ADAS Platform Root of Trust

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

Jean Lee (Pr. Embedded Solutions Engineer)

Sep 27, 2022

Agenda

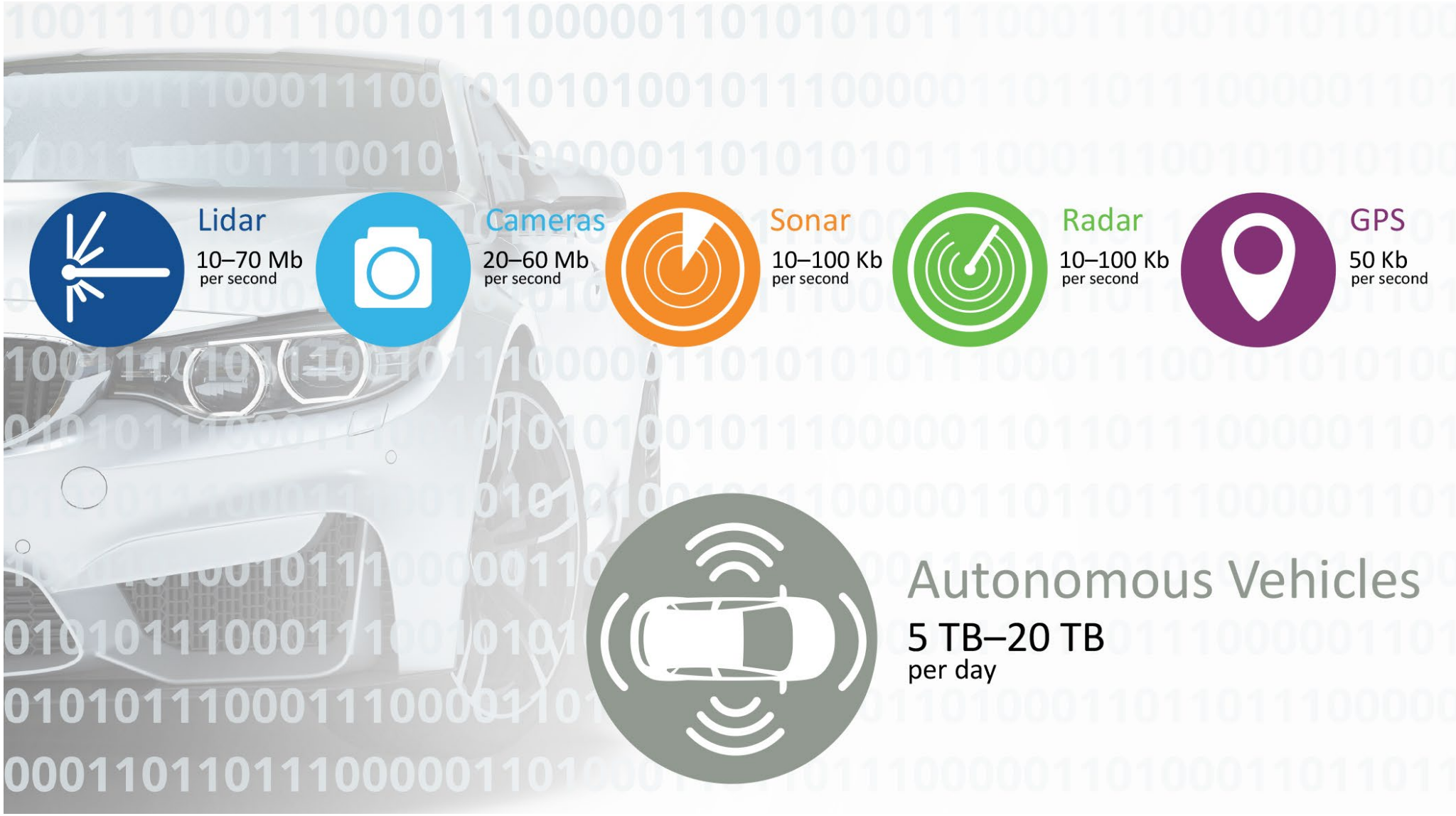
- ADAS market and technologies
- Vulnerabilities and risks
- CEC1712 Platform Firmware Resiliency MCU features
- Microchip and ADAS

Automotive Growth Drivers

- Infotainment system development and updates
- Assisted and autonomous driving – while maintaining vehicle and road safety
- Electrification of vehicles and related infrastructure
- Automotive cybersecurity

