ememory

Embedded Wisely, Embedded Widely

Design Zero-Failure NVM Solutions for Automotive Applications

WHITEPAPER

Modern vehicles need secure, reliable NVM solutions that can function well even under extreme conditions. eMemory's AEC-Q100 qualified OTP and MTP solutions are well positioned to meet quality and reliability demands of the automotive industry.

Introduction

Over the past 20 years, there has been a substantial increase of automotive electronic systems. With proliferating of automotive electronics, the cars today and tomorrow need more than ever embedded programmable NVM (Non-volatile Memory) for storage, user setting, function configuration and security.

As alluring as the market can be, many electronic component vendors, including NVM providers, are intimidated by the automotive industry's stringent requirements of reliability and quality. In addition to density and performance, the automotive industry has very specific requirements to NVM, such as proven reliability under extreme operating conditions for a longer lifespan of 10-15 years.

eMemory offers logic-based embedded OTP (one-time programmable) and MTP (multiple programmable) IP solutions that passed the automotive industry's AEC-Q100 standard (Grade0,1) as well as foundry quality tests. The data retention is 10 years at operating temperatures from -40°C to +150°C.

Our automotive IP solutions – NeoBit, NeoFuse, NeoEE, NeoMTP –do not require additional masks, and can support program at post-fabrication stages (CP/FT/Assembly), providing design flexibility and reducing integration risks.

With the cars increasingly connected, security and privacy protection should also be integrated into automotive semiconductor design. eMemory's security IP NeoPUF provides a chip-unique ID, which can prevent against component counterfeiting, and secure in-vehicle or outside-the-vehicle communication.

Automotive Industry's Requirements to embedded NVM

From infotainment to ADAS (Advanced Driver Assistance Systems), NVM's usage is comprehensive in modern cars. In-vehicle NVM is responsible not only for the aforementioned functions, but also for car safety, especially in mission critical applications such as ADAS. As a result, NVM for automotive applications must meet automotive industrial standards such as AEC-Q100, ISO26262 [1], or pass other tests specified by OEMs and Tier 1 automotive suppliers.

The automotive industry has far more demanding requirements to NVM's temperature tolerance and lifespan. This is to ensure the NVM is reliable enough to weather all the harsh conditions a vehicle might be exposed to throughout its life time.

The operating temperature range expected of an automotive-grade NVM IP is between -40°C and +150°C (ambient), and expected life time 10-20 years. Rigorous tests must be done to ensure the IP behaves as specified in the datasheet under all conditions.

Other requirements to automotive NVM include programmability, small area, low power, low bit error rate (BER), and error-correction schemes. In some safety critical systems, the memory must contain redundancy schemes.

Design Zero-Failure NVM Solutions

eMemory's OTP solutions (NeoBit and NeoFuse) and MTP solutions (NeoEE and NeoMTP) are designed to reliably retain data for 10 years at temperatures from

1. AEC-Q100 is a failure mechanism based stress test qualification for integrated circuits, established by the Automotive Electronics Council. ISO 26262 defines standards for functional safety applied to safety-related systems that include one or more electrical and/or electronic systems.

-40˚C to +150˚C (ambient). The solutions are robustly designed and rigorously tested in compliance with AEC-Q100 and ISO26262.

Redundancy schemes (e.g. dual-core lockstep) are adopted to detect errors and seamlessly switch to the redundant device should a primary device become non-functional. In addition, redundant cell arrays and error correction circuits are implemented to further ensure reliability.

To achieve zero failure rates, the following design techniques are employed.

- FMEA, FTA and DFA [2] analysis conducted to identify weaknesses and test modes (e.g. burn-in and high voltage stress tests) designed accordingly to screen out weak devices.
- Dual core lockstep scheme
- 2-cell-per-bit arrays, with strict tests done on individual cells
- Error correction circuits
- Error-alarm reporting or analog voltage monitoring test modes

Figure 1. eMemory IP design features for high-temperature requirement applications

IP Category	Application	Operating Junction Temperature	Failure Reduction	In-field Safety	Quality Analysis
1. High Temperature	Consumer or Industrial Grade	-40˚C - 150˚C	QM level	NA	BKM**
2. Zero Failure AEC-Q100 Grade 0	Automotive	-40˚C - 175˚C Read -40˚C - 150˚C PGM / ERS*	1. Comprehensive test modes. 2. ECC (Optional)	NA	FMEA
3. Functional Safety ISO 26262	Automotive with ASIL requirements	-40˚C - 175˚C Read -40˚C - 150˚C PGM / ERS*	1. Comprehensive test modes 2. ECC 3. Dual-Core Lockstep Design	1. Power-On Self-Test (POST) 2. Error report or Monitor Modes	1. FMEDA 2. Safety manual

*ERS (Erase) check is for NeoEE only
**eMemory's Best Know Methodology standards on cell device, circuit design, layout design skills and design for testing (DFT).

