Atmel®

Automotive Compilation

Volume 11, August 2015

Table of Contents

Atmel®

Immobilizer-Protocol Selection Considerations and Guidelines

Toby Prescott

Introduction

Immobilizers prevent an automobile´s engine from running unless the correct key or another token is present. The modern immobilizer system has had to evolve as the technologies and tools available to criminals have become more complex.

Immobilizer technology once involved the use of a unique, but unprotected, electronic number. The security of the system rested in the considerable technical challenge of reading this unique number and then replaying it as a clone of the valid key. With advancements in available technology, would-be thieves can now easily accomplish this goal in just a few minutes with readily available hardware. Over time, vehicle-security designers have added security measures, primarily through the use of cryptographic algorithms.

Selecting an immobilizer system presents a range of options for designers´ consideration. This article discusses the pros and cons of these options to help designers make these decisions after they have a solid understanding of how these choices will affect each piece of the immobilizer system.

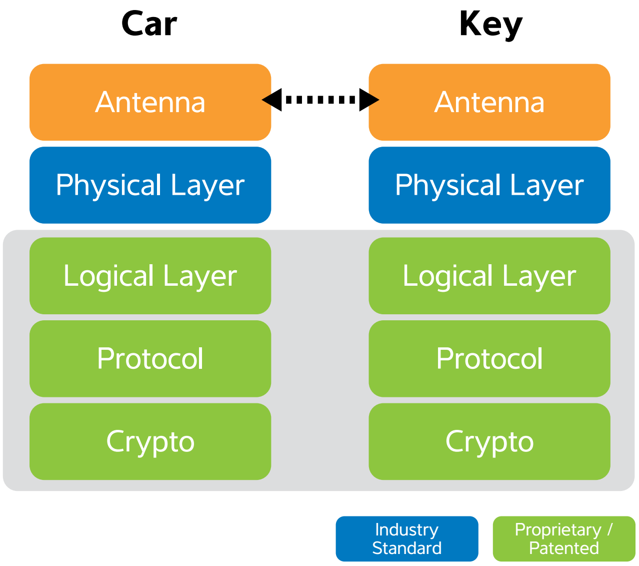


Figure 1. Layers Within An Immobilizer System

Mechanical and Physical Layers

The mechanical layer of immobilizers involves the antennas. Most modern immobilizers use the inductive-coupling principle to transfer energy to the transponder, allowing passive—that is, batteryless—operation. The vehicle creates a magnetic field to induce a corresponding current and voltage in the transponder antenna. Most of the antennas comprise a series of copper-wire windings on a ferrite core. The coil is predominantly inductive, and designers must match it to the desired resonant frequency through a specific capacitance. The electrical parameters of this tuned antenna can vary greatly, but the main considerations should be the dimensions and sensitivity of the antenna. The area enclosed by the antenna coil should be as large as possible but within the mechanical constraints of the final devices. Sensitivity varies as a function of the inductance, core material, Q factor and geometry of the antenna.

The physical layer is similar to the mechanical layer in that it must allow the transfer of both power and data between the vehicle and the transponder. To achieve this transfer, designers have various options, all involving how the physical layer controls the antennas in the immobilizer field. The two most prevalent options are FDX (full-duplex) and HDX (half-duplex) systems. This choice plays a fundamental role in the overall design of the architecture. Devices that use FDX cannot function on systems using the HDX option, and those that use HDX cannot function on systems that use FDX. This constraint may limit designers' choice of suppliers and can dictate some other choices in the design of immobilizers.