MICROCHIP

Data Center on Wheels



Assisted Driving: Safety and Comfort

Sensor Processing

- MCUs, MPUs and FPGAs
- Security/Trust Anchor
- Oscillators
- Memory
- Power Management
- Amplifiers
- ADC and DAC
- Thermal Management

Communications

- LIN
- CAN and CANFD Controllers
- 802.3 Ethernet Controllers
- 10Base-T1S
- 100Base-T1
- 1000Base-T1
- CoaXPress®

Vehicle Computer/ ADAS Controller

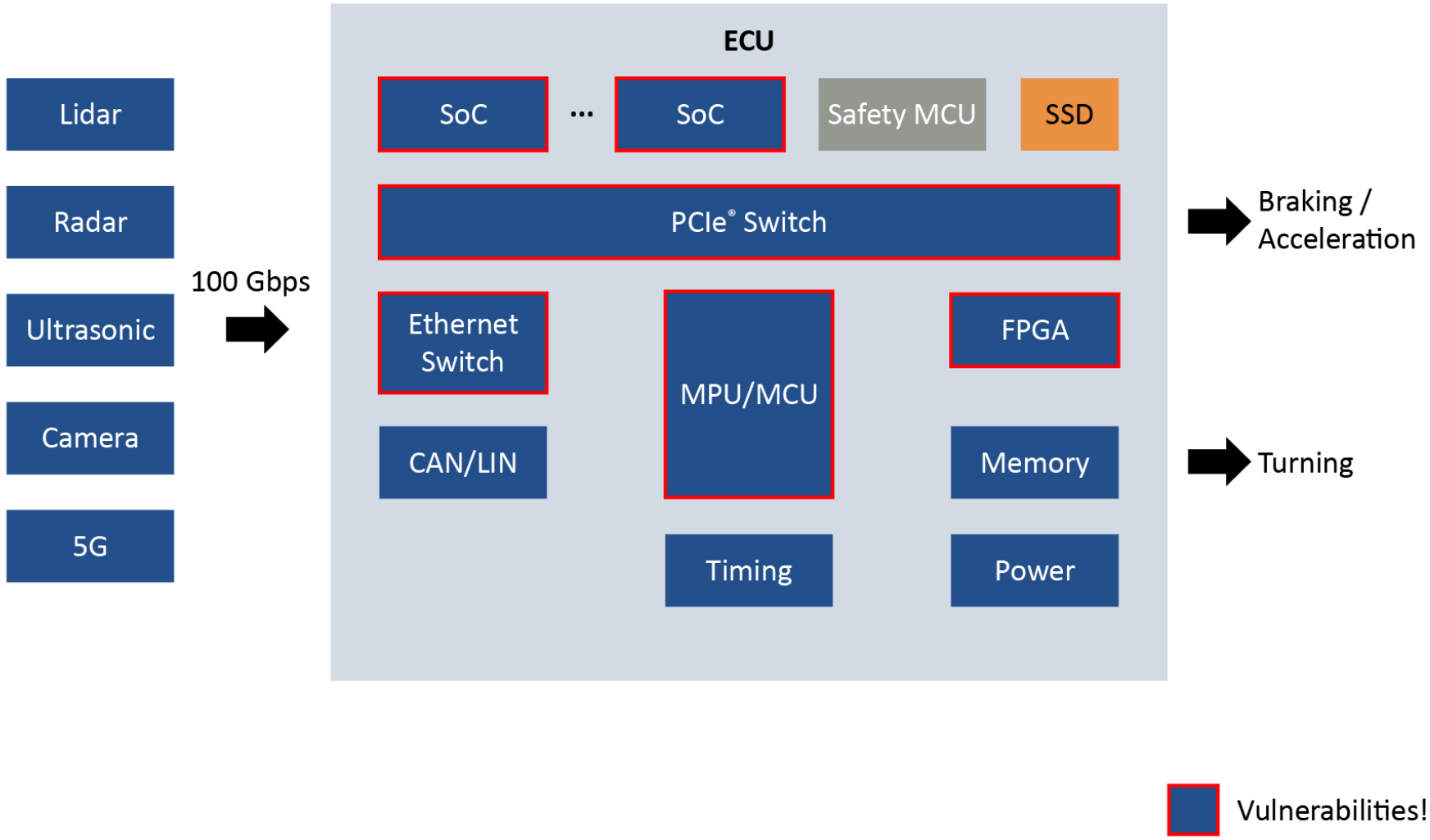
- PCIe® Switch
- FPGA and MPUs
- Power Management
- Ethernet
- Security/Trust Anchor
- MEMS Clock
- Clock Retimers
- Memory