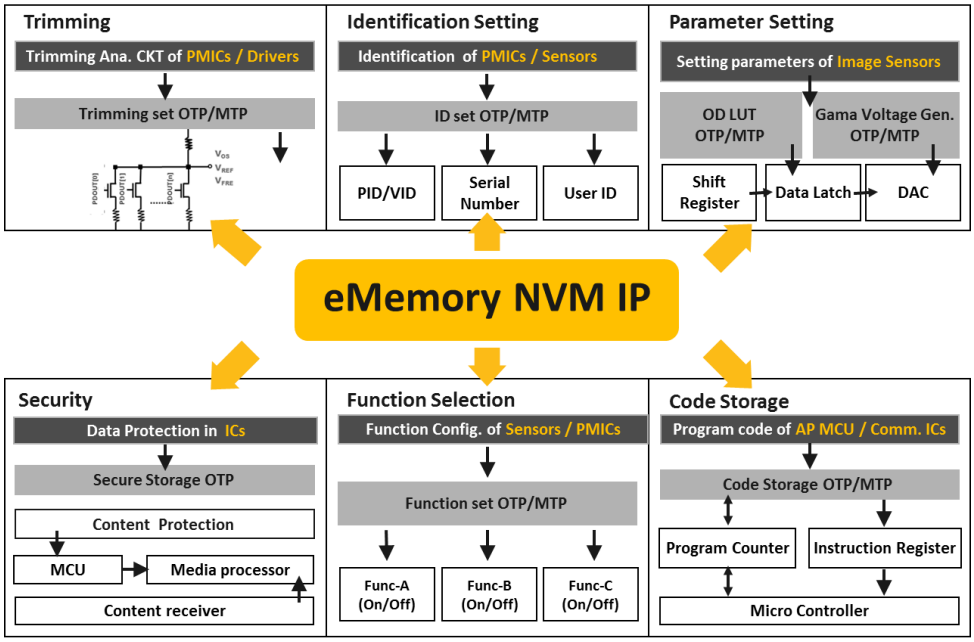
2. FMEA: Failure Mode and Effects Analysis; FTA: Failure Tree Analysis; DFA: Dependent Failure Analysis

eMemory IPs have passed AEC-Q100 qualification tests including HTOL, ELFR and HTSL[3] with zero failure rates. Quality analysis materials such as FMEDA[4] and safety manuals are prepared in compliance with ISO26262, and can be provided to accelerate design in and time to market. Last but not the least, we can tailor to customer needs and add more safety functions in IP blocks.

Use of eMemory IPs in Automotive Applications

IC circuit design involves defining parameters for input and output signals. These parameters are stored and allowed for last-minute changes using eMemory's programmable OTP and MTP.

Figure 2. Examples of eMemory NVM usage in automotive applications



3. HTOL: High Temperature Operation Life; ELFR: Early Life Failure Rate; HTSL: High Temperature Storage Life
4. Failure Modes, Effects, and Diagnostic Analysis

Other functions of eMemory's IPs include trimming, function configuration, FW/SW code storage, device ID setting and security. With the programmable NVMs, designers can accurately trim reference voltages, current, analog circuitry performances etc.

Embedded NVM can also help improve yields of display drivers ICs by trimming liquid crystal gamma curves at board level. Another use case is for power management ICs to store and program power up sequencing.

eMemory offers four embedded programmable NVM solutions, with different memory densities and write cycle endurances. The IP solutions can be customized to meet specific requirements for targeted applications.