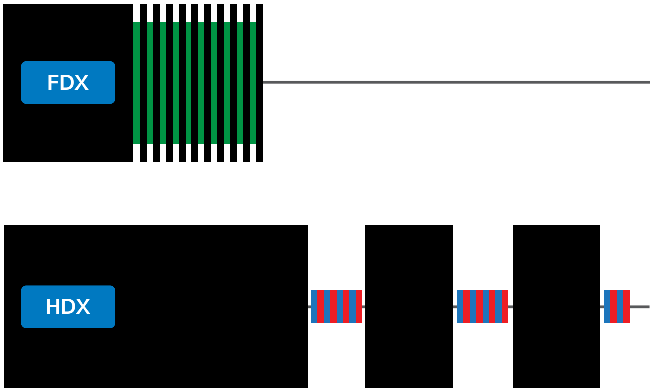


Figure 2. Physical Layer - FDX vs HDX

FDX can simultaneously transfer both power and data. The vehicle-to-transponder downlink typically uses the all-OOK (on-off-keying) modulation of the carrier. The transponder-to-vehicle uplink normally uses AM (amplitude modulation) during constant carrier activity. Loading, or increasing the current consumption, of the transponder antenna creates this constant activity. This load couples back to the vehicle's side coil, and a sensitive receiver can detect it. The downlink is similar on an HDX system. The carrier is initially on to provide power by creating a constant carrier. Once a buffer capacitor on the transponder side fully charges, the vehicle sends data using all-OOK modulation and then shuts off the carrier. The transponder replies on the uplink by internally generating an FSK (frequency-shift-keying)-modulated signal, which then transmits to the vehicle side.

Logical Layer

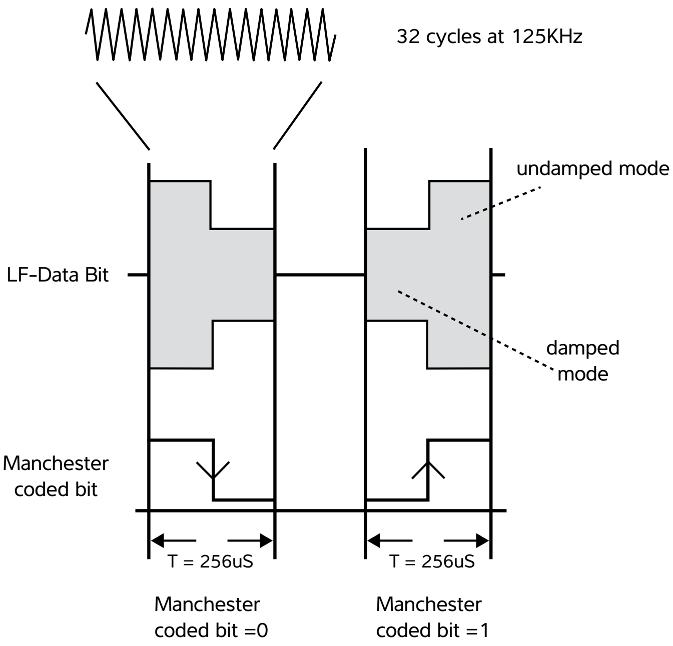


Figure 3. Manchester Data Bit Encoding

The logical layer describes the creation of individual bits; the uplink's and downlink's methods of forming logic ones and logic zeros may differ. The uplink may typically use Manchester coding, and the downlink path may use binary-pulse-length modulation. The logical layer also defines the

