Secure F-RAM for Event Data Recording in ADAS Systems

Douglas Mitchell

Automotive Megatrends

Flash Memory Summit

Connectivity	Automation	Digitalization	Electrification
Totally Connected Car	*Levels 1 - 5*	*Intuitive, Adaptive & Responsive*	*Electrified Transportation*

"Connected Car" transforms transportation and drives semiconductor growth in vehicles

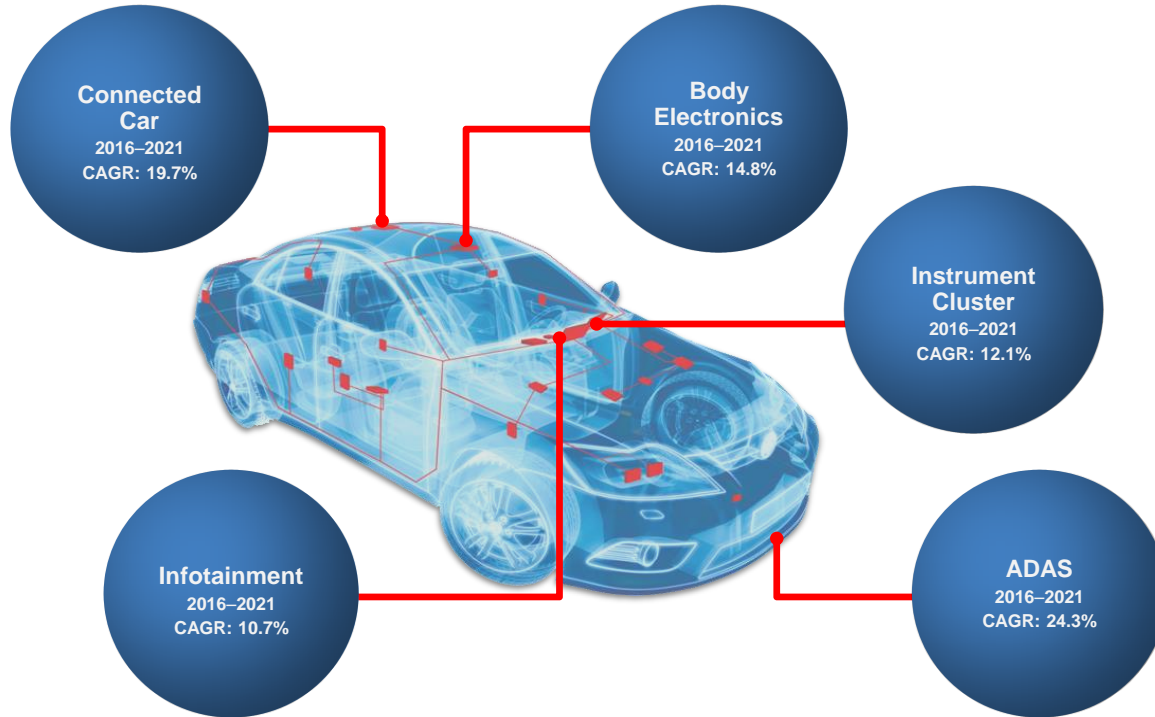$300 ~ $1,000
Semiconductor Content
2017

Auto Semi CAGR = 5.6% 2017 – 2022

$400 ~ $2,000+
Semiconductor Content
2022

Electronics Content

Connected Car
2016–2021
CAGR: 19.7%

Body Electronics
2016–2021
CAGR: 14.8%

Instrument Cluster
2016–2021
CAGR: 12.1%

Infotainment
2016–2021
CAGR: 10.7%

ADAS
2016–2021
CAGR: 24.3%

Source: Strategy Analytics, Cypress internal estimates

Automotive Infotainment System Trends

NEXT

Integrated Cockpit

Intelligent Connectivity + Multiple displays + More personalization

Single ECU system

NOW

Connected Infotainment

Wireless connectivity + Intelligent HMI

Separated ECU systems

PAST

Traditional Infotainment

AM/FM Radio + CD + Navigation

Separated ECU systems

Driver Information* Market Growth

Vehicle Production Growth
(Units in Millions)

2.4%

95.1

107.3

2017   **2022**
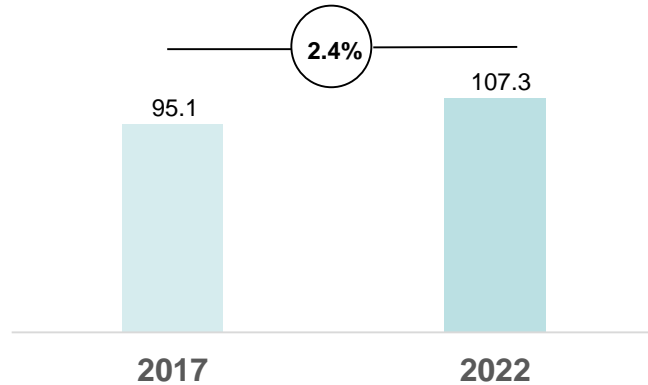
Driver Information Growth
(US Dollars)