- NeoBit: a OTP solution using floating gate technology, ideal for applications requiring medium density and endurance, available from 0.5um to 55nm.
- NeoFuse: a OTP solution using anti-fuse technology, suitable for applications at advanced nodes, available from 0.11um to 16nm.
- NeoEE: a EEPROM solution using floating gate technology, needed for high-endurance applications (max. over 500K cycles).
- NeoMTP: a MTP solution using floating gate technology, featuring higher density (max.512K).

From 0.5um to 7nm

As a leader in the industry, eMemory has had its NVM IPs embedded in over 17 millions of wafers shipped worldwide since 2002. The IPs are widely adopted by worldwide customers for competitive advantages including reliable technologies, small macro size, wide availability, and quality design services. Our IPs are compatible to standard logic CMOS processes without the need for additional masks or process steps, helping accelerate development and time-to-market.

While tests can be done at design and CP levels, designers often need to modify deviated device settings following chip packaging or assembling. They might also need to write in device ID and security codes at the assembling phase. Our NVM solutions support read/write throughout product lifecycles, from chip manufacturing, packaging, assembling all the way to in field, with write cycles ranging from 10 to over 500K.

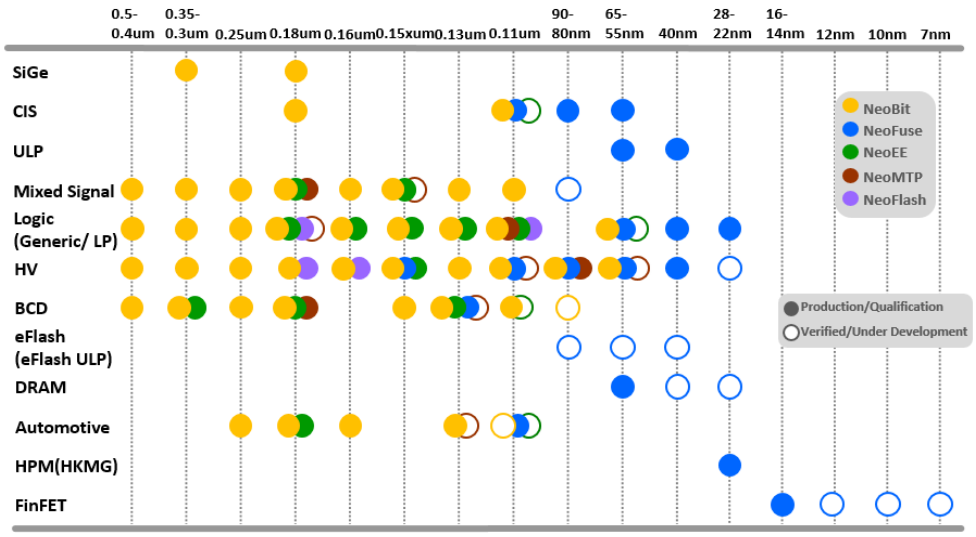


Figure 3. eMemory Technology Roadmap

eMemory's technologies have extensive production records, geometrically spanning from 0.5um, 0.18um to 16nm and covering platforms including BCD, mixed signal, HV and automotive. We have also completed 7nm OTP silicon function checks with fairly positive results.

For automotive applications, our NVM technologies have been qualified and in mass production at 0.25um, 0.18um and 0.13um, and developments for 16/12nm FinFET process technologies are well underway.

Secure Connected Cars with Chip-Unique ID

Modern cars are increasingly interconnected and autonomous, which in turn introduces additional cyber attack vulnerabilities. To protect the connected cars, it is essential to safeguard in-vehicle electronic systems and data stored in it.

In-vehicle OTP must contain security features to prevent against unauthorized readout of critical information such as crypto keys, user information and software codes. eMemory's antifuse OTP solution NeoFuse, certified by worldwide third-party CAs, provides a secure storage against wide-ranging attacks and is increasingly used as a replacement of attack-prone eFuse.

