Secure F-RAM for Event Data Recording in ADAS Systems

Douglas Mitchell
Automotive Megatrends

Connectivity

* Totally Connected Car

Automation

* Levels 1 - 5

Digitalization

* Intuitive, Adaptive & Responsive

Electrification

* 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

Source: Gartner, Strategy Analytics, Cypress internal estimates
Electronics Content

Source: Strategy Analytics, Cypress internal estimates
Automotive Infotainment System Trends

PAST
Traditional Infotainment
AM/FM Radio + CD + Navigation
Separated ECU systems

NOW
Connected Infotainment
Wireless connectivity + Intelligent HMI
Separated ECU systems

NEXT
Integrated Cockpit
Intelligent Connectivity + Multiple displays + More personalization
Single ECU system
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 Growth

Vehicle Production Growth

(Units in Millions)

<table>
<thead>
<tr>
<th>Year</th>
<th>2017</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>95.1</td>
<td>107.3</td>
</tr>
</tbody>
</table>

2.4% growth from 2017 to 2022

Driver Information Growth

(US Dollars)

<table>
<thead>
<tr>
<th>Year</th>
<th>2017</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$32.5B</td>
<td>$46.6B</td>
</tr>
</tbody>
</table>

7.4% growth from 2017 to 2022

Driver Information* market growing significantly faster than underlying vehicle production

Source: Strategy Analytics, Cypress internal estimates
Note: Drive Infotainment includes Infotainment and Cluster
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.law.cornell.edu/cfr/text/49/part-563)
    - [https://www.nhtsa.gov/](https://www.nhtsa.gov/)

- **EU – EC Europa**
  - 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.
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?
Is the driver liable?

Is the manufacturer liable?

Who pays when a driverless car crashes?

Who was in control - the driver or the car?

What was the time and location of the crash?

Memory Challenges
1. Records instantly
2. Keep writing fast
3. Highly reliable
4. Lasts lifetime of the car
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”
Secure F-RAM
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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>F-RAM state</th>
<th>Read / Write Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power up</td>
<td>Locked</td>
<td>Blocked</td>
</tr>
<tr>
<td>2</td>
<td>Authenticate</td>
<td>Unlocked</td>
<td>Allowed</td>
</tr>
<tr>
<td>3</td>
<td>MCU locks F-RAM</td>
<td>Locked</td>
<td>Blocked</td>
</tr>
<tr>
<td>4</td>
<td>Power Down / Loss</td>
<td>Locked</td>
<td>Blocked (N/A)</td>
</tr>
<tr>
<td>5</td>
<td>Power Up after Event</td>
<td>Locked</td>
<td>Blocked</td>
</tr>
</tbody>
</table>
## Secure F-RAM Logging Options

### User Option 1 (Shared Key):

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>F-RAM state</th>
<th>Read / Write Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power up</td>
<td>Locked</td>
<td>Blocked</td>
</tr>
<tr>
<td>2</td>
<td>Authenticate</td>
<td>Unlocked</td>
<td>Allowed</td>
</tr>
<tr>
<td>3</td>
<td>Logging</td>
<td>Unlocked</td>
<td>Allowed</td>
</tr>
<tr>
<td>4</td>
<td>Power Down / Loss</td>
<td>Locked</td>
<td>Blocked (N/A)</td>
</tr>
</tbody>
</table>

### Host

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

### F-RAM

1. Generate nonce
2. Receive hmac
3. auth_hmac(key, nonce)
4. If pass then unlock F-RAM

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

### User Option 2 (No key on MCU):

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

### Host

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

### F-RAM

1. Host detects event
2. Host sends lock()
3. “permanent” lock F-RAM

### Forensic Key

Forensic key is used in lab to retrieve logged data
Host is connected to Blackbox
Signature confirmed. Host is allowed access
Data log read successful
FRAM is unlocked successfully! Ready for logging
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**

<table>
<thead>
<tr>
<th>130-nm F-RAM Array</th>
<th>Memory Interconnect</th>
<th>arm Cortex® M0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC</td>
<td>Diagnostics</td>
<td>Secure Authentication</td>
</tr>
<tr>
<td></td>
<td>Safe Boot</td>
<td>Secure Key Store</td>
</tr>
<tr>
<td></td>
<td>Data CRC</td>
<td>SPI</td>
</tr>
<tr>
<td></td>
<td>Interface CRC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sector Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safe RESET</td>
<td></td>
</tr>
</tbody>
</table>

**Sophisticated Write Protection Schemes**

- Secure Bootstrap
- Data CRC
- Interface CRC
- Sector Protection
- Safe RESET

**Functional Safety**

- Secure | Reliable | High-Performance

**Security**

- Functional Safety
- Security
- Reliability
- Performance

**Family Table**

<table>
<thead>
<tr>
<th>Density</th>
<th>Standby Current (Typ.)</th>
<th>Active Current (Typ.)</th>
<th>Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Mb</td>
<td>1 µA</td>
<td>3 mA</td>
<td>SOIC (8)</td>
</tr>
<tr>
<td>4Mb</td>
<td>1 µA</td>
<td>3 mA</td>
<td>SOIC (8), GQFN (8)</td>
</tr>
<tr>
<td>8Mb</td>
<td>1 µA</td>
<td>3 mA</td>
<td>GQFN (8)</td>
</tr>
<tr>
<td>16Mb</td>
<td>1 µA</td>
<td>3 mA</td>
<td>SOIC (8), GQFN (8)</td>
</tr>
</tbody>
</table>
Thank You!