MACRONIX

The Role of Secure Flash Memory in Automotive Applications

Anthony Le

Vice President Marketing

Macronix America

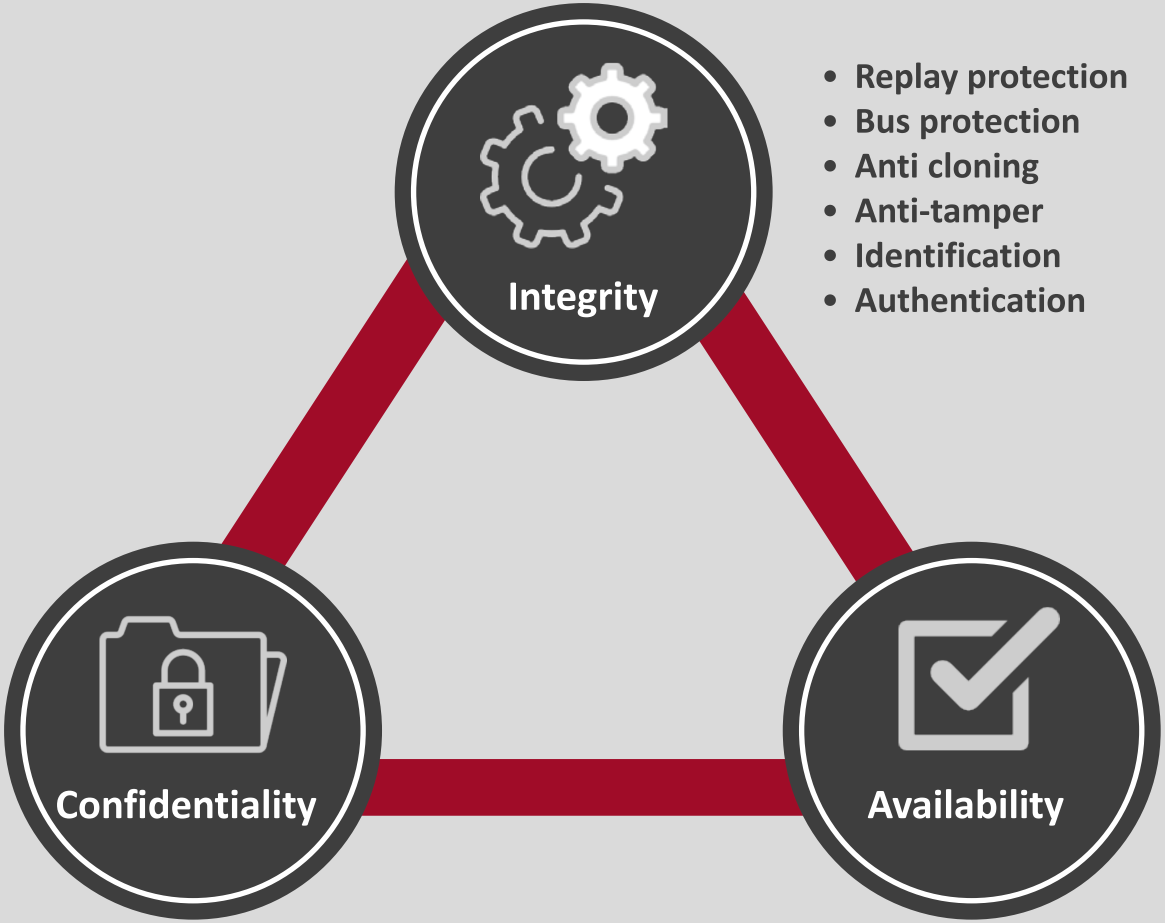
August 6, 2019

MACRONIX

Agenda

- Security Objectives
- Why Secure Flash in Automotive?
- Types of Information that Needs to be Kept Secure
- Flash Comparisons
- Conclusion

Security Objectives in Auto Designs



Integrity

- Replay protection
- Bus protection
- Anti cloning
- Anti-tamper
- Identification
- Authentication

Confidentiality

- Secure storage
- Secure boot
- Secure data exchange

Availability

- Access Management

Why Secure Flash in Automotive?