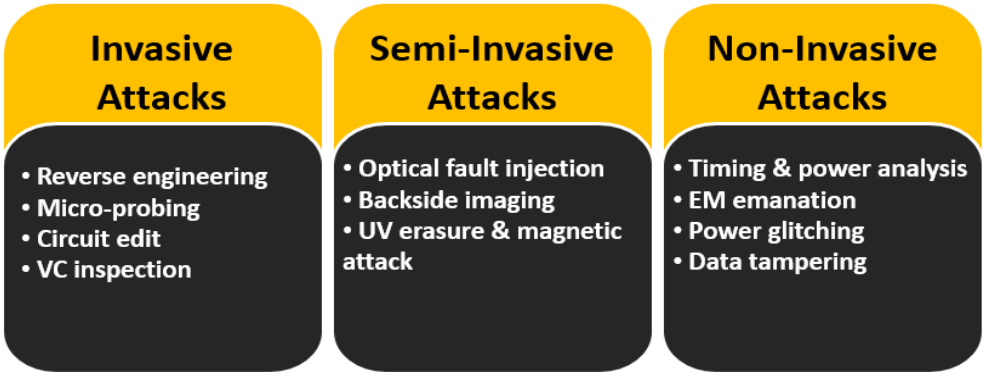


Figure 4. Immune to the attacks with NeoFuse secure storage

For more deep-rooted security implementation, eMemory offers the NeoPUF solution, a silicon-based root of trust unique by each chip. The solution is based on unclonable physical characters of integrated circuits originated from process variations. The chip-embedded security is able to avoid risks of conventional technologies by minimizing human interferences.

Turning the physical characters into digital, the NeoPUF solution provides a chip-unique ID or an entropy source which can enable cryptography applications such as authentication, encryption and key exchanges.

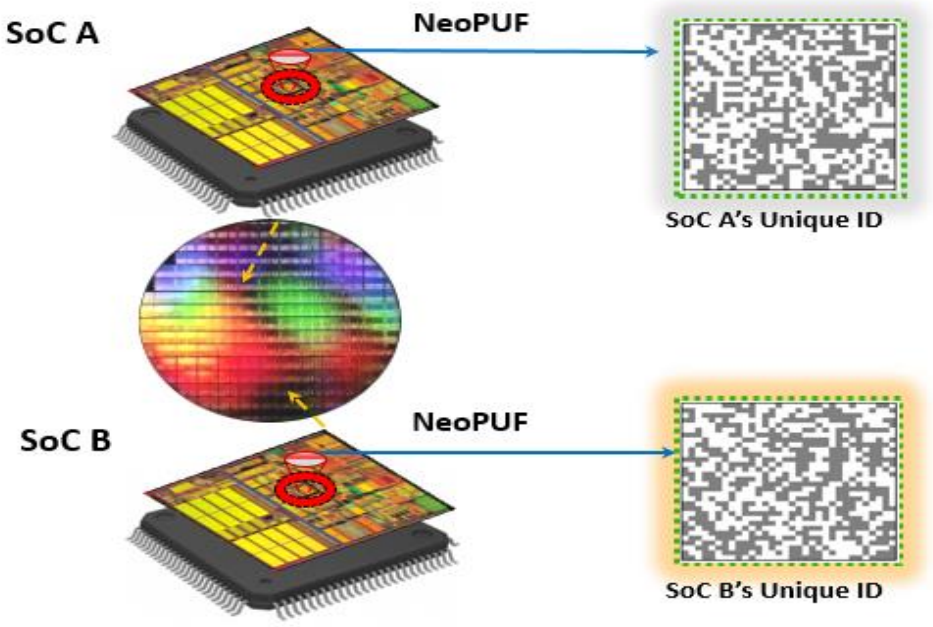


Figure 5. Every chip with a unique ID derived from its physical characters

High-grade automotive parts are frequent targets for counterfeiters. With car safety at stake, automotive chips can be nothing but authentic. It is not sufficient to use serial numbers or other forms of ID assigned externally. A chip-unique ID embedded from the very beginning at the design phase can best guarantee authenticity of a chip.

Aside from providing a Chip-unique ID, the NeoPUF solution can also enable secure boot and secure on-board and external communication. It can restrict access to critical components of the vehicle, preventing core operations being compromised. It can also be used to protect sensitive data stored in cars, and enable authentication processes at firmware updates

Conclusion

Today's vehicles are able to optimize its operation and maintenance as well as the convenience of its passengers using various onboard electronic systems. From infotainment to ADAS, the adoption of embedded NVM is growing rapidly in automotive, though challenges remain with the industry's demand on quality and reliability.

eMemory's OTP solutions (NeoBit and NeoFuse) and MTP solutions (NeoEE and NeoMTP) are designed to reliably retain data for 10 years at temperatures from -40°C to +150°C (ambient). The solutions are robustly designed and rigorously tested in compliance with AEC-Q100 and ISO26262.

