

Radar and Functional Safety technology for advanced driving assistance

Yves Legrand (Freescale Semiconductor)

This presentation will describe advanced development in 77 GHz radar technology, enabling smaller and better collision avoidance systems. Then new development in functional safety chipset solution, MCU and analog, will be explained. The combination of these technologies forms a comprehensive safe solution for advanced driver assistance or autonomous driving. The development of these technologies is driven by the automotive market and can be redeployed to many other types of mobile machines.

Radar systems will become more and more prevalent in cars in the near future. They offer a number of comfort and safety applications. Short range radar from a few centimeters up to 30 meters can be used for blind spot detection, backing aid or parking slot measurement to guide the car to self-park. Long range radar up to 250 meters can be used to enable an adaptive cruise control aligned with the speed of the preceding car. More critical functions can be enabled such as collision warning, emergency braking and even pre-crash sensing that could trigger seat-belt tensiometer or other active and passive safety features. With these later functions, it is obvious that the electronic control system needs to reach highest functional safety level as the system will eventually steer or brake the car without the driver intervention.

The advance in this radar technology development can be leveraged in other applications such as mobile industrial machine, cranes, factory safety equipment where an area needs to be closely protected. Coupling radar with machine vision can also create a powerful combination with both technologies supplementing each other in order to create more accurate and reliable systems. Radar works through rain, fog and dirt when vision does not. Radar also extends further in distance and event in non direct line of sight. A system combining vision and radar with some smart sensor fusion algorithm could leverage the benefits of both sensing technologies.

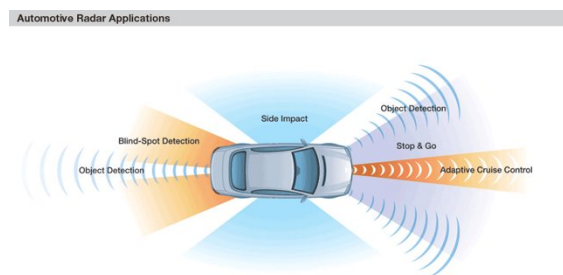


Figure 1: Automotive Radar Application

77 GHz Radar Technology

In a collision warning system, a 77 GHz transmitter emits signals that is reflected from objects ahead and are captured by multiple receivers integrated throughout the vehicle. The transmitter emits a frequency modulated continuous wave signal, meaning that the frequency varies up and down over a fixed period of time by typically a triangle wave signal. Since radio waves propagate at constant speed of light, distance can be calculated by measuring the frequency difference between the transmitted and received waves knowing the frequency slope over time. Speed measurement uses the Doppler effect which uses the difference between the observed reflected signal frequency and the emitted frequency.

Radar systems are not new. What is new is that car makers want to include them in medium line kind of cars in a few years, so the system has to be really low cost and high quality. This is a big shift from specialized and costly radar systems to standard car equipment type. The challenge is then to reduce cost while actually improving quality and defect part

per million. This shift is illustrated by the quality versus cost marketing value map.

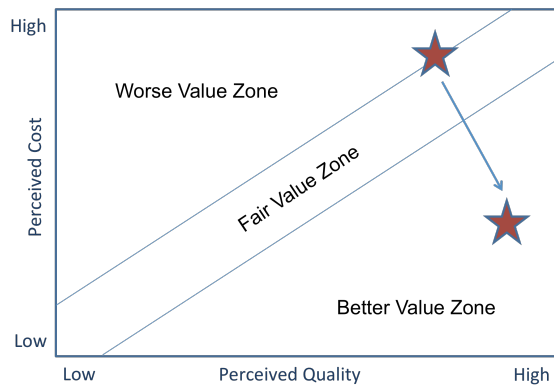


Figure 2 : Marketing Value Map

This marketing value map illustrate the shift from a high cost and good quality system to medium / low cost with even greater quality. To achieve this many challenges have to be addressed.

Radar cost and quality challenges

Traditional radars use a rotating antenna. This is how the spatial mapping of object is done. This might be OK for large system with expensive control system but certainly not for volume car production. One solution to eliminate rotating antenna is to use phased array or patch antenna with multi channel transmit and receive channels. Spatially separated antenna will receive reflected signals with a slight time difference. That difference is then used to reconstruct the object position without the need of a moving antenna. The drawback of the patch antenna is that several Tx and Rx channels are needed to be connected to the antennas. A typical system will use something like 4 Tx and 16 Rx antennas. Duplicating Rx and Tx circuitry 16 and 4 times is not economically viable.