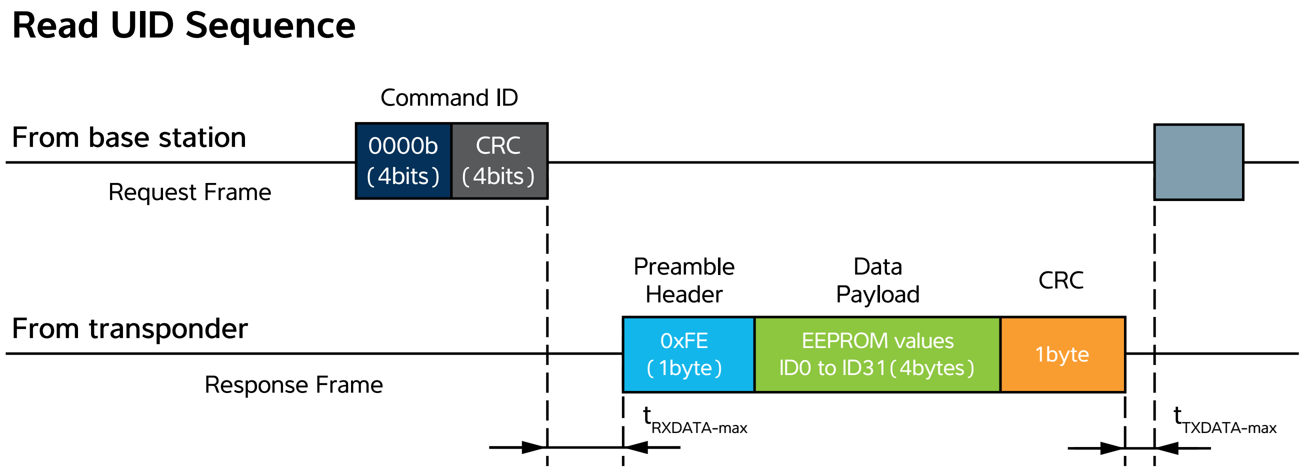


Figure 4. Typical Protocol Layer

baud rate—typically around 3.906kbaud for immobilizer systems—on both paths. The baud rate plays a crucial role because the need for higher security typically involves the transmission of more data bits. However, higher baud rates may lower overall system performance because higher rates require a lower Q factor on the antennas to achieve the data rate. Other options for higher baud rates involve compressing multiple bits into symbols. Once the system has established the logical layer, it can send and receive groups of logical bits to convey information.

Protocol Layer

To create usable functions in a system, the protocol layer must provide the transferred bits with a meaning. The protocol layer also details the sequence of operations that must occur to perform a function. This sequence usually involves a list of commands and responses between the vehicle and the transponder. The system may lock some of these commands from use until other commands complete execution. These commands can prevent memory access, for example, until after a successful authentication has occurred.

In most current systems, the protocol is proprietary, meaning that manufacturers do not share with the industry the details of how these systems work. In many cases, patents prevent implementation by anyone except a system's owner. Many manufacturers claim the availability of an "open immobilizer," but these claims can be misleading. A system may use encryption that is open to the public, but the protocol the system uses may not be open to the public. The protocol layer can create a lock-in situation to one supplier, thereby removing competition and limiting options.

When evaluating the security of an immobilizer system, designers must also evaluate the protocol layer. The encryption may be secure and may have undergone thorough expert review in the public domain, but these steps do not ensure the security of the system. Rather than decoding the encryption itself, many attacks focus solely on weaknesses in the transfer of the information. For example, a dictionary attack does not lead to knowledge of any secret-key information but instead focuses on weak protocols using low-possibility message combinations.

To ensure a secure immobilizer system with a secure and stable supply base, the protocol layer must possess complete and open access by the security community for review and analysis and must enable and allow interoperability among suppliers of the system components. The use of a proprietary closed protocol can compromise both of these points.

Encryption Algorithm

Designers can use encryption to secure communication and to prevent would-be criminals from accessing and understanding sensitive information. This feature could be important for memory contents that require protection of the data values, for example. An immobilizer system uses encryption only to prove valid identity. Without knowledge of the secret key the system uses, a would-be thief cannot possibly create a clone of a valid transponder. The encryption algorithm simply takes some input and creates an output that is unpredictable unless the user has this key. With encryption, only those users with the secret key can recover the correct information. The overall system security meets the level of encryption security only if no other weak points in the system exist.

In most cases, the immobilizer system truncates the length of the output to satisfy other system requirements, such as system-response time. This truncation weakens the security of the overall system, and such a scenario further demonstrates that designers must review the protocol layer with the same intensity as they scrutinize the encryption algorithm itself to ensure that the protocol does not become the weak link.

The security community widely agrees that peer review is the best method of ensuring a robust and secure algorithm and protocol. The community thus cautions designers against the selection of a proprietary encryption solution, about which the designers may know few details. These encryptions almost always fail over time, especially if would-be criminals perceive a significant incentive or reward for breaking them. Once a hacker breaks these encryptions, it is almost impossible to repair the vulnerability to systems in the field.

A proprietary protocol prevents other parties from introducing their own solutions and further complicates this issue. For this reason, many new systems are moving to open-source encryption, such as the AES (Advanced Encryption Standard). The public knows all the details of AES except for the secret keys the system uses. This feature allows thorough scrutiny; as a result, no one has successfully attacked AES in more than a decade.

