ISSN 2348 – 9928
IJAICT Volume -1, Issue-3, July 2014 Doi:01.0401/ijaict.2014.01.12 Published Online 05 (05) 2014

EMBEDDED JUST DRIVE FOR AUTOMOTIVE APPLICATIONS USING CAN AND ANDROID IN SUPPORT WITH FPGA INTELLIGENCE

Ms. M. Shalini Pushpa
PG Scholar, Embedded System Technologies,
GKM College of Engineering and Technology
Chennai, Tamilnadu, India

Abstract— ***Society is becoming increasingly dependent on embedded computing and sensor technology to enable complex networks of autonomous systems, such as robots, unmanned aerial vehicles (UAVs), self-driving cars, and unmanned underwater vehicles (UUVs). Infact, several recent developments highlight the realization of advanced autonomous systems that were deemed science fiction just a few decades ago. Smart Just Drive for Automotive using embedded blue tooth is designed to provide comfortable feel to the user or passenger to check the vehicle status by reading different vehicle parameters like fuel levels, engine temperature etc., and remote by using Smart mobile with Bluetooth Connectivity. This is an inexpensive device which reduces the problem associated with anti-theft control as well. This tracking system is mainly composed of PIC18F4480 Microcontroller and a Bluetooth receiver. Automotive theft has been a persisting problem around the world and greater challenge comes from professional thieves. In this paper, we present an automotive security system to disable an automobile and its key auto systems through remote control when it is stolen. It hence deters thieves from committing the theft.***

Keywords— Automotive, CAN Bus, ECU, MEMS, Accelerometer.

I. INTRODUCTION

Automotive systems are nowadays complex distributed computer systems with various demands on networking capabilities. Moreover, regulations requiring emissions diagnostics together with the ever increasing in-car electronics further increase the number of applications relying on communications. Different automotive applications have different requirements on the networking capabilities, resulting in a number of networking protocols.

A modern car (automotive system) contains a lot of electronic devices (subsystems) such as advanced safety systems, power train control, sensors, and means for diagnostics. These subsystems have evolved over time, relying on various communication services provided by different networking technologies. For efficient, reliable operation of all system and sub systems, the vehicle has been networked using CAN network.Automobiles are designed around computers, storage, and software and are now as much an electronic system as a mechanical one. In a real sense, personal vehicles are also mobile consumer electronic devices. As a consequence, automobiles are becoming true applications platforms where users will download applications that can customize the features, performance, and the capabilities of the vehicle to suit the needs and desires of the consumer—today's car is "my car, my way."

1.1 Advanced Autonomous Systems

Three key technologies are needed to enable advanced autonomous systems. First, at least one embedded processor is necessary to guide and control a specific platform's activities. In many applications, the autonomous platform can possess more than one embedded processor, where each processor is assigned a dedicated task. For example, most vehicles on the road today possess at least 80 embedded processors, all of which are interconnected with each other.

Second, an array of sensors is needed to provide the autonomous system and its collection of embedded processors with situational awareness about the physical world. The embedded processors use this information to make the appropriate decisions about what actions the autonomous system should perform. The last necessary component is a communication system which relays information to and receives information from a command center as well as information shared by other autonomous systems that form part of the network.

Embedded processors in these complex autonomous systems often do not act alone, but rather in concert with each other. Consequently, information sharing between embedded processors within the same autonomous system or between two different systems is crucial for many

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.01.12 Published Online 05 (05) 2014

operations. As with many of these complex networks of systems, it's possible for external intruders to intentionally compromise the proper operation and functionality of these systems. However, unlike complex networks such as the Internet, where the issue of security has been extensively researched and funded, security issues surrounding complex networks of autonomous automotive systems haven't been as readily studied.

1.2 Automotive Computing & Sensing

Autonomous automotive systems require accurate situational awareness of the physical environment around them to function properly. As a result, we must leverage sensory information and control data together with available embedded- computing resources between the different platforms to enable reliable autonomy for these systems.