This is where another piece of innovation comes to the rescue. Instead of using discrete RF circuitry, Freescale has developed a specific RF BiCMOS process with enough performance to integrate 77 GHz RF circuitries into a single chip. Starting from a high performance Silicon Germanium Carbide (SiGe:C) 180 nanometer process, Freescale has developed a specific 300 GHz Fmax RF transistor capable of handling the 77 GHz radar signals on chip. Together with

analog and digital CMOS circuits, this process enables a comprehensive integration of multi channel 77 GHz system on chip. So the multi channel cost overhead is absorbed by the on chip integration.

Advanced Packaging Technology

Having 77 GHz solid state silicon process is a great asset but handling it and reporting it on a printed circuit board is another challenge. At these high frequencies traditional package parasitic impedance can destroy the signal information. One way to cope with this problem is to use bare die soldered on specific PCB with precision wire bonding techniques and not typical packages and wave soldering meaning higher cost. Here again new advanced packaging technology called Redistributed Chip Package ⁽¹⁾ (RCP) comes to the rescue.

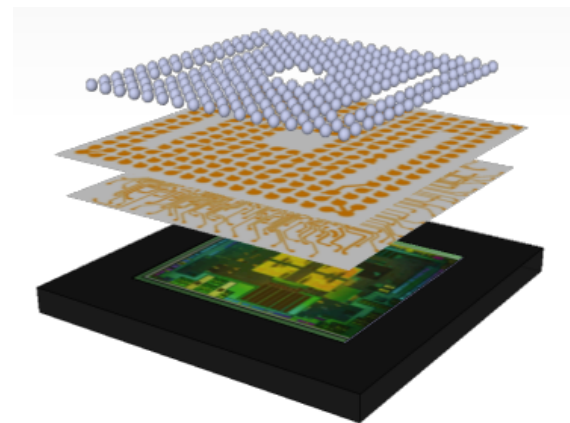


Figure 3: RCP package build-up layers

RCP uses coarse lithography technology to build up copper interconnect layers on top of a die or multi-dies system instead of using PCB type materials. This substrate-less packaging technology has much lower capacitive and inductive parasitic behavior. It is then possible to route high frequency signals at 77 GHz through this package with acceptable performance compared to the bare die soldering process. The advantage is that traditional PCB tool set can be used to solder this parts; meaning low cost processing.

With this process and packaging technologies Freescale is designing

integrated transmitter and receiver radar circuits.

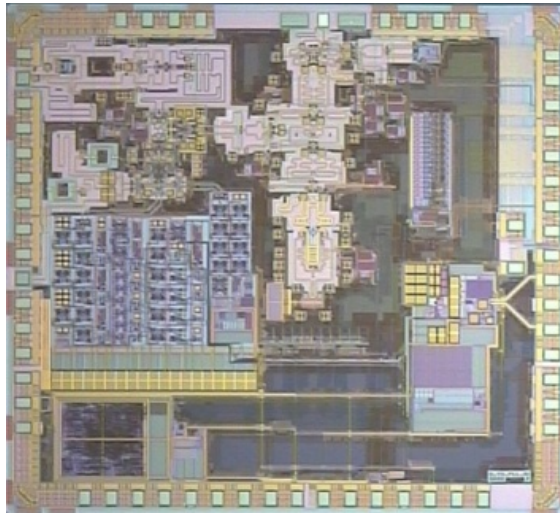


Figure 4: 77 GHz radar transmitter die

The Transmitter integrates a 77GHz frequency synthesizer, a VCO at half the frequency, a 10GHz fractional N PLL, and a Power Amplifier with a 28 bit sigma delta modulator. This comes with specific ESD protection (RF and DC) and digital control through a SPI interface.

On the receiver side, we integrate typically 4 receive channels with a local oscillator at 38 GHz, and differential IF output. Typical noise figure of 13 dB is achieved without the need of a low noise amplifier. This helps keep power consumption low with high linearity.

