Autorama, Connecting Your Car to the Internet of Tomorrow

Nicholas Sargologos, Senior Marketing Manager, Digital Networking – Freescale Semiconductor

Overview

Automotive OEMs need a secure, managed process to deliver software updates to the cars they build, without requiring owners to bring them into a dealership. In the event of an accident, emergency response agencies could be automatically notified of the incident, where it occurred and who was in the car. And what about those annoying
parking lot dings that no one ever knows how they happened? What if a car could automatically detect the event when it happens, record it and not only alert the owner, but also provide video capture of the incident? All of these capabilities and more are coming soon, supported by the newest generation of automotive gateways that designed to connect your car to the Internet of Tomorrow.

This article will focus on how the evolving Internet of Tomorrow (IoT) is changing the way your car will operate, behave, and will soon get you from here to there more safely and efficiently.

Before we dive into what a mobile IoT Gateway is and what new capabilities it will enable, we should first look at what makes up the IoT.

Essentially, the IoT is really about machine to entity with the objective of supporting two primary aspects:

- Remote Monitoring, Management and Control (RMMC) of the millions of interconnected devices
- Big Analytics, or data mining, to support “push” services and other uses

Some examples related to automotive applications are:

- **Machine to Machine:**
  - Automatic diagnostics for cars: automatic information collection from your car’s engine management system and sending real-time alerts to drivers or service centers

- **Machine to Infrastructure:**
  - Automatic bridge monitoring: sensing and monitoring the structural integrity of a bridge in case of flooding
Machine to Human:
- Automatic detection of a driver's and passenger's vitals information (alertness, reaction times, etc.)

Machine to Nature/Environment:
- Early detection of severe weather or earthquakes: distributed sensors to detect early tremors in specific places or rapid atmospheric changes that accompany tornados

How are these various IoT sensors and the information they provide organized and connected so that the information they provide can be accessed, organized and intelligently managed? Figure 1 illustrates the layers and key attributes from the IoT edge into the data center:

What is an automotive IoT gateway?
An automotive IoT gateway will allow the bridging of onboard systems that control and monitor the car's engine, drivetrain, steering and braking systems together with the navigation, entertainment, safety and vision systems, and enable secure, two-way, communications and data transfers between cloud based services and the automobiles systems and passengers.
What will driving a car be like in the not too distant future? Many of the capabilities being enabled in modern automobiles are extensions of the technologies that have become common in homes and businesses.

For example:

- Broadband access to the internet
- Surveillance systems that can record events in and around the premises and alert monitoring services
- Environmental control
- Automated downloads and software updates for connected electronic devices

In most homes today, it's a manual process to turn on and off certain lights, set temperature zones and turn on and off a washing machine. As IoT capabilities deploy throughout the home, doors, windows, electrical outlets, appliances and
many other types of standalone equipment will become “smart” with a unique internet ID. Such smart devices can then be connected via wired or wireless communication, allowing a user to monitor his or her house remotely, change settings on a refrigerator or washing machine and control household tasks through a laptop, mobile phone, or from an automobile. In fact, there are some services offered today by security or Internet service providers that already do this, but on a much smaller scale and with fewer capabilities than we’ll see in the Internet of Tomorrow.

Let’s begin with how an IoT Gateway coupled with an intelligent infrastructure will make everyday driving safer by borrowing a chapter from the aviation industry, which pioneered a system to prevent aircraft collisions called traffic collision avoidance system (TCAS). In that system, when two airplanes were approaching each other on a collision path, the ‘machines’ in the two airplanes would take over. The system first would send an audible warning to the pilots about the danger ahead, while at the same time communicating between the two planes and deciding how each plane should move to avoid a collision. The assumption was that if the two pilots were warned and were in control to make quick decisions, they could both decide to make turns that would still cause a crash. To prevent this, the TCAS machines in each aircraft took control under these conditions, and steered their respective aircraft in a coordinated manner that pre-empted the possibility for the aircraft to collide.

"...smart devices can then be connected via wired or wireless communication, allowing a user to monitor his or her house remotely, change settings on a refrigerator or washing machine and control household tasks through a laptop, mobile phone, or from an automobile."

Today most new cars offer driver assistance systems that can alert drivers to impending danger. Higher end vehicles are now offering automatic systems that will essentially “take over” in the manner of the TCAS system used in aviation,
but are limited to stopping a vehicle that is approaching an obstacle unsafely. In the future, as automotive IoT gateways evolve in performance and the necessary highway infrastructure systems are deployed, the ability for a vehicle to automatically steer itself safely will open the door to fully autonomous, context-aware decision optimized driving systems.