With researchers continuously discovering new security vulnerabilities for these platforms, research activities focusing on automobiles' physical security have the potential to be transformative and high impact given our growing reliance on this technology and its evolution into semi and fully autonomous platforms. Furthermore, research activities focusing on secure autonomous auto-motive systems span numerous research Concentrations in electrical engineering, computer engineering, and computer science, with many of the issues and their solutions lying at the boundaries of embedded processing, hardware security, robotics, sensor systems, cyber-physical systems, and communications.

Every action performed by today's automotive vehicles is increasingly being handled by a computing device called an electronic control unit. ECUs are responsible for various operations, from power locks, seat adjustments, and automotive stereo systems to power steering, fuel injection, and emissions control. Given the growing threat of attacks against these systems, researchers have been working on identifying security threats toward these ECUs, as well as with automotive sensor systems, with most experiments in this area involving conducting physical security attacks against an actual road vehicle. Similarly, many researchers have devised' 'hardware-in-the-loop'' computer simulations that incorporate the input and output data paths of automotive-components.

II. PROJECT DESIGN

Accounting to cars, the natural scenario is that, the vehicle parameters can be monitored only after entering inside the car. In the existing system, there is no remote monitoring of vehicle parameters. Parameters like Fuel level, Engine temperature and Tire pressure can be monitored in- vehicle only. This is merely a time-consuming process, since we tend to spend some time in monitoring soon after getting into the car. Various parts of automobile are connected with mechanical lever or unreliable wired network. Due to this system, the automotive controls may lead to unpredictable operation or effect. At present, only keys and smart card technology are pre-dominant to reduce vehicle thefts and prevent unauthorized access. So if either key or smart is stolen, the security mechanism becomes ineffective. The Embedded just-drive concept has two main objectives. One is to provide sure destination and comfortable feel to the user whenever he gets into the car to make a drive.

This methodology allows one to check his/her vehicle status, by reading different vehicle parameters (Engine oil level, Tire Pressure, door control, Hazard indication etc.,) using his Smart mobile with Bluetooth Connectivity / Zig bee. The second objective is to provide antitheft control by disabling an automobile and its key auto systems through automation and remote when it is stolen.

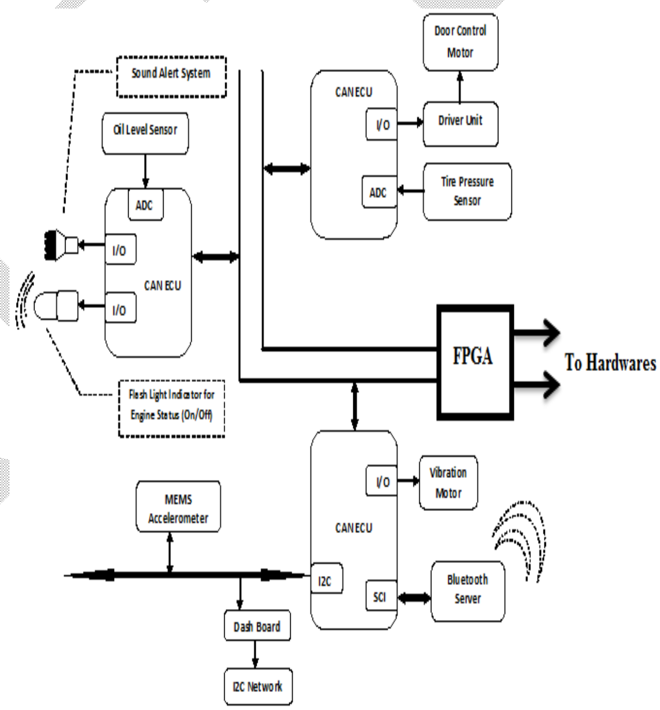

Fig 1: Various embedded computing and sensors employed in an automotive platform

Mobile based Bluetooth Parameter monitoring can be done staying outside the car. In this proposing methodology, the automotive has a Bluetooth server interfaced with the car. All the sensors, such as, engine oil level, antitheft system using MEMS Accelerometer sensor, Vibration Motor, horn, Flash Light and door Control unit are networked to communicate with ECU (Electronic Control Unit) using Control area Network (CAN). With the help of Bluetooth communication, the automotive data's are monitored by smart android phones.