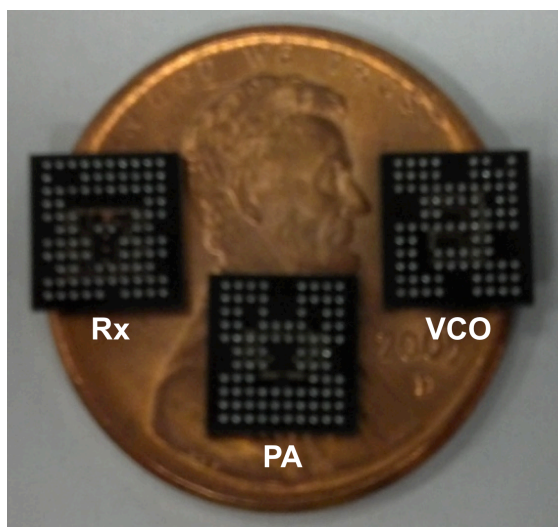


Figure 5: RCP packaged radar chip set

Functional Safety Microcontroller

A microcontroller is used to control the RF radar transmitter and to process the data coming from the receiver. Given the critical safety nature of the application, a functional safety MCU is used. The challenge for system engineers is to architect their system in a way that prevents dangerous failures or at least sufficiently controls them when they occur. Dangerous failures may arise from:

- Random hardware failures
- Systematic hardware failures
- Systematic software failures

The functional safety standard IEC 61508 and its automotive adaptation ISO 26262 are applied to ensure that electronic systems in general industry and automotive applications are acceptably safe. The IEC 61508 document defines four general Safety Integrity Levels (SILs) with SIL 4 denoting the most stringent safety level. The ISO document defines four Automotive Safety Integrity Levels (ASILs) with ASIL D denoting the most stringent safety level. Each level corresponds to a range of target likelihood of failures of a safety function.

There is no direct correlation between the SIL and ASIL levels, but the ISO 26262 takes the safety process and requirements to a deeper level. From the beginning of the design process, evidence must be collected to show that the product has been developed according to regulation standards. Any potential deviations that have been identified must be documented to ensure that adequate mitigation is in place.

They are different ways to implement safe MCUs. The traditional technique is to use two separate MCUs to duplicate the software on physically different controllers. The same software can be run identically on each MCU and then the results are compared. If they are the same all is good, if not then the system knows there is an error and either solves it and/or puts the system into a safe state. Another option is that one MCU only runs safe software and monitor the other MCU which is running the application software.

With separate MCUs the system designed has to design and implement from scratch the safety system.

On the opposite, there are now pre-certified MCU solutions available. These solutions focus on detecting and mitigating single-point faults, latent faults and dependent faults. This is achieved through built-in safety features, including self-testing, monitoring and hardware-based redundancy in the MCUs, but also power management ICs and sensors. For the MCU on-chip redundancy is offered for the critical components such as:

- Multiple CPU computational cores with delayed lockstep
- I/O processor core
- Direct Memory Access controller
- Interrupt controller
- Dual crossbar bus system
- Memory protection unit
- Fault collection unit
- Flash memory and RAM controllers
- Peripheral bus bridge
- System and watchdog timers
- and end-to-end Error Correction Code

The main benefit of this sphere of replication is the capability of the MCU to detect single point failures that tend to occur more frequently as soft errors, not only in the cores but also in key sub-modules.

Built-in self test (BIST) mechanisms are also provided for the cores, memories, crossbars, communication blocks and peripherals. In addition, the device is optimized for prevention of common cause failures induced by clock or voltage supply issues. The MCU provides hardware blocks for detection of clock deviations as well as hardware monitors for main voltages such as internal core voltage and Flash supply voltage.

Dual-core lock-step MCUs do not alleviate the need to implement safety measures at SW level and at system level, such as sufficiently independent monitoring of output values calculated by the SW path. However, among other aspects, such as higher integration, these MCUs do offer a separation of concerns for validation. In solutions based on multiple single-core

MCUs the ability to detect and control random hardware failures depends largely on the SW.

For a dual-core lock-step MCU, it is possible to verify and validate key functional safety-related properties of the computational infrastructure at the hardware level independently from the SW since the computational infrastructure is offered in an integrated form and represents an integrated safety mechanism. This is a significant benefit within the HW/SW co-design process. Furthermore, the separation of concerns facilitates faster location of issues. If the safety mechanisms monitoring the dual-core lock-step trigger then the cause can most likely be attributed to random hardware failures at the HW level, while if the SW monitoring triggers then the cause is most likely to be a fault at system level or a systematic fault within the SW.

