Requirements for Fail-Safe Automotive Solutions with NOR Flash Memory

Sandeep Krishnegowda
Marketing Director, Flash Business Unit
Cypress Semiconductor
Automotive Megatrends

**Implications**

- All sub-systems grow in connectivity and intelligence
- User interface transitions from mechanical to electronic
- Sensors proliferate → ever-increasing need for bandwidth
- Safety and security requirements increase
- In-car experience = home/office experience on wheels
Automotive Megatrends

Electrification
- Electrified Transportation

Connectivity
- Totally Connected, Digitized

Autonomy
- Levels 1 - 5

Implications
- Need more compute performance to support digitization of the vehicle
- Increasing functionality implies growing software complexity
- Low power to support electrification of the vehicle
- Rising functional safety requirement to meet ISO 26262 standard
- Cannot compromise on security
“Connected Car” transforms transportation and drives semiconductor growth in vehicles

- **Electrification**
  - Electrified Transportation

- **Connectivity**
  - Totally Connected, Digitized

- **Autonomy**
  - Levels 1 - 5

**Automotive Megatrends**

- **Electrification**
  - Semiconductor Content 2017: $300 ~ $1,000

- **Connectivity**
  - Auto Semi CAGR 2017 – 2022: $6%

- **Autonomy**
  - Semiconductor Content 2022: $400 ~ $2,000+

$400 ~ $2,000+ Semiconductor Content 2022
Cyber Attacks and Electronic System Safety are Growing Concerns

U.S. TRAFFIC DEATHS REPORTEDLY TOPPED 40,000 AGAIN IN 2018

Per National Safety Council estimates

Reuters reports that based on estimates provided by the National Safety Council, traffic deaths in the U.S. topped 40,000 last year. That would make 2018 the third year in a row with traffic deaths above that mark, according to the nonprofit organization. And while the good news is that the NSC estimates there were 231 fewer deaths than in 2017, a decrease of about 1 percent, those figures are 14 percent higher than they were back in 2014. An additional 4.5 million people were seriously injured in wrecks in 2018, which represents a 1-percent decline, as well.


Hackers crack Tesla Model 3 in competition, Tesla gives them the car

Source: https://electrek.co/2019/03/23/tesla-model-3-hacker-competition-crack/

Lawmakers Propose Bills to Secure Connected Planes, Trains and Automobiles

JULY 22, 2019

The legislation would set “reasonable” security measures for the numerous IT systems that power our increasingly connected vehicles.


Our Responsibility: Assure highest degrees of functional safety and security
What is Functional Safety?

“Absence of unreasonable risk due to hazards caused by malfunctioning behavior of electronic systems.”

- Risk = function of probability and extent of damage/harm
- Functional safety = detecting and managing failures
- Architected and designed-in safety features to the product
- Measures to identify random failures during operation

<table>
<thead>
<tr>
<th>ASIL Level</th>
<th>Failure Rate</th>
<th>SPFM</th>
<th>LFM</th>
<th>Application (example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>&lt;1000 FIT</td>
<td>Not relevant</td>
<td>Not relevant</td>
<td>Rear Lights</td>
</tr>
<tr>
<td>B</td>
<td>&lt;100 FIT</td>
<td>≥ 90%</td>
<td>≥ 60%</td>
<td>Cluster</td>
</tr>
<tr>
<td>C</td>
<td>&lt;100 FIT</td>
<td>≥ 97%</td>
<td>≥ 80%</td>
<td>Adaptive Cruise Control</td>
</tr>
<tr>
<td>D</td>
<td>&lt;10 FIT</td>
<td>≥ 99%</td>
<td>≥ 90%</td>
<td>Powertrain</td>
</tr>
</tbody>
</table>

ASIL=Automotive Safety Integrity Level; SPFM= Single Point Failure Mode; LFM= Latent Failure Mode
How Safety is Implemented in Automotive Today

ISO 26262 Processes

- ASIL D System (ADAS)
- Development Interface Agreement (DIA)
- ASIL B
- ASIL D
- ASIL A
- ASIL B
- ASIL C
- Safety-Element-Out-of-Context (SEooC)

Implication to Flash Memory Supplier?

