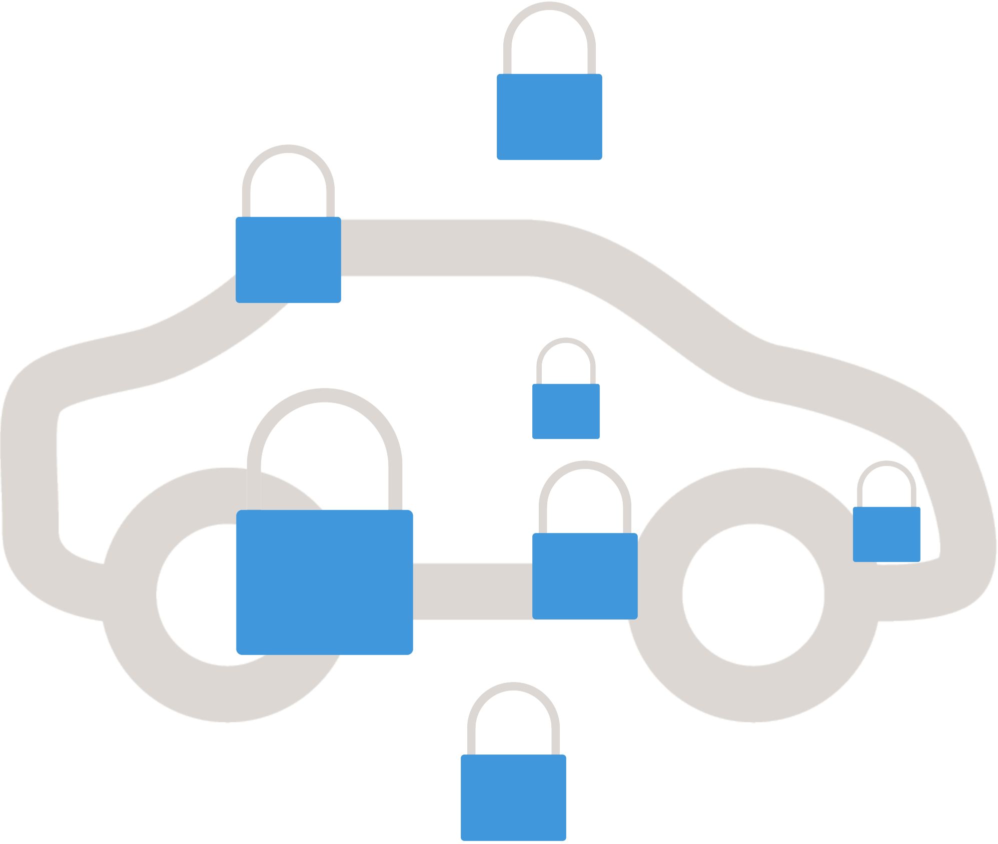
Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organization Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Source: *ISO/IEC/IEEE 15288: 2015*

- ISO 15288 good framework
- Code first vs specification
- Not just engineering
- Aims to enable ‘organizational learning’ -> same breach does not happen twice
- Work split between OEM/T1 and AGL ?