Here is an example of a context-aware automation and decision optimization in an IoT gateway enabled car: using its active safety radar system (sensing node) in conjunction with image processing cameras (sensing nodes), the car communicates with an embedded processor (embedded processing node) in the center stack of the car to make an appropriate decision regarding danger ahead. Or, the vehicle could leverage its built-in GPS and wide-area-network (WAN) wireless communication capability (connectivity node) to pass along information to a central processing server on the network (in the cloud). The network could then make the car aware of the information it had just received from the sensors of an unstable bridge (sensing node) on the road ahead indicating that due to a flood from heavy rain, the bridge was losing its structural integrity. And, with this information, guide the car to a different route to avoid danger.

For automotive manufacturers, the process of delivering firmware updates to the microcontrollers that monitor and manage nearly all of the electronically controlled systems in an automobile is highly dependent on voluntary action by the car owner. Many times, needed updates are delayed or never completed due to a failure or unwillingness of the car owner to take the car in to the dealership for the necessary work. In some cases, the lack of such updates can lead to dangerous situations when they involve drivetrain or braking system problems. With the secure communication capabilities enabled by an on-board IoT gateway, automotive OEMs will be able to unobtrusively download software updates to a
vehicle without the need for owners to bring the vehicle in to the dealership. In addition, just as is common today in the aviation industry, cloud-based systems will be able to monitor and analyze vehicle systems in real-time, and notify owners of impending failures or preventive maintenance that may be needed. Together, these capabilities will improve safety and help reduce the overall cost of ownership and accident liability supported by insurance carriers.

‘One-in-five cars will be self-aware and capable of sharing information on mechanical health and surroundings’

On the subject of insurance liability, another capability of automotive IoT gateways is the skill to link on-board synthetic vision systems to accelerometers embedded in the cars bodywork, as well as data recording and playback systems in the IoT gateway. With these capabilities, if a parked car is struck, a device-driven event triggers a series of events to happen. Accelerometers detect the impact to the vehicle and send a wake-up signal to the microprocessor in the IoT gateway, which immediately activates the synthetic vision system of the car and begins recording the video streams to the onboard recording system. Simultaneously, the IoT gateway can be programmed to send a notification to the vehicle owner’s phone, to alert them of the event, and even stream the video recording over the cellular network to the owner’s smartphone. Additionally, the vehicle’s IoT gateway can notify a monitoring service as well as the insurance carrier.
Market sizing forecasts for connected cars show that by 2018:

- One-in-five cars will be self-aware and capable of sharing information on mechanical health and surroundings
- The number of cars connected to the Internet will increase 6X to more than 150 million by 2020
- Outside the vehicle, this will demand increased cellular bandwidth to support vehicle to vehicle (V2V) and vehicle to infrastructure (V2I)
- Advances will connect the car for both comfort and safety, providing options for both Automated and fully Autonomous driving

The figure below shows what the connectivity will look like for a car enabled with an IoT gateway.

To support the processing demands, as well as multiple levels of wired and wireless connectivity across 4G, Wi-Fi, Bluetooth, CAN and increasingly Ethernet-based sub-nets that will exist in automobiles, vehicles will require a purpose designed communications microprocessor, capable of supporting industrial temperatures as well as secure, trusted data transfers between cloud based RMM applications and the vehicle.
Freescale Semiconductor and its value line of QorIQ Communications processors like the LS1021A have the features needed to support these demanding requirements, including security firewall protecting access to the sensitive processing and memory areas of the microprocessor from intrusion or hacking attempts.

In the end, secure, two-way data transfers between cloud-based services, automotive systems and passengers need to be supported by specific communications processors. These processors need to offer several connectivity features such as 4G, Wi-Fi, Bluetooth, CAN and Ethernet, and provide security through features like secure boot, trust architecture and Firewall protection from intrusion or hacking attempts. For more information about Freescale solutions visit [www.em.avnet.com/Freescale-QorIQ-Layerscape-Architecture](http://www.em.avnet.com/Freescale-QorIQ-Layerscape-Architecture) or [www.freescale.com/LS1021A](http://www.freescale.com/LS1021A).

**NICHOLAS SAROLOGOS**

Nicholas Sargologos is Senior Marketing Manager, Digital Networking at Freescale. He has managed product development programs targeted at the IoT, Smart Grid and Industrial Automation markets, and has published several papers and industry articles on communications, industrial automation and security. Prior to joining Freescale, Mr. Sargologos established a track record of success developing award winning products for several high tech companies, including IBM, Motorola, Applied Micro and Dell. He received his Bachelors of Science degree from the University of Texas at Austin in 1982. Following his graduation, he earned a commission in the US Navy, where he served as a Naval Aviator from 1983 – 1989.