System Performance

The performance of a vehicle's immobilizer system generates much discussion in the automotive industry. Although antenna geometries, drive currents and sensitivity greatly influence the performance of the security system's hardware, the immobilizer protocol can also play a role. The selected protocol can imply several trade-offs in performance parameters.

Range

When checking system performance, designers' first question is often about the operational distance between the vehicle and the transponder. Styling concerns often drive the physical-hardware design, and these concerns often give rise to small key-fob geometries. Despite these concerns, however, designers must focus on better system performance so that the operational range remains as large as possible. Improvements in system performance may also allow the use of lower-tolerance components, providing a cost benefit and still maintaining an acceptable operating range.

The protocol can influence range in several ways. First, designers should carefully consider the selection of the encryption algorithm to analyze its effect on the transponder's current consumption. Implementing the encryption in hardware blocks can provide an advantage, but more complex algorithms require higher processing loads, which, in turn, require more power and result in lower range.

Designers should also consider the message-packet structure and baud rate. The combination of lower baud rates and shorter messages can cause the transponder to take longer to harvest the necessary power to provide longer range. Lower baud rates also allow the use of higher-Q-factor antennas. Error-detection and retry strategies can also provide an efficient means of detecting and recovering from transmission errors at the fringe of the operational range.

Because hardware is the predominant driver of range, these measures do not provide dramatic improvements in range but can combine to provide the small amount a given system requires.

Response Time

The automotive market strongly focuses on how long the immobilizer system takes to authenticate the transponder. However, the latest passive-start vehicles have largely eliminated this problem because they use the immobilizer only as backup method for starting the vehicle if the key-fob battery is depleted. With these vehicles, the driver must place the key fob in a special location and then press the start button. This sequence takes considerably longer than turning the key in a traditional ignition cylinder.

Response time depends almost entirely on the protocol. The baud rate dictates how many bits of a message a system can send during a specified interval. To optimize response time, the command set should provide an efficient message length. The system transmits the largest number of bits in an immobilizer sequence during the security-authentication transaction.

Wireless systems are prone to transmission errors, so designers should evaluate response time by including a number of expected retries. A protocol with features that allow fast, easy retries can provide better overall system performance. The use of a simple CRC (cyclic redundancy check) may prove valuable, even if it adds a small amount of additional overhead time during a normal sequence.

Security Strength

A primary concern in security strength is the length of the secret key, and, although this concern is important, it deals only with the difficulty of attacking the encryption algorithm itself. The secret key's bit length alone provides inadequate protection for the system. The protocol can introduce elements causing it to be the limiting security factor. The most common such element is truncation. The number of bits necessary for authentication are the main drivers of response time. To improve this parameter, the protocol truncates inputs and outputs to the security algorithm.

To use AES-128, for example, a typical AES sequence would require 128 bits of input and 128 bits of secret key to provide a 128-bit output. At a standard 3.906kBps, this action would take more than 65msec to transmit the input and output bits in the system, excluding any overhead commands or processing. To clearly show how the protocol can drive the limiting security strength, consider taking the truncation to an extreme. Reducing the input to 64 bits would shorten the time by 16msec. If the output is now truncated to 4 bits, system-response time would be slightly little longer than 18msec—a lot faster than the 65msec in the other scenario. Reducing the number of bits allows some attacks to have a better probability of success. In this case, the system could simply ignore the message from the vehicle and reply with all 16 possible combinations. The secret key need not be broken for the system to become compromised. This situation illustrates the importance of an open and transparent protocol, which designers can thoroughly review to ensure that no weaknesses can compromise the system.

A flexible protocol allows designers to configure the amount of truncation of the input and output bit lengths and to optimize for individual use cases.