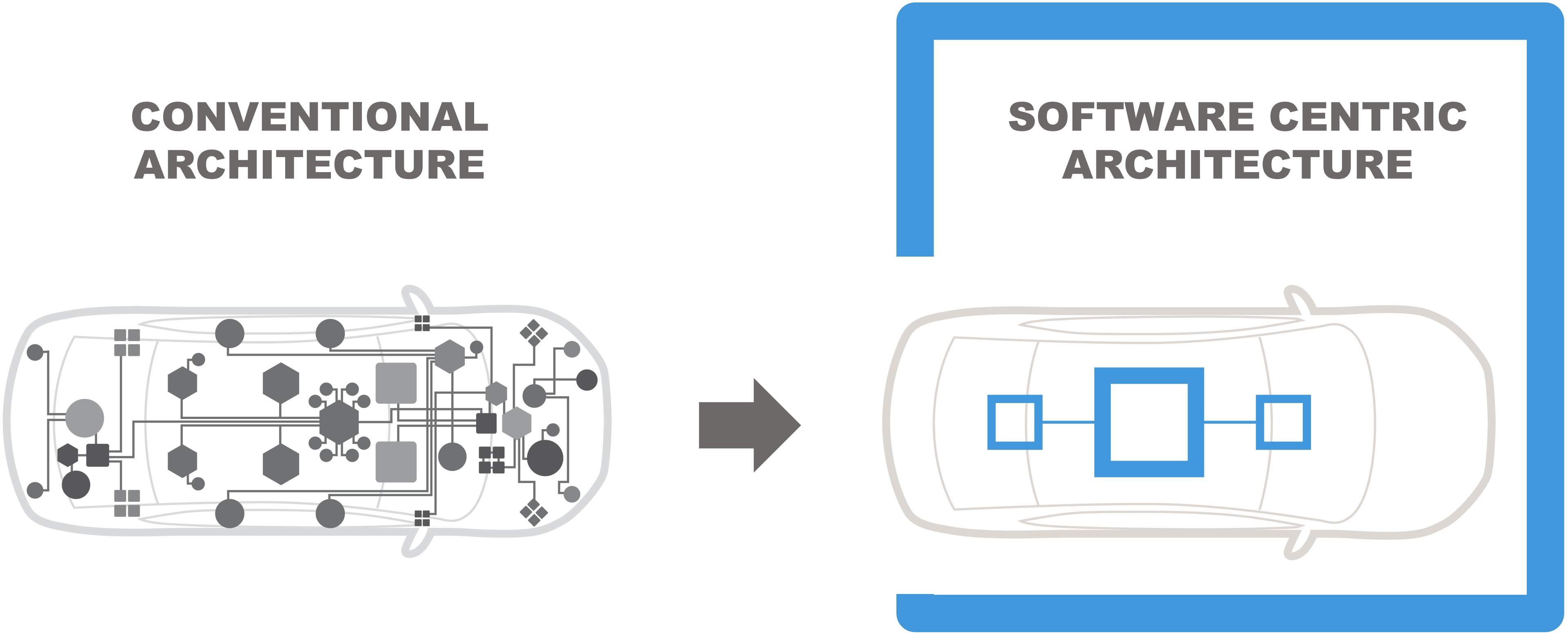
MORE SECURITY SOLUTIONS



- More cost-efficient solutions enable better security
  - AGL, APPSTACLE, ASSET
- Improve overall level of security
- Implement HW solutions with SW
- Developer training

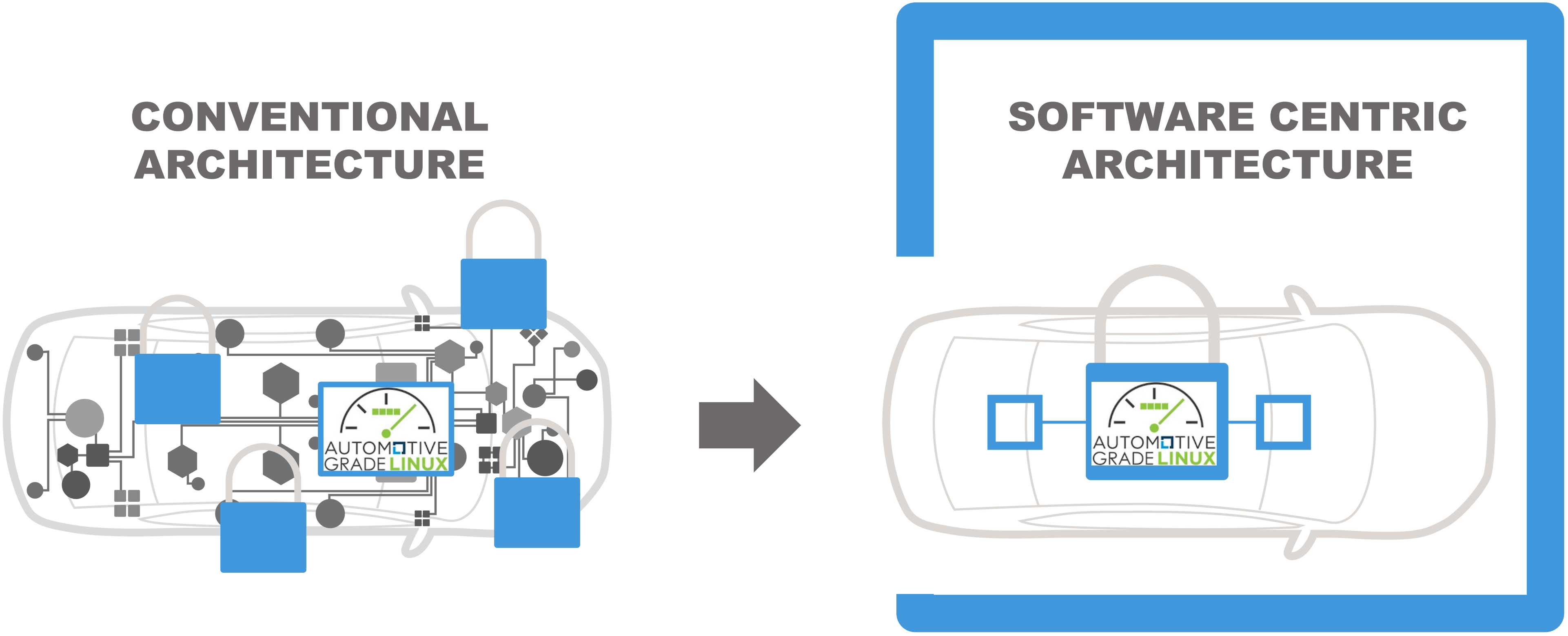
link motion

SOFTWARE DEFINED CAR



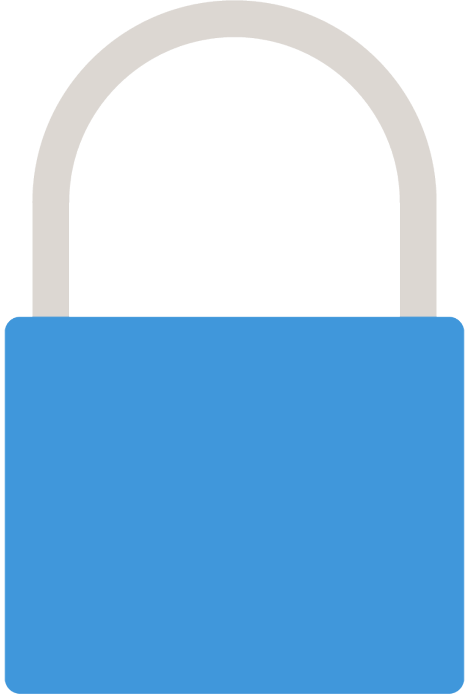
link motion

SOFTWARE DEFINED CAR



link motion

SUMMARY



- Connected vehicles are happening now
- Need uncompromised solutions
  - Same as safety
- There are plenty of solutions
  - But none solves it alone
- More holistic approach is future

link motion

NOMOVOK

LINK-MOTION.COM

info@link-motion.com

mikko.hurskainen@link-motion.com
kanae.kubota@link-motion.com