- Upgrade to ISO 26262 compliant development process
- Invest in Functional Safety Organization
- Add safety mechanisms to the architecture to achieve required safety level
- Lots of functional safety documentation
- Safety analysis and compliance process
## Addressing Failures in Flash Memory Device

### Early Detection of Potential Errors to Achieve Functional Safety Requirements

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>Failure Description</th>
<th>Safety Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flash Cell Failures</strong></td>
<td>Charge loss and layer defects can lead to read/write errors</td>
<td>ECC (SECDED)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Integrity Check</td>
</tr>
<tr>
<td><strong>Reliability Latent Failures</strong></td>
<td>Number of program/erase cycles vs. data retention can lead to margin loss and read/write errors</td>
<td>Program Failure Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Erase Failure Detection</td>
</tr>
<tr>
<td><strong>Noise Failures</strong></td>
<td>Device interface and internal power supply spikes can cause incorrect operations</td>
<td>ECC (SECDED)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interface CRC</td>
</tr>
<tr>
<td><strong>System and Component Power Fault</strong></td>
<td>Faulty boot and power loss during erase/program can lead to wrong configuration, wrong data write</td>
<td>SafeBoot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safe RESET</td>
</tr>
</tbody>
</table>
Next generation automotive MCU’s migrate to 28nm and below technology nodes

- Challenging to offer viable automotive-qualified eNVM technology
- Growing code size and complexity requires more eFlash and eSRAM with limited scalability
- Secure MCU need external secure Flash to protect code, data and system secrets

SHE (Secure Hardware Extension)

HSM (Hardware Security Module)

HSM + External Secure Flash
### Automotive Evita Standard is a Good Benchmark

<table>
<thead>
<tr>
<th>Cryptographic Architecture/Implementation</th>
<th>Sensor/Actuator ECU</th>
<th>Gateway ECU</th>
<th>V2X Comm. ECU</th>
<th>Secure Flash Light</th>
<th>Secure Flash Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Use Case</td>
<td></td>
<td></td>
<td></td>
<td>ASIL-A/B Safety Systems</td>
<td>ASIL-C/D Safety Systems</td>
</tr>
<tr>
<td>Cryptographic Algorithms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric encryption/decryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Symmetric encryption/decryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hashing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hardware Acceleration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric encryption/decryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Symmetric encryption/decryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hashing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Features</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓</td>
</tr>
<tr>
<td>Key control per use / bootstrap</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓</td>
</tr>
<tr>
<td>PRNG with TRNG seed</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Monotonic counters 32 / 64 bit</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tick/UTC-synced internal clock</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓/✓</td>
<td>✓</td>
</tr>
<tr>
<td>Internal processing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User extendable feature set</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Internal V/NV (Key) memory</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Cryptographic Algorithms**
- Asymmetric encryption/decryption
- Symmetric encryption/decryption
- Hashing

**Hardware Acceleration**
- Asymmetric encryption/decryption
- Symmetric encryption/decryption
- Hashing

**Security Features**
- Secure / authenticated boot
- Key control per use / bootstrap
- PRNG with TRNG seed
- Monotonic counters 32 / 64 bit
- Tick/UTC-synced internal clock

**Internal processing**
- User extendable feature set
- Internal V/NV (Key) memory

AES: Advanced Encryption Standard  
ECC: Elliptic Curve Cryptography  
RSA: Rivest–Shamir–Adleman cryptosystem  
DES: Data Encryption Standard (superseded by 3-DES)  
TRNG/PRNG: True/Pseudo Random Number Generator  
SHA: Secure Hash
Secure NOR Flash Use Cases

- Cryptographically secure storage of code, data, and system secrets (keys, certificates)
- Firmware over the air (FOTA) updates between host, secure storage, and cloud
- Fast secure boot for firmware authentication, version attestation, and rollback protection
- Secure provisioning in unsecure manufacturing facilities and unsecure service centers
Protecting, Managing, and Updating Connected Edge Devices

- Real-time attack prevention of firmware manipulation & reliable status and alerts
- Prevent outsiders, insiders and supply-chain attacks
- Reliable OTA updates and status through a root-of-trust
- Big data analysis - Unique and trusted device analytics to identify critical patterns and anomalies.

Security risks for connected systems is growing and customers need an end-to-end solution.
Functional Safety
- Architected and designed to automotive safety standards
- ASIL-B compliant and ASIL-D ready

Security
- Root of Trust and secure storage

Best Reliability and Endurance
- EnduraFlex™ architecture enables >1M endurance cycles and 25 years data retention
- Grade-1 (125°C) automotive qualified

Highest Density
- MirrorBit® technology delivers up to 4Gb with 400 MB/s bandwidth