7.4%

$32.5B

$46.6B

2017   **2022**
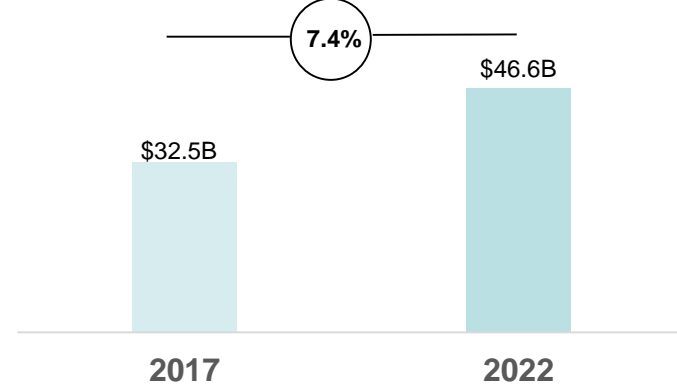
- **Smart Phone-based and wireless-connected infotainment replacing traditional embedded system**
- **HMI solution trend towards to large display and multimodal interaction**
- **USB-C is everywhere in peripherals for mobile phones and PCs and now emerging in automotive**
- **Automotive manufacturers are pushing for initial Boot (Splash Screen) with fast NOR Flash to meet "Instant-on" required by certain features (backup cameras, chimes, cluster displays)**

Driver Information* market growing significantly faster than underlying vehicle production

REGULATIONS CONCERNING EDRs

- **NA – NHTSA .**
  - Regulations for required data elements for conventional Airbag module black boxes.
    - https://www.law.cornell.edu/cfr/text/49/part-563
    - https://www.nhtsa.gov/
- **EU – EC Europa**
  - https://ec.europa.eu/transport/road_safety/specialist/knowledge/esave/esafety_measures_known_safety_effects/black_boxes_in_vehicle_data_recorders_en
  - Conclusions from the stakeholder meeting to make EDR mandatory in EU. Consensus is to make ADAS active safety data also to be made mandatory to be logged in addition to conventional black box parameters defined in NHTSA part 563.
    - https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/pdf/edr05062014/summary_and_conclusions.pdf

Automotive Event Data Recorders

Gen1 EDRs in light duty vehicles for >40 yrs

- Air bag deployment timing
- Supplemental inflatable restraint (SIR) lamp status
- Longitudinal acceleration
- Seat belt status
- Limited vehicle sensor status (what triggered the event)

Automotive Event Data Recorders

Next generations (1999+)

- Vehicle speed, engine RPM, percent throttle, service brake switch circuit status

- Accelerator position, transmission gear status, ABS activity, stability control status, traction control activity, yaw rate, steering wheel angle, individual wheel speed, cruise control status, etc.

Automotive Event Data Recorders

NHTSA-2006-25666

- Rule defining parameters to be recorded after 2012

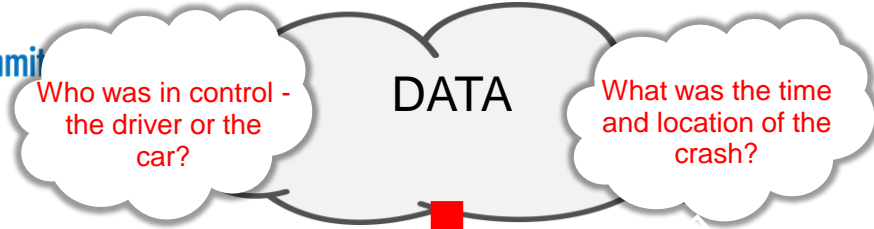- By model year 2013 96% of new passenger vehicles were EDR-equipped

Automotive Event Data Recorders

- So…why do we need EDRs?
  - Data forensics!
  - Post mortem analysis!

- What does the future hold?

Design Challenges

- Semi-Autonomous, Autonomous vehicles
- Sensors; Cameras, Lidar, Radar, Ultrasonic
- GPS
- V2X
- Signal integrity/interference/spoofing

➢ These sources add to the challenges of ensuring data integrity

No-Data-Loss EDR

- **PROBLEM**:
  - Conventional flash-based EDRs buffer data into volatile memory and then periodically store into Flash. In the event of a crash, these systems are at risk of losing the last moment critical system data due to instant power failure.