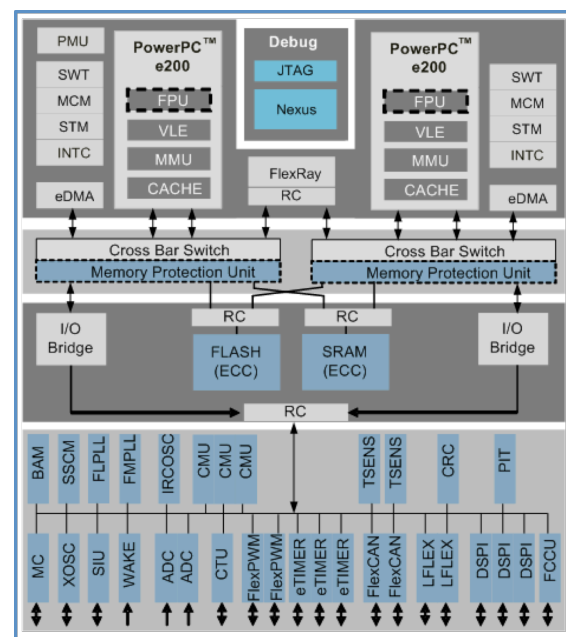


Figure 6: Dual-core lock-step MCU block diagram

The dual-core lock-step MCU approach offers a potential availability advantage. In modern MCUs, the core area is diminishing well below 5 percent of the overall MCU, while the MCU as a whole is typically allocated a budget of approx 1percent contribution to the Probabilistic Metric for random hardware failures (PMHF). Hence, the contribution of the core is at first approximation in the region of 0.05 percent. However, certainty about

the correct operation of the cores is key for any forward recovery technique implemented in SW to address the remaining 99.95 percent of contributions to the PMHF in order to maintain availability of the system. Additionally the dual-core lock-step MCU provides an appropriate infrastructure to implement multiple sufficiently independent channels.

Functional Safety Companion Device

To support a total system solution for functional safety applications, a class of companion power system basis chips (SBCs) combining both safety monitor role for the MCU and power supply generation has been developed.

These SBC devices provide power to MCUs and other system loads and optimize energy consumption through low-power saving modes. They also typically integrate physical layers interfaces and a serial peripheral interface to allow control and diagnostic with the MCU. The combination of the MCU and analog system basis chip, designed as a Safety Element out of Context (SEooC), facilitates the assessment of the safety of a system. This architecture enables the number of components at the system level to be reduced, addresses the functional safety requirements and increases reliability.

Four safety measures are implemented to secure the interaction between the MCU and SBC:

- uninterrupted supply
- fail-safe inputs to monitor critical signals
- fail-safe outputs to drive fail-safe state
- and watchdog for advanced clock monitoring

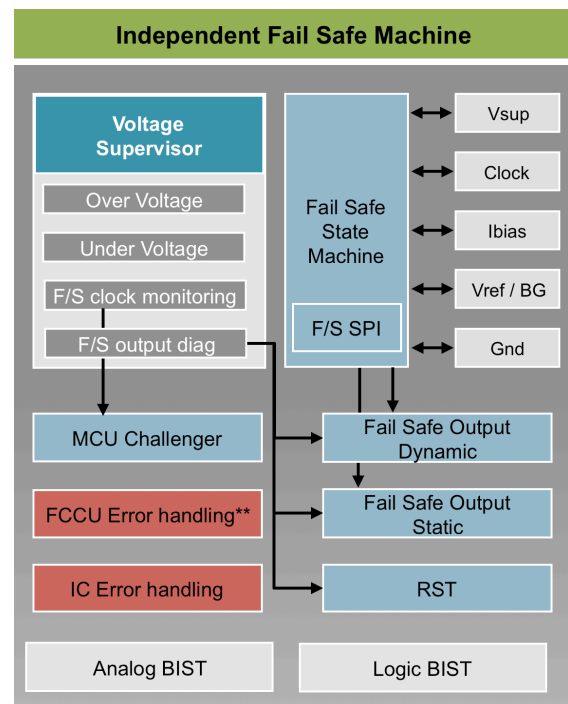


Figure 7: SBC Fail Safe Machine

When combined with the MCU, each safety measure is optimized for the highest level of safety performance. At the system level, safety check mechanisms proposed by the MCU can be monitored by the SBC device through the bi-stable protocol of the Fault Collection Control Unit (FCCU). This IC cross-checking, like the challenger for monitoring timing, provides external measurement of the system and offers a redundancy to further secure fault detection. In line with safety architecture of the system basis chip family, a redundant path for safety state activation occurs through dedicated fail-safe outputs. These outputs complement the MCU fail-safe outputs by setting the application into a deterministic state when a failure condition occurs.