Firmware Vulnerabilities in Automotive

- One of highest-value system attacks
- Historically little to no protection
- Launching point for additional security breaches
- Difficult to keep pace with as security and threats advance

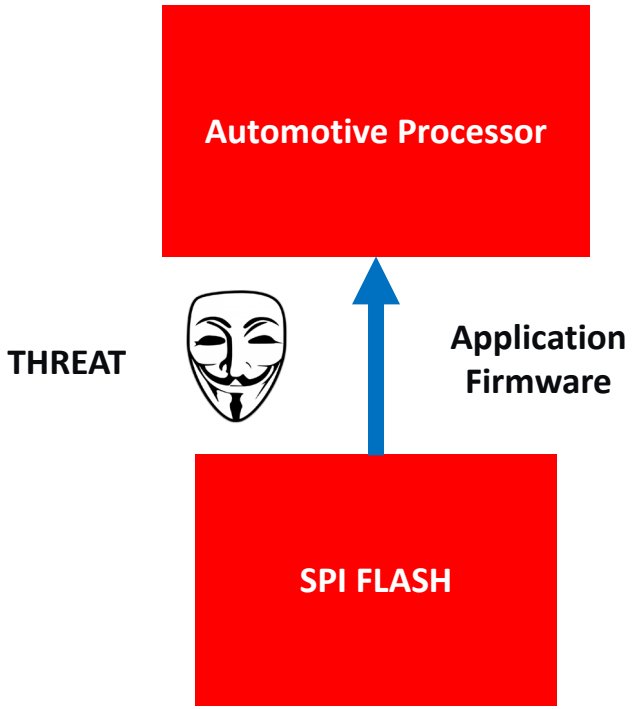
MICROCHIP

Vulnerabilities in Assisted Driving

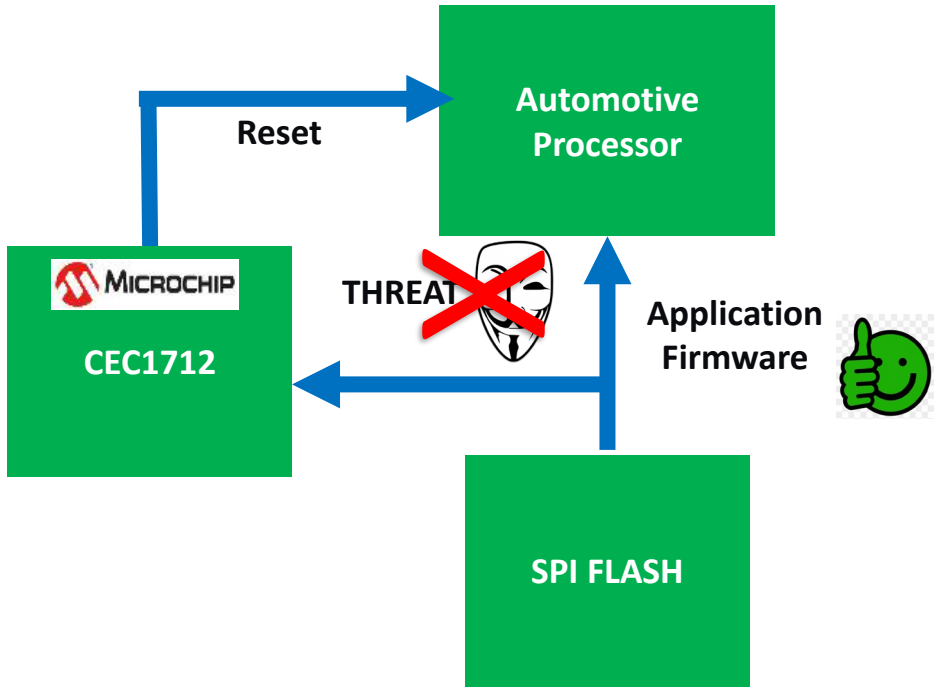


Firmware Vulnerability and Protection Simplified