- ADAS and electrification functions/features in automobiles rapidly growing
- Exponential rise in stored data, particularly in ADAS functions
- Connectivity to public networks creating a unsecure environment
- More onboard pay-for-use apps and capabilities requiring numerous authorization credentials
- Auto as a payment platform on the rise (Tolls, Parking, etc.)
- Strong correlation with security and safety and a need for deterministic behavior
- Support for Root of Trust (RoT) requirements through unique ID, authentication, and an encrypted link
- ***Traditional embedded flash densities are increasingly becoming inadequate to store all this data***

Flash Comparisons

	eFlash	External SPI Flash	Secure Flash
Interface	Parallel	Standard SPI	Standard SPI (with ArmorFlash)
Density Options	Low	High	High
Information Confidentiality	Usually Strong	Weak	Strong
Information Integrity	Usually Strong	Weak	Strong
Security Availability	Usually Strong	Weak	Strong

Opportunities for Hacking

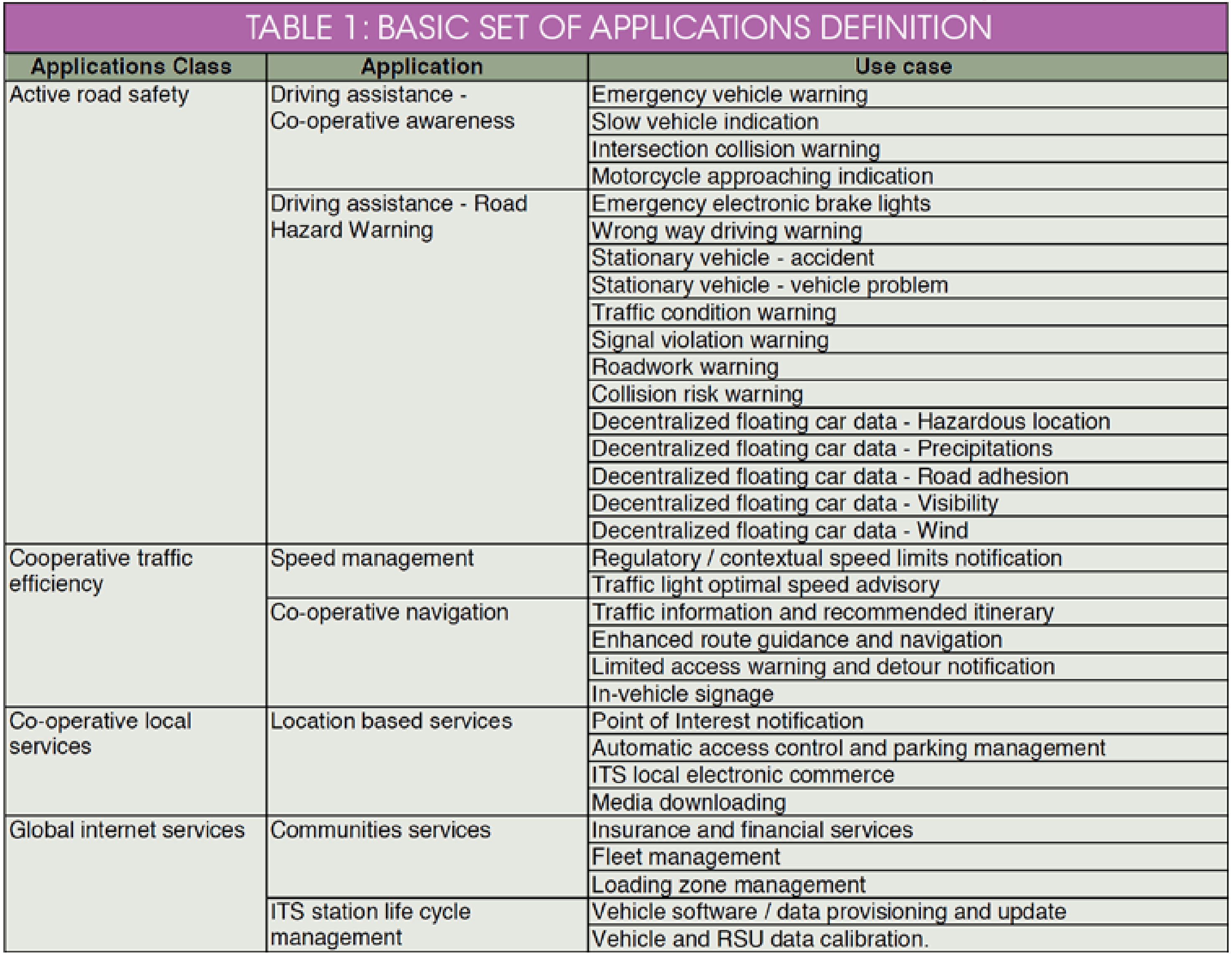


TABLE 1: BASIC SET OF APPLICATIONS DEFINITION

Applications Class	Application	Use case
Active road safety	Driving assistance - Co-operative awareness	Emergency vehicle warning
		Slow vehicle indication
		Intersection collision warning
		Motorcycle approaching indication
	Driving assistance - Road Hazard Warning	Emergency electronic brake lights
		Wrong way driving warning
		Stationary vehicle - accident
		Stationary vehicle - vehicle problem
		Traffic condition warning
		Signal violation warning
		Roadwork warning
		Collision risk warning
		Decentralized floating car data - Hazardous location
		Decentralized floating car data - Precipitations
		Decentralized floating car data - Road adhesion
		Decentralized floating car data - Visibility
		Decentralized floating car data - Wind
Cooperative traffic efficiency	Speed management	Regulatory / contextual speed limits notification
		Traffic light optimal speed advisory
	Co-operative navigation	Traffic information and recommended itinerary
		Enhanced route guidance and navigation
		Limited access warning and detour notification
		In-vehicle signage
Co-operative local services	Location based services	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet services	Communities services	Insurance and financial services