These hardware implementations help software engineers simplify the software architecture and implement a software development strategy that focuses on safety using a single MCU approach.

System versus chipset compliance

Functional safety compliance is achieved at system-level which is the responsibility of the system designer. The MCU and SBC chip set are designed independently

of its final application which can be a parking car system, Advanced Driver Assistance System or a moving crane. The chip set is thus developed by treating it as a safety element out of context (SEooC). An SEooC is a safety-related element which is not developed in the context of a particular vehicle function or end application. We can then follow the tailored guideline for developing SEooC components from the ISO26262 specification.

systems that comply with ISO 26262 and IEC 61508 standards and to simplify the process of system compliance, with solutions designed to address the requirements of the specific automotive and industrial functional safety standards.

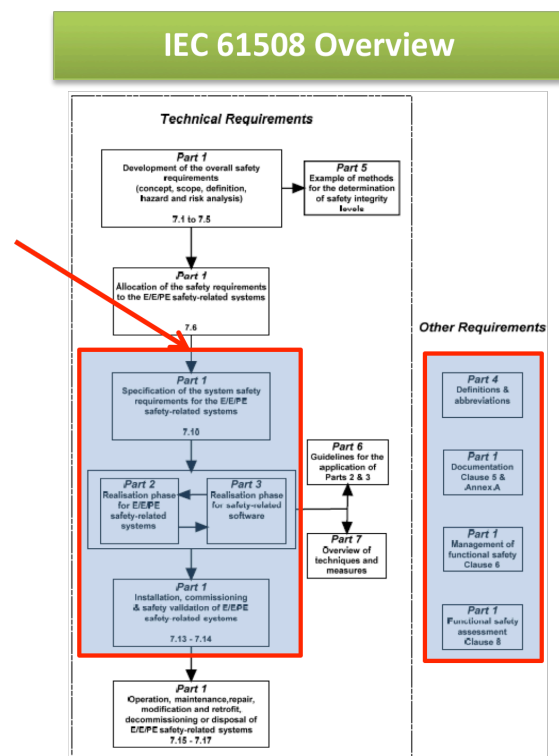


Figure 8: Chipset IEC applicable area

Freescale has summarized its initiatives to support the functional safety needs of the market under the SafeAssure brand. It covers safety support, safety hardware, safety software and a safety process to ensure that procedural aspects are covered adequately during the development phase of the various products. Typical deliverables will include:

- Safety Analysis of Architecture: FMEDA, CCA or FTA
- User Guide: Safety manual, safety application notes
- Development Process evidence: PPAP, Safety Plan, Certificates

The objective is to reduce the time and complexity required to develop safety

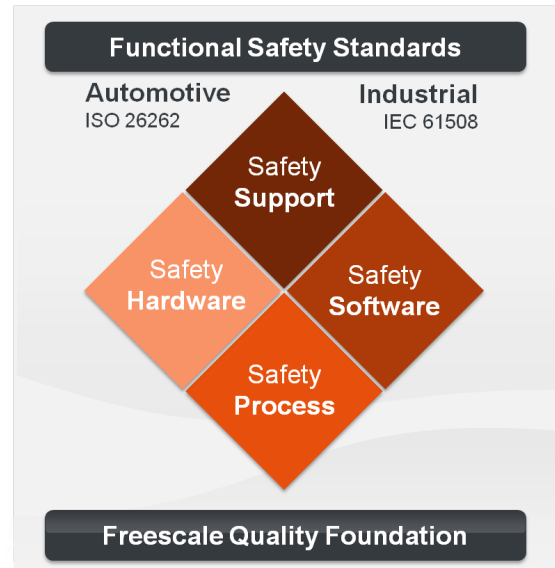


Figure 9: Freescale Safe Assure Program

(1) Freescale is licensed by EPIC Technologies Inc. to make and sell packages that include EPIC's "Chips First" technology and other related patents

Yves Legrand
 Freescale Semiconductor
 134 avenue du Général Eisenhower
 31023 Toulouse, France
 Phone: +33 5 61 19 17 96
 yves.legrand@freescale.com
 www.freescale.com

References

- [1] EE Times, Christopher Temple, Freescale Semiconductor
- [2] Freescale.com/safeassure