Unprotected Boot of Automotive Processor



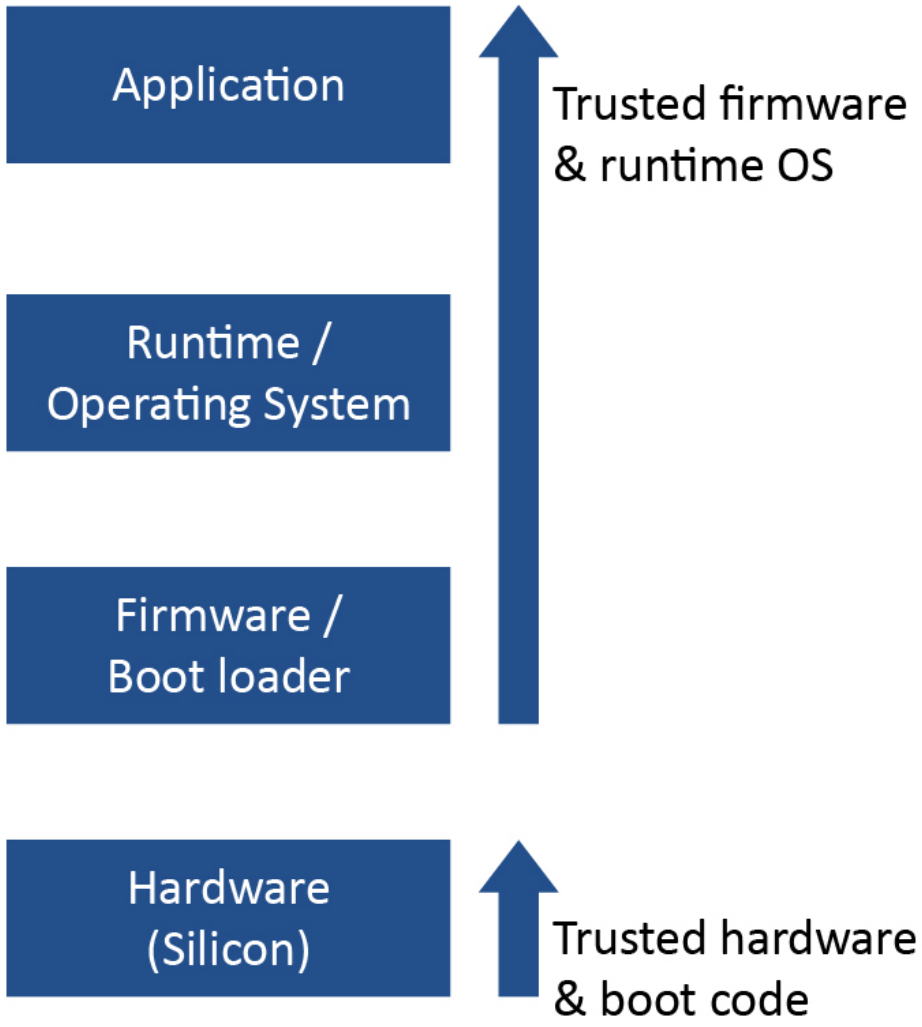
Secure Boot of Automotive Processor



MICROCHIP

Securing Firmware Updates

Why CEC1712 as Root of Trust Co-Processor?



NIST 800-193 Platform Firmware Resiliency	
Multiple Image Authentication	Key Revocation
AEC-Q100 Qualified	Code Rollback Protection
Attestation Ready	Secure Firmware Update
Prompt Security Standard Updates	CSNA Secure Boot (P-384)