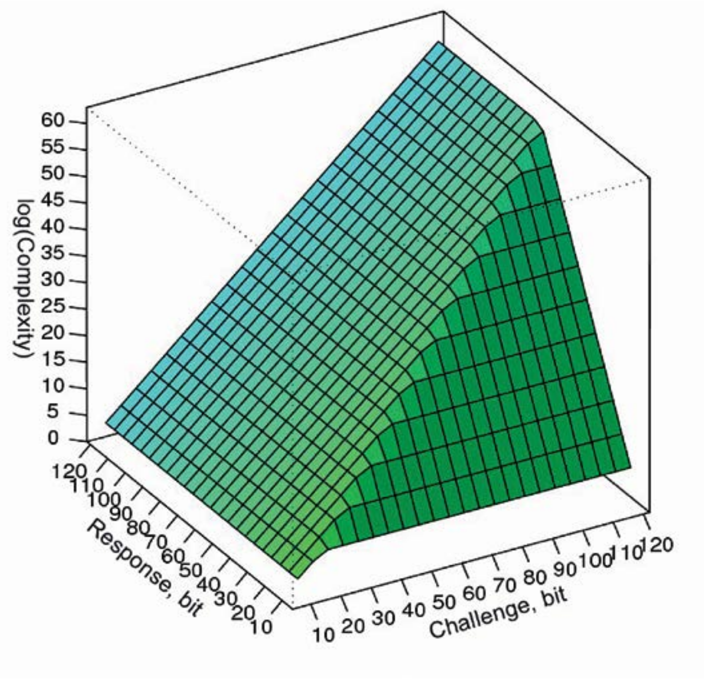


Figure 5. Challenge & Response Bit Length Effects on Security Strength (AES-128)

Conclusion

Since the introduction of the immobilizer, the number of stolen vehicles has significantly decreased. Although the protocol layers are complex, designers need not hide them from general knowledge to preserve system security. Although some system providers want to retain proprietary protocols, doing so provides no benefit to the overall market. On the contrary, keeping protocols proprietary can often reduce security to an unacceptable level. The supplier is the only beneficiary of this practice because, once the industry adopts a proprietary protocol, the supplier becomes the sole source of system components, eliminating the effect of market forces that could otherwise drive lower costs. Weakness in proprietary solutions becomes evident only after the system has been in production for a significant amount of time. At that point, containment and permanent corrective action would affect such a large population that it would become cost-prohibitive for suppliers to implement a fix. The best approach for ensuring a robust and secure system is to allow the security community to thoroughly review the entire protocol and encryption algorithm before the manufacturer deploys it in the vehicle.

Designing an immobilizer system requires many trade-off decisions to optimize various performance factors. A protocol that allows easy configuration options will provide a foundation on which to build platform architecture. High-security systems can use the same underlying protocol and can achieve fast system response. These benefits provide commonality among various applications and meet current automotive requirements.

Practical Ways to Increase Robustness and Extend Range of Automotive RF-Control Systems

Jim Goings

Introduction

Today's highly integrated and advanced radio designs, such as the ATA5831/2/3 transceivers and ATA5781/2/3 receivers, enable engineers to build robust RF systems with better performance than ever before. To build an RF system with increased robustness and extended range, it is important to understand the advanced capabilities of these radios. This document explores RF-system attributes, such as frequency, data rate, bandwidth, multichannel abilities, sensitivity and blocking, and consider their effects on system performance.

Robustness of the RF Link

Unwanted RF signals at or near the system's operating frequency can compromise the receiver's ability to accurately demodulate the desired RF data packet. Disturbers that occur near the desired operating frequency are near-band, and those that occur at the desired operating frequency are in-band. Wideband RF interference appears at a significant distance from the desired signal, such as three to five times the radio's local-oscillator frequency, and can also block proper demodulation. Methods are available to mitigate each of these interfering signals.

Near-Band and Wideband Interference

Near-band- and wideband-interference suppression focuses on improving the radio's selectivity and blocking characteristics. "Selectivity" describes the radio's ability to select the desired signal from other RF spectra. "Blocking" describes the IC's ability to receive the wanted RF signal in the presence of a jamming interference signal.

One common approach to suppressing this type of noise is to add a surface-acoustic-wave (SAW) filter between the receiver's antenna and the RF front end. This component acts as a bandpass filter, which enables the desired signal to enter the radio with little attenuation and subjects both near-band and wideband interference to increased attenuation. Figure 1 shows the typical bandpass characteristics of a SAW filter. In some cases, a SAW filter provides additional suppression that is insufficient to fully block the interference. This approach also incurs the cost of adding the SAW filter.