- **SOLUTION**
  - This risk is mitigated when using datalogging memories that enable instant nonvolatile writes

What is Ferroelectric RAM (F-RAM)

NVM which stores data as a polarization **of a ferroelectric material (Lead-Zirconate-Titanate).**

As an electric field is applied, dipoles shift in a crystalline structure to store information

Advantages

Symmetrical atomic position → Non volatility

Switch in states is instantaneous → Fast writes and Low energy

Based on "atomic position" vs. "trapped charge" → SER immunity and Radiation tolerant

Two symmetrical states with no reason to degrade → Virtually Infinite Endurance Data retention 100 yrs

Cypress' F-RAM is the perfect choice for
*"**Power Efficient, Instantaneous Data-logging**"*

Electric field

Secure F-RAM

CYPRESS®
EMBEDDED IN TOMORROW™
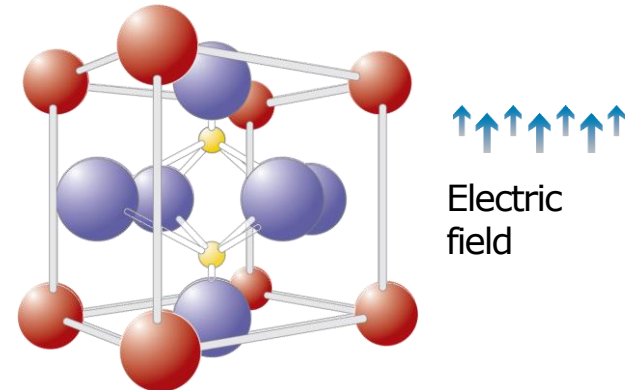
Product Overview

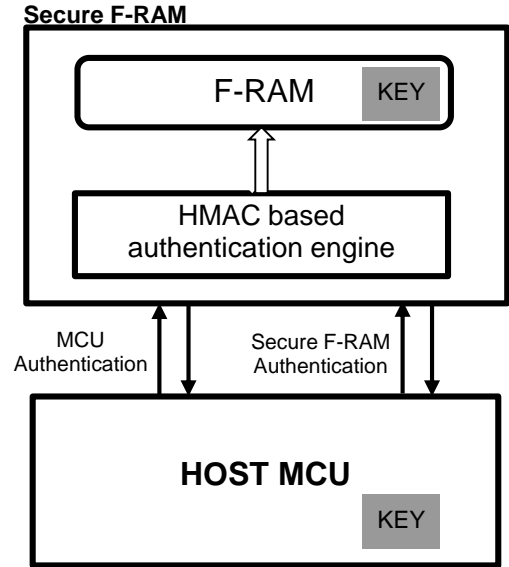**Problem Statement:** Datalogs containing sensitive personal or legal data may be modified or damaged through malicious intent

Current Solution: Limited product ID and serial number–based security; inadequate for malicious attack

Solution:

- Add authentication protocols to Excelon™ F-RAM
  - Option 1; MCU shared key (secure MCU)
  - Option 2: No key on MCU (non-secure MCU)

Secure F-RAM

F-RAM   KEY

HMAC based authentication engine

MCU Authentication

Secure F-RAM Authentication

HOST MCU   KEY

Step	Activity	F-RAM state	Read / Write Access
1	Power-up	Locked	Blocked
2	Authenticate	Unlocked	Allowed
3	MCU locks F-RAM	Locked	Blocked
4	Power Down / Loss	Locked	Blocked (N/A)
5	Power Up after Event	Locked	Blocked

Secure F-RAM Logging Options

User Option 1 (Shared Key):

Step	Activity	F-RAM state	Read / Write Access
1	Power up	Locked	Blocked
2	Authenticate	Unlocked	Allowed
3	Logging	Unlocked	Allowed
4	Power Down / Loss	Locked	Blocked (N/A)
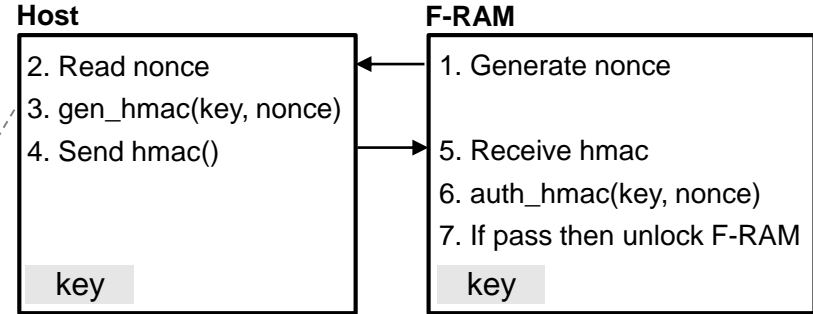
User Option 2 (No key on MCU):