MICROCHIP

CEC1712 – *In Production*

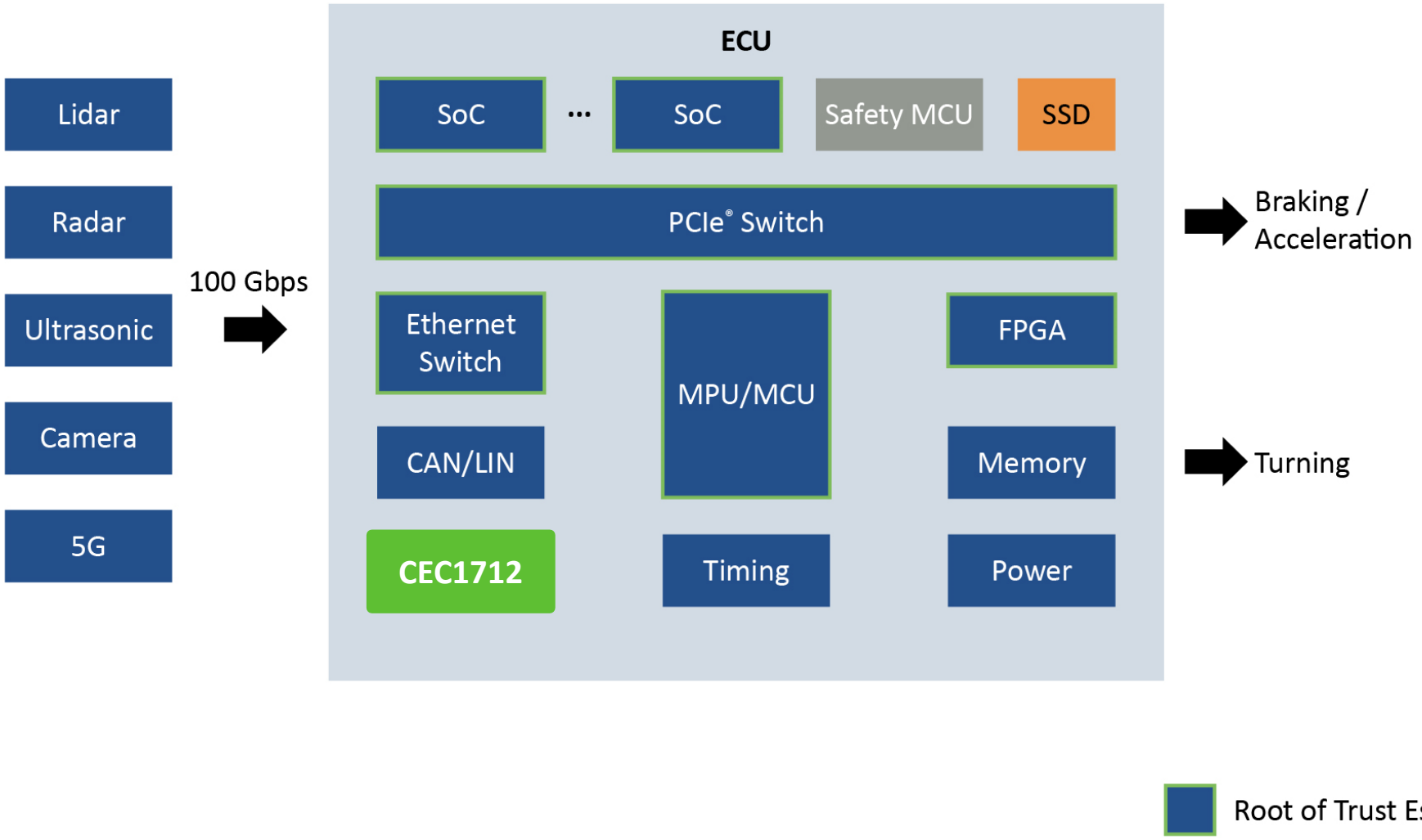
- **Root of trust for the platform**
  - Fully NIST 800-193 compliant
- **Cost effective embedded controller**
- **Broad hardware crypto cipher suite**
- **Key revocation and code rollback protection**
- **AEC-Q100 Grade 1 (-40C to +125C)**
- **Aimed at any SoC booting out of external SPI Flash**

CEC1712 Hardware Crypto Cipher Suite

		CEC1712
Symmetric Encryption		AES-128, AES-192 and AES-256
	Modes:	ECB, CBC, OFB, CFB, CTR
Hashing		SHA-1, SHA-256, SHA-384, SHA-512
Public Key Engine	RSA	RSA-1024 to RSA-4096
	ECC	192 to 521 bits in GF(p) 160 to 571 bits in GF(2m) Curve25519
	DSA	ECDSA, EC-KCDSA, Ed25519
		Modular Arithmetic Primitives
		Miller-Rabin Primality Testing
Random Number Generator		True RNG
		1K FIFO for pre-calculation
User Programmable OTP		4k bits
	Field Programmable	Yes

- **CNSA Secure Boot (P384)**
- **FIPS 800-193 100% Redundant Boot**
  - Two independent SPI Flash
- **In-Circuit Programmable OTP**

Vulnerabilities in Assisted Driving



Automotive Platform Firmware Protection

CEC1712 Secure Boot Controller

Immutable HW Root of Trust

Hardware-based Code Authentication

Secure Firmware Updates

NIST 800-193 Platform Firmware Resiliency

Advanced Algorithms to Keep Pace with Change

AEC-Q100 Automotive Qualified

MICROCHIP

Microchip in ADAS

Most Comprehensive Wired Connectivity Technologies

Ethernet

Leading energy efficiency
>115M ports shipped

PCIe Switch

Industry's highest density
lowest power

Security

Industry's first automotive security development kit

CAN and LIN

#1 LIN SBCs SiPs supplier
Industry's first Grade 0 CAN.
Largest product portfolio with
1 Billion nodes shipped

Power Discrete

One of the most comprehensive power product selections.
Quality meets the industry's toughest standards

Timing

Best quality and reliability with superb shock and vibration immunity.
Smallest size, full-clock tree support

MICROCHIP

Thank You

MICROCHIP