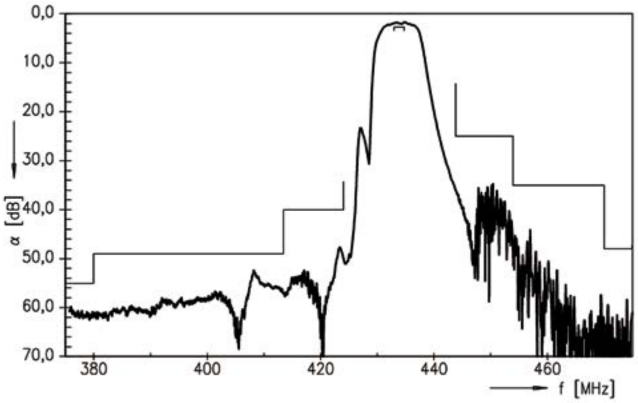


Figure 1. Typical Frequency Response of a 433.92MHz SAW Filter

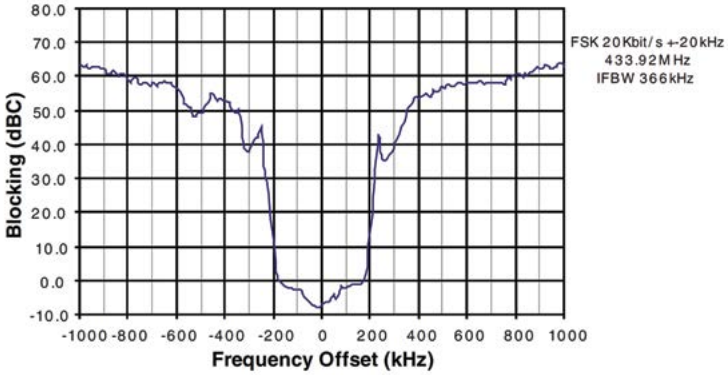


Figure 2. Blocking Characteristics of ATA58xx / ATA57xx (433.92MHz, IFBW=366KHz, FSK, DR=20kbps, f_{DEV}=±20kHz)

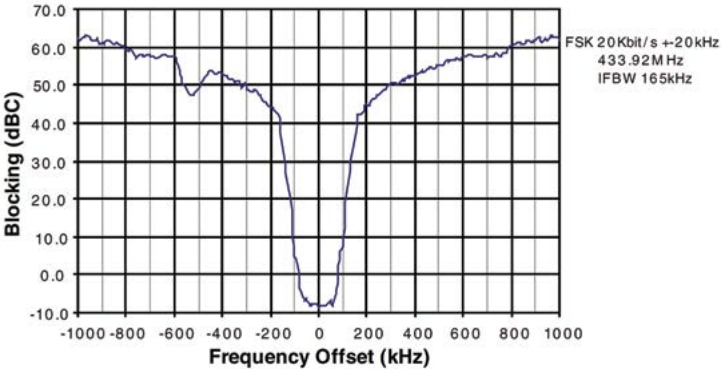


Figure 3. Blocking Characteristics of ATA583x/ATA578x (433.92MHz, IFBW=165kHz, FSK, DR=20kbps, f_{DEV}=±20kHz)

Another approach to addressing this type of noise would be to reduce the receiver's intermediate- frequency bandwidth (IFBW), or channel filter. Refer to Figure 2 and consider interference appearing 200kHz below the desired operating frequency. In this case, an IFBW of 366kHz for which the corner frequency is 183kHz would attenuate the disturber by only 10dB. In contrast, refer to Figure 3 and note that using a 25kHz IFBW would increase the attenuation of the disturber to 43dB.

In the past, the IC design fixed the IFBW. However, high performance Atmel® devices, such as the ATA583x and ATA578x, enable selection and adjustment of the IFBW through the use of a configuration table. The user-configurable IFBW range spans 25 to 366 kHz and offers 26 IFBW settings. When optimizing the design, engineers must exercise caution to ensure that the selected IFBW remains wide enough to account for variations in the RF frequency of both the receiver and the transmitter; these variations can result from modulation and tolerance of the internal-frequency references. RF signals from the intentional radiator—the transmitter, for example—have carrier-frequency error terms due to initial tolerance, temperature and aging. In addition to the worst-case stack of crystal-frequency tolerances on the receiver and the transmitter, engineers selecting minimum IFBW must also consider the necessary RF spectral bandwidth for transmitting the RF data packet at a desired baud rate and modulation.