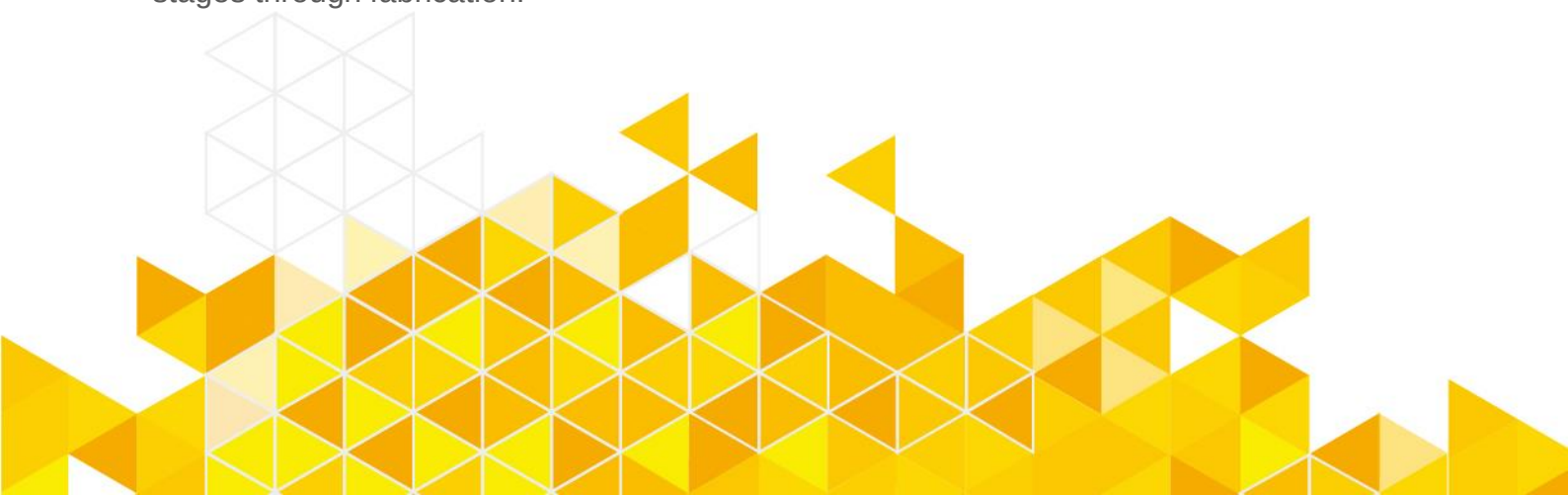
To design zero-failure NVM solutions, redundancy schemes (dual-core lockstep, 2C1B arrays) are adopted, and error correction circuits are also implemented. Our IPs have passed AEC-Q100 qualification tests including HTOL, ELFR and HTSL with zero failure rates.

For vehicular security, eMemory offers the NeoPUF security solution, which can prevent against component counterfeiting as well as enable crypto applications such as authentication, encryption and key exchanges by providing a chip-unique root of trust.

By 2020, around one in five vehicles on the road worldwide will have some form of wireless network connection, according to Gartner. The more than 250 million connected vehicles need reliable IP solutions, and eMemory is well positioned to provide best-in-class services with its zero-failure design capabilities.

About eMemory

eMemory is a global leader in logic process embedded non-volatile memory (eNVM) silicon IP established in 2000. eMemory has devoted itself to research and development of innovative technologies, offering the industry's most comprehensive platforms of patented eNVM IP solutions which are supplied to semiconductor foundries, integrated devices manufacturers (IDMs), and fabless design houses worldwide. eMemory's eNVM silicon IPs support a wide range of applications, including trimming, function selection, code storage, parameter setting, encryption, and identification setting. The company has the world's largest NVM engineering team and prides itself on providing partners with a full-service solution that sees the integration of eMemory eNVM IP from initial design stages through fabrication.



ememory

Embedded Wisely, Embedded Widely

eMemory Technology Inc.
8F, No.5, Tai-Yuan 1st St., Jhubei City, Hsinchu County 30265 Taiwan
T +886-3-5601168 F +886-3-5601169
www.ememory.com.tw