Corresponding Author: Ms. M.Shalini Pushpa, GKM College of Engineering and Technology, Chennai, Tamilnadu , India.

ISSN 2348 – 9928
IJAICT Volume -1, Issue-3, July 2014 Doi:01.0401/ijaict.2014.01.12 Published Online 05 (05) 2014

2.1 Overview of Can Bus Attributes

As more and more electrical equipment's are application in an automotive, automotive electrical system has formed a complex large system which is concentrated control in the cab. The electrical equipment's are from engine control to the transmission system control, from the driving, braking, steering control to the safety assurance and instrument alarm system, what is more, and all the effort to make comfort from power management. Moreover, with the development of IT recently, the emergence of new electronic communication products, i.e. 3G, has put forward higher requirements in the car cabling interaction and information sharing.

It is analyzed from the wiring perspective; most of the traditional electrical system uses a single point to point communication, which is lack of contact with each other, so that the wiring system will inevitably lead to large. According to statistics, cable lengths are up to 2000 meters and 1500 electrical nodes in the Luxury cars when traditional wiring was used. What's more, the figure was about growing 1time per decade, thus the conflicts exacerbated between the thick wiring harness and the limited available space of a car. Hence in terms of the efficiency or the costs of materials, the traditional wiring was not suitable for the car development. In order to meet the real-time requirements of each subsystem, it is necessary to implement sharing of public data, engine speed, wheel speed, and throttle pedal position etc. in the car.

CAN bus is designed to meet these requirements. CAN is a serial communication protocol. It has a communication rate of 5Kbps/10Km and 1Mbps/40m. The maximum numbers of CAN nodes can be up to 110. It has several transmission media such as twisted pair and coaxial cable. CAN can receive data via point to point, multipoint, and global broadcast sending.

CAN bus uses differential voltage as a digital signal. There are two differential voltage states. When there is 2V pressure between two lines, it is called the dominant state. However, when the bus line voltage is equal, it is called the recessive state. Obviously, there is as long as a node on the bus that sends dominant signal level, it will keep dominant. If it is being recessive, all nodes send recessive signal level. CAN protocol do not require 0 or 1 representatives dominant? But in the actual application, 0 generally represents the dominant position, 1 represents recessive. CAN have automatic disconnection of nodes, which are found faulty. Each node will have its own crystal clock and hence there is no common clock needed. Also, theoretically there is no limitation in the number of CAN nodes – which adds an advantage.

2.2 System Implementation

There is growing consumer demand for wireless communication technologies in transport applications from point- to-point to multiplexed communications. Advances in portable devices (mobile phone, personal digital assistant and GSM devices) may exploit the possibility of interconnection using in- vehicle communications. Also advances in wireless sensor networking techniques which offer tiny, low power and MEMS (Micro Electro Mechanical Systems) integrated devices for sensing and networking, will exploit the possibility of in-vehicle communications.

This proposing system consists of three CAN nodes. Each CAN node resembles a CAN ECU (Electronic Control Unit). CAN ECU consists of a microcontroller, CAN controller, CAN transceiver. The sensors for sensing Tire pressure, Oil level, MEMS accelerometer motors for door control and engine(vibration), Flash light indicator for engine status and sound alert system for hazard indication are connected to the CAN nodes as shown in the above figure. All the three CAN nodes are connected using bus topology. Bluetooth server is connected to the SCI (Serial Communication Interface) which is nothing but UART. So this node acts as the server/master node. And the other two nodes acts as slave nodes.