Step	Activity	F-RAM state	Read / Write Access
1	Power up	Unlocked	Allowed
2	Logging	Unlocked	Allowed
3	MCU locks F-RAM	Locked	Blocked
4	Power Down	Locked	Blocked (N/A)
5	Power Up after Event	Locked	Blocked

Host

2. Read nonce
3. gen_hmac(key, nonce)
4. Send hmac()

key

F-RAM

1. Generate nonce

5. Receive hmac
6. auth_hmac(key, nonce)
7. If pass then unlock F-RAM

key

Host

1. Host detects event
2. Host sends lock()

F-RAM

3. "permanent" lock F-RAM
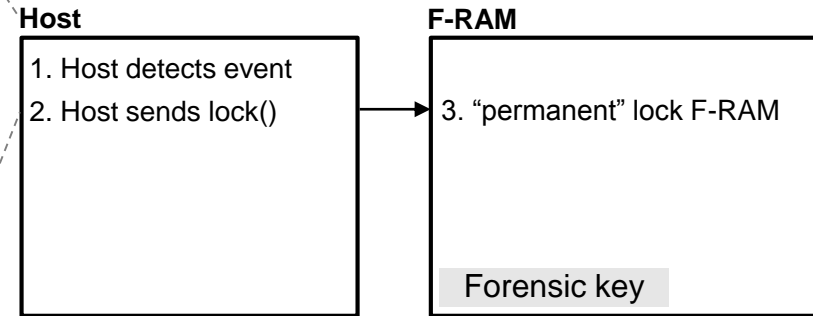
Forensic key

Forensic key is used in lab to retrieve logged data

Use case: Protect high-value logs in F-RAM

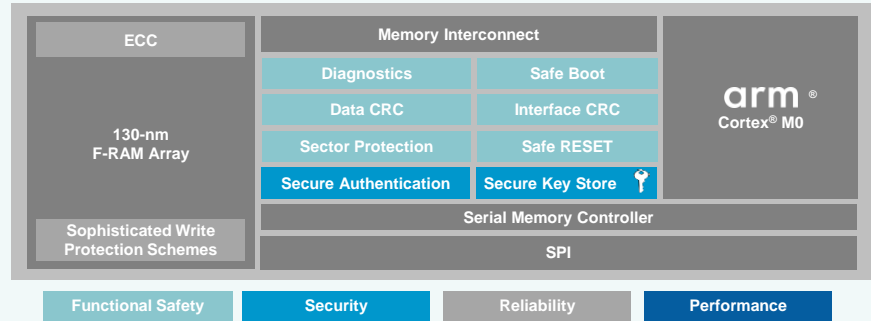# SECURE F-RAM DEMO IN EMBEDDED WORLD

2Mb-to-16Mb Excelon™ F-RAM

Features

- **Excelon-Ultra**
  - 4Mb
  - 108-MHz Single Data Rate (SDR)/54-MHz Double Data Rate (DDR) Quad SPI
  - Industrial temperature range: -40°C to +85°C
- **Excelon-Auto**
  - 2Mb Auto E, 4Mb Auto A
  - 50-MHz SPI
  - Automotive (AEC-Q100) temperature range grade A: -40°C to +85°C
  - Automotive (AEC-Q100) temperature range grade E: -40°C to +125°C
- **Excelon-LP**
  - 4Mb, 8Mb
  - 20-MHz SPI (Commercial), 50-MHz SPI (Industrial)
  - Ultra-low (0.10-µA) hibernate current
  - Ultra-low (0.75-µA) deep power-down current
  - Ultra-low (1.00-µA) standby current
  - Commercial temperature range: 0°C to +70°C
  - Industrial temperature range: -40°C to +85°C
- **Common Features for Excelon-Ultra/Auto/LP**
  - Operating voltage range: 1.71–1.89 V, 1.80–3.60 V
  - 100-trillion read/write cycle endurance
  - 100-year data retention

Excelon F-RAM

Secure | Reliable | High-Performance

ECC

130-nm F-RAM Array

Sophisticated Write Protection Schemes

Memory Interconnect

Diagnostics | Safe Boot
Data CRC | Interface CRC
Sector Protection | Safe RESET
Secure Authentication | Secure Key Store

arm® Cortex® M0

Serial Memory Controller

SPI

Functional Safety | Security | Reliability | Performance

Family Table

Density	Standby Current (Typ.)	Active Current (Typ.)	Packages
2Mb	1 µA	3 mA	SOIC (8)
4Mb	1 µA	3 mA	SOIC (8), GQFN (8)
8Mb	1 µA	3 mA	GQFN (8)
16Mb	1 µA	3 mA	SOIC (8), GQNF (8)

Thank You!