In-Band Interference

Engineers must approach unwanted RF signals within the desired operating frequency spectrum differently from the way in which they approach other unwanted signals. With RF signals, it is impossible to differentiate between a strong source of interference and the intended RF data packet. The use of redundant information is the only method of mitigating this problem. To convey redundant information, systems use either time-domain redundancy or a combination of time- and frequency-domain redundancy.

When the source of interference is intermittent, it is possible to send multiple copies of the same RF data packet, delayed by a finite amount of time. Figure 4 illustrates this scenario. This straightforward approach enables the use of one RF-carrier frequency for both the transmitter and the receiver sides of the RF system. This simple and low-cost approach is common. However, it is ineffective if the disturber has a continuous presence, as the red arrow in Figure 4 shows. With the recent releases of advanced and inexpensive integrated-radio ICs, such as the ATA5831/2/3 and ATA5781/2/3, time- and frequency-redundancy methods are replacing this approach.

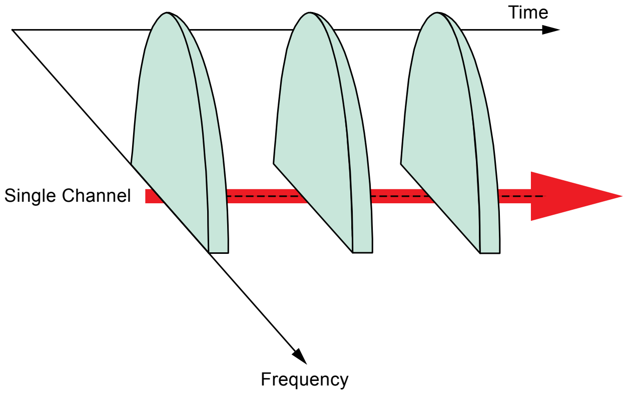


Figure 4. Single-Channel Time-Domain RF-Data-Packet Redundancy

By adding the dimension of frequency to the time-domain redundancy, a system can avoid a continuous RF disturber if the disturber's spectrum occupies a small frequency range. If the disturber occupies a wider frequency range than the channel spacing allows, problems may still occur. This approach offers a substantial improvement in radio performance. Figure 5 represents the time domain on the horizontal axis and shows redundant data packets that occur after a finite time delay. The vertical access represents the frequency domain and shows redundant RF spectral content appearing on different frequencies—for example, channels 1, 2 and 3. A red arrow represents the disturber, which disturbs only Channel 1 but not redundant channels 2 and 3.

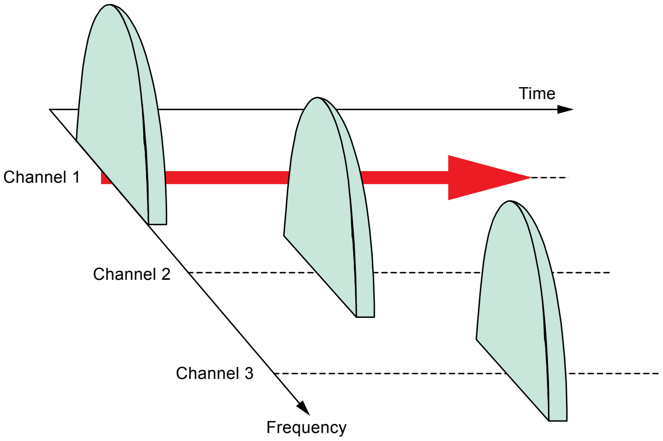


Figure 5. Multichannel Time- and Frequency-Domain RF-Data-Packet Redundancy

Channel-frequency spacing must be at least as wide as the RF spectral content of the basic RF data packet to prevent channel overlap. Atmel recommends a channel spacing of at least twice the IFBW for the ATA583x and ATA578x. The channel spacing in today's automotive remote and passive keyless-entry systems typically ranges from 400 to 450kHz.