Car and smart phone are interfaced with authenticated pairing with Bluetooth communication. When a command is given via mobile, Bluetooth server in the car receives it. Command is shared by all the 3 CAN nodes, since all the nodes are connected through bus topology. Each node performs its actions accordingly. Oil level sensor senses the engine oil level, Pressure sensor senses Tire pressure, Door control unit causes the door to Open/Close. On the receipt of a command, each node will automatically perform its job of sensing and controlling. Finally all the sensed data will reach the master node through the bus. This information will be displayed on the car dash-board and all it will be sent back to the user's mobile via Bluetooth connectivity. Using this information, the user can take the necessary controlling measures. If all the actions are verified to be correct, the user can post a command to ON the engine. As per the user's command, the engine will start. If any abnormal conditions occur, the MEMS accelerometer will go above a certain threshold value. Automatically, this will be indicated by a buzzing sound.

2.3 *Bluetooth Technology*

Bluetooth is a high-speed, low-power microwave wireless link technology, for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building Personal Area Network. Unlike infra-red, Bluetooth does not require line-of-sight positioning of connected units. It is a wireless alternative to RS232 data cables. It can connect several devices, overcoming problems of synchronization. The technology uses modifications of existing wireless LAN techniques but is most notable for its small size and low cost.

An interesting aspect of the technology is the instant formation of networks once the Bluetooth devices come in range to each other. A Piconet is a collection of devices connected via Bluetooth technology has an ad hoc fashion.

A Piconet can be a simple connection between two devices or more than two devices. Multiple independent and non-synchronized Piconets can form a Scatternet. Any of the devices in a Piconet can also be a member of another by means of time suitably sharing the time.

Several Piconets can be established and linked together in adhoc, where each Piconet is identified by a different frequency hopping sequence. All users participating on the same Piconet are synchronized to this hopping sequence. If a device is connected to more than one Piconet it communicates in each Piconet using a different hopping sequence. A Piconet starts with two connected devices, such as a portable PC and cellular phone, and may grow to eight connected devices. All Bluetooth devices are peer units and have identical implementations. However, when establishing a Piconet, one unit will act as a master and the other(s) as slave(s) for the duration of the Piconet connection.

In a Piconet there is a master unit whose clock and hopping sequence are used to synchronize all other devices in the Piconet. All the other devices in a Piconet that are not the master are slave units. A 3-bit MAC address is used to distinguish between units participating in the Piconet. Devices synchronized to a Piconet can enter power-saving modes called sniff and hold mode, in which device activity is lowered. Also there can be parked units which are synchronized but do not have a MAC addresses. Also, these parked units have an 8 bit address; therefore there can be a maximum number of 256 parked devices in the Piconet.

III. MEMS ACCELEROMETER

Modern accelerometers are often small micro electro-mechanical systems (MEMS), and are indeed the simplest MEMS devices possible, consisting of little more than a cantilever beam with a proof mass (also known as seismic mass). Mechanically the accelerometer behaves as a mass- damper-spring system; the damping results from the residual gas sealed in the device. As long as the Q-factor is not too low, damping does not result in a lower sensitivity.

Under the influence of gravity or acceleration the proof mass deflects from its neutral position. This deflection is measured in an analog or digital manner. Most commonly the capacitance between a set of fixed beams and a set of beams attached to the proof mass is measured. This method is simple and reliable; it also does not require additional process steps making it inexpensive.

Integrating piezoresistors in the springs to detect spring deformation, and thus deflection, is a good alternative, although a few more process is needed. For very high sensitivities quantum tunneling is also used; this requires specific fabrication steps making it more expensive. Optical measurement has been demonstrated on laboratory scale.

The LIS302DL is an ultra-compact low-power three axes linear accelerometer. It includes a sensing element and an IC interface able to provide the measured acceleration to the external world through I2C/SPI serial interface.

Fig 2 : MEMS Accelerometer (Pin Connection)

The sensing element, capable of detecting the acceleration, is manufactured using a dedicated process developed by ST to produce inertial sensors and actuators in silicon. The IC interface is manufactured using a CMOS process that allows to design a dedicated circuit which is trimmed to better match the sensing element characteristics. The LIS302DL has dynamically user selectable full scales of ±2g/±8g and it is capable of measuring accelerations with an output data rate of 100Hz or 400Hz.