		Fleet management
		Loading zone management
	ITS station life cycle management	Vehicle software / data provisioning and update
		Vehicle and RSU data calibration.

The ETSI TR-102-638 Intelligent Transport Systems technical report exemplifies that the opportunities for hacking are enormous

Some Examples of Information Being Stored in Automobiles

Keys

Authorized users & access levels

Secure Logs

Medical info.

Passwords

Credentials

Certificates

Financial / eCommerce information

Vehicle experience authentication keys to unlock additional capabilities

Contacts

DRM
(Digital Rights Management)

Device identity / identities

Audio/video streaming

Biometrics
(fingerprints, facial etc.)

Other Use Cases for Secure Flash

- Secure data storage along with code storage
- Design upgrades for security without changing CPUs/MPUs (or MPUs without secure embedded memory)
- Combining non-volatile memory with a secure element (lowering BOM costs)
- OS architectures with several users requiring multiple sets of credentials (multi-tenancy / hypervisors)
- Secure (re)provisioning in unsecure manufacturing environments or in the field
- Protecting firmware rollback and anti-cloning
- Securing against host/device ease-dropping and memory tampering

Conclusion

The growth of connected vehicles& ADAS applications continues to explode and along with it the exponential growth of data.

Safety and security
- A robust security framework protects against unauthorized actions taken by individuals, while improving safety by incorporating additional controls in the system design

Non-volatile memory requires a range of security mechanisms and policies to ensure identity, confidentiality, integrity, authenticity, and availability

Advanced secure memory storage features found in devices such as the Macronix ArmorFlash™, is a critical component to achieving security objectives in future automotive systems

Additional Reading

Integrating secure non-volatile in internet of vehicles article in Electronic Design magazine
https://www.electronicdesign.com/automotive/integrating-secure-non-volatile-memory-internet-vehicles-systems

MXIC

MACRONIX
INTERNATIONAL CO., LTD.