Safety & security architecture for automotive ICs

Yash Saini, Arun Jain - September 25, 2013

The automotive industry is changing rapidly to address the stringent requirements for safety and security of vehicular systems. Requirements are not only coming from customers, but regulatory authorities are also pressuring for greater safety and security in vehicles. The requirements include high bandwidth networks, improved data security, enhanced functional safety, and reduced energy consumption.

The ISO 26262 standard defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems. The standard is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems.

Automotive systems need to be protected against any real-time defects to make it safe for use. Real-time defects can include internal and external errors (e.g., the vehicular communication network).

Automotive data security ranges from vehicle theft protection to enabling secure communication with external devices such as smart phones, MP3 players, or navigation devices. Security also means protection against hackers. After gaining access, a hacker could control everything from the entertainment system to braking.

Safety options for automotive chips

Below are few options to facilitate safety at the chip level.

1) Redundant Critical Hardware Modules
Redundant critical on-chip modules like processor, DMA controller, internal clock generator, and communications peripherals can improve reliability should a primary hardware module become non-functional while the vehicle is running. Such a system can have in-built error detection mechanisms and on-the-fly switching to redundant hardware to mitigate threats to passenger safety.

But this kind of redundant hardware architecture comes with the penalty of increased area and higher power consumption in silicon. Area penalties can be minimized by intelligent selection of which functions need to be duplicated in silicon. Power can be minimized by adopting power and clock gating in the redundant modules. Some redundant modules can be implemented in lock-step of each other, where primary and redundant modules process the same input. Mismatch in the output of the lock-step modules indicates a defect in either of the modules. The system can switch itself off or take appropriate safety measures to avoid any real-time failure. Redundant hardware should be placed quite far in silicon from the primary hardware module to avoid tampering of both modules together.

2) Self-Corrective Hardware

Chips can implement hardware monitors to detect failures. Faults like loss of lock in a PLL, sudden temperature change, change in clock frequencies, change in signal/power voltage levels, etc. can be monitored with such implementations. SoCs can intelligently control these faults and take self-corrective measures to safeguard users.

3) Glitch Filters

Spurious events at input pins can cause functional failures to a chip. Critical pins like reset and interrupt can have glitch filters to stop noise and transient spikes from getting in.

4) Watchdog Timers

SoCs can have timers which will bring a processor or any other controller out of a hung situation by making them transit to a safe state. It can implement a safety feature to execute a task periodically. Timers can specify a period in which a task needs to be executed. If that task does not get executed in the predefined duration, the system is assumed hung. Thus, the SoC can monitor the execution of the task and take appropriate safety measures.

5) Logic & Memory BIST

Functional safety standards for automotive chips like ASIL (Automotive Safety Integrity Level) recommend BIST (Built-In Self-Test) to be part of a chip. Before transitioning to functional mode, it goes through logic and memory-BIST to assure that the chip has not encountered any manufacturing or aging faults. Chips can implement BIST for critical modules like hardware monitors to detect any dormant faults. Chips can even implement a controller to control and manage the BIST operations.
6) ECC and CRC

Data integrity is a requirement for making safe & secure vehicular networks. CRC (Cyclic Redundancy Check) mechanisms provides reliable data communication inside & outside of the system. ECC (Error Correcting Code) mechanisms not only provide detection of multi-bit errors in data transmission, but are also able to correct smaller bit errors.

Security options

Vehicle security relies significantly on the electronics of the automotive system. Hence it is extremely important to safeguard the electronic system and data stored in it. Below are a few options for securing the vehicular system.

1) Locking the system

A system can be locked to avoid manipulation of configuration data that would disrupt the proper functioning of the chip. A password mechanism can be deployed to unlock and enable reconfiguration. This is a simple and cost-effective single-tier security measure.

2) Prevent write, read, and erase of flash memory

Chips can implement security features to protect memory data. On & off-chip flash memories are protected to avoid unauthorized erase, read, and write access. Failing to do so can expose a system to various types of attack which seek to extract the information stored or transported across vehicular communication networks.

3) Register Protection

There may be modules in the design whose configuration should not change during the run phase of the chip, and in doing so may affect the proper operation of the system. One can disable access to these registers during run phase, or make such registers as write-once.

4) Secure Boot

An automotive system gets configured during boot phase to run the application. Some may have an option to boot using code stored in external memory. In such systems, an IC can have a mechanism to prevent booting with spurious code. During boot, part of the sequence requires the security device to verify the signature accompanying the application. Only if the verification succeeds does the application gets executed.

5) Secure Debug and Test

To ease the testing and development of firmware, SoCs are provided with test and debug ports, and in doing so, designers are exposing the SoC configuration to the external world. Such exposure can be used by hackers to manipulate the chip functions and compromise safety. Therefore, there should be a mechanism to lock the debug & test feature by default, unless a password is written to unlock it.

Conclusion
With increasing use of electronic systems in vehicles for managing critical functionality, the requirements for safety and security in automotive chip architecture is becoming paramount. Safety can be ensured by the proper functioning of chip during run-time via detection & rectification of random failures. Security prevents theft of data and IP by reverse engineering. Security also ensures that a hacker is not able to manipulate the system to disrupt normal functionality, which may have a severe impact on passenger safety.

Today, automotive chip designers are required to implement safety & security features in addition to the general functionality of the chip. Once a designer identifies the level of safety & security required by the market, they can explore the spectrum of solutions discussed above to select the ones that meet the industry’s standards and the customer’s requirements.

References

- Freescale SafeAssure program
- Freescale security technology
- ISO 26262

Also see:

- Connected cars: Managing and securing data exchange and processing
- Testing safety-critical automotive parts
- Security module protects automotive electronics from hacking and tampering
- TI introduces SafeTI Compiler Qualification Kit to ease functional safety development for automotive and medical
- Virtual Prototyping Benefits in Safety-Critical Automotive Systems
- Virtualizer Development Kit for Freescale’s Qorivva family boosts automotive ECU design
- ISO26262 in automotive IC development: is it just a tick-box exercise, or does it induce manufacturers to make safer components?