3.1 Pressure Sensors

In automotive industry, pressure sensors form an integral part of the engine and its safety. In the engine, these sensors monitor the oil and coolant pressure and regulate the power that the engine should deliver to achieve suitable speeds whenever accelerator is pressed or the brakes are applied to the car. For the purpose of safety, pressure sensors constitute an important part of anti-lock braking system (ABS). This system adapts to the road terrain and makes sure that in case of braking at high speeds, the tires don't lock and the vehicle doesn't skid. Pressure sensors in the ABS detail the processor with the conditions of the road as well as the speed with which the vehicle is moving. Along with this, it all ensures the safety of the passengers whenever high amount of pressure is experienced by the vehicle.

The MP3V5050 sensor integrates on- chip, bipolar op-amp circuitry and thin film resistor networks to provide a high output signal and temperature compensation. The small form factor and high reliability of on-chip integration make the Free scale Semiconductor, Inc. Pressure Sensor a logical and economical choice for the system designer. The MP3V5050 series piezoresistive transducer is a state-of-the-art monolithic silicon pressure sensor designed for a wide range of applications, but particularly those employing a microcontroller with A/D inputs. This patented, single element transducer combines advanced micromachining techniques, thin-film metallization, and bipolar processing to provide an accurate, high level analog output signal that is proportional to the applied pressure.

3.2 Motor Drivers

Motor driver IC allows DC motor to drive on either direction. This 16-pin IC can control a set of 2 DC motors simultaneously in any direction. It is also called as Dual H-Bridge Motor Driver IC, with its working based on H-Bridge. H-Bridge circuit allows voltage to flow in either direction; hence H-Bridge IC is ideal for driving a DC Motor successfully. 1 L293D IC has 2 H-Bridge circuits (capable of rotating 2 DC motors independently).

L293D IC has 2 Enable pins – pin1 and pin 9. To drive the motor, EA pins should be high. To drive the motor with left H- bridge, enable pin 1 should be high. To drive the motor with left H- Bridge, enable pin 1 should be high. If either pin1 or pin 9 goes low, the motor in the corresponding section will suspend working hence its acts like a switch.

There are 4 input pins. Pins 2, 7 on the left side and pins 15, 10 on the right side. Left input pins will regulate the rotation of motor connected across left side and right input for motor on the right hand side. Motors rotate on the basis of the inputs provided across the input pins (LOGIC 0 or LOGIC 1).

IV. CONCLUSION

The CAN bus technology is used for the optimization of the automobile and the whole performance vehicle monitoring and control. This paper has presented the on-going research being undertaken to investigate the suitability of using Bluetooth technology for real-time monitoring and data acquisition in auto motives. Cars with fixed features designed long before their delivery to consumers are an anachronism. The car of the future will be different. The work presented here demonstrates the initial phase of such an embedded car that will be visible in near future. Customized vehicles will not only provide a more interesting drive but also a safer one, and will become a major time-saver. The main idea behind this project is to engineer all embedded related technology to make a drive a smart just-drive.

References

[1] Aoyama .M (2012), ‘‘Computing for the Next Generation Automobile,’’ Computer, pp. 32-37.

[2] Guizzo.E (2011), ‘‘How Google’s Self-Driving Car Works,’’ IEEE Spectrum Automation blog.

[3] Kocher .P (2004), ‘‘Security as a New Dimension in Embedded System Design,’’ Proc. 41st Ann. Design Automation Conf. (DAC 04), ACM.

[4] Liu, Z. (2005),” A New Embedded Car Theft System,” In Proc. of the Second Int’l Conf. on Embedded Software and Systems (ICESS ’05).

[5] Nusser .R and Pelz .R (2000),” Bluetooth-based wireless connectivity in an automotive environment,” Vehicular Technology Conference.

[6] Papadimitratos .P, Buttyan .L, Holczer .T, Schoch .E, Ma.Z, Kargl .F, Kung .A, and Hubaux .J.P (2008),”Secure Vehicular Communication Systems Design and Architecture,” IEEE Communcations Magazine.

[7] Velupillai .S and Guvenc .L (2007),” Tire pressure monitoring,” IEEE Control Systems Magazine.