Factors influencing the selection of RF-data-packet spacing delay in the time domain include settling time to change channel frequency, managing the average amount of the RF carrier's on time and managing overall system response time. The channel-frequency settling times are typically less than 1msec and are of only second-order concern. The primary factor is managing RF energy to optimize range and maintain local regulatory compliance. Through duty-cycle averaging, systems can transmit higher peak RF power if the average power falls below the local regulatory agency's threshold. Higher output powers enable RF systems to attain greater range. Note that designers can also achieve range improvements on the receiver side of the system by specifying devices with high sensitivity, such as the ATA578x and the ATA583x.

RF Modulation

Amplitude-shift keying (ASK) and on-off keying (OOK) are not interchangeable terms. ASK is a special case of AM (amplitude modulation), whereas OOK is an RF carrier that gates on or off. Upon closer examination of the equations for ASK and OOK, these fundamental difference should become clear.

AM:

$F_{AM}(t) = \{1 + a \bullet m(t)\} \bullet A \bullet \sin(\omega t)$, where

- **Asin(ωt)** is the RF carrier with amplitude A,
- **m(t)** is the modulation signal ranging in value from –1 to +1—typically, a sinewave—and
- **a** the modulation index that can possess a value from 0 to 1.

ASK modulation:

$F_{ASK}(t) = \{1 + a \bullet m(t)\} \bullet A \bullet \sin(\omega t)$, where

- **ASK** occurs when the modulation signal, **m(t)**, is a square wave, ranging in value from –1 to +1, and the modulation index, **a**, is 1;
- the maximum amplitude is 2A; and
- the minimum amplitude is 0.

OOK Modulation:

$F_{OOK}(t) = g(t) \bullet A \bullet \sin(\omega t)$, where

- **Asin(ωt)** is the RF carrier with amplitude A;
- **g(t)** is gating signal, which is either on with value 1 or off with value 0;
- the maximum amplitude is A; and
- the minimum amplitude is 0.

Although both ASK and OOK share an envelope profile, the amplitude of an ASK signal is twice as large as its OOK counterpart. Thus, receiver-sensitivity measurements with an ASK-modulated input will yield a 6dB better value than the same receiver using an OOK-modulated signal.

Due to the fundamental differences in the methods for measuring ASK and OOK sensitivity and the inherent characteristics of the receiver itself, a receiver that uses frequency-shift-keying (FSK) modulation tends to have an overall sensitivity advantage of 4 to 6dB over a comparable OOK-modulation receiver.

The selection of FSK versus OOK also has implications on the receiver's ability to perform when encountering interference and jamming signals. Demodulation errors generally appear in an OOK receiver if the disturbance measures 10 to 12db below the desired RF signal. In the case of Atmel ICs, these errors occur when the bit-error rate is larger than 0.001 if the disturber is greater than 10 to 12dB below the desired RF signal. However, with an FSK receiver, the RF disturber must be larger—typically, 4 to 6dB below the useful signal—before errors occur. Thus, it appears that FSK modulation is superior to OOK in this regard.

However applications that are subject to stringent power-consumption requirements favor OOK modulation because, assuming Manchester encoding, it uses 50% less energy during RF transmission than FSK due to the on/off cycling of the RF carrier. With FSK, the RF carrier is continuously on during FSK modulation because only frequency is shifting.

Sensitivity

In-Band Interference

System data rate has a tangible effect on system performance. In some cases, data rate is fixed. However, when designers have the flexibility to do so, they should choose a lower data rate because it generally improves receiver sensitivity when all other things remain constant. In practice, doubling the data rate causes the receiver to lose 3dB of sensitivity. Table 1 illustrates this effect with an example from the ATA573x receiver datasheet.

Sensitivity (dBm)	Data Rate (kbps)
–108	20
–111	10
–114	5

Table 1. ATA573x Sensitivity versus Data Rate (FSK, Manchester, IFBW=165kHz)

Optimum FSK Deviation

What may have been true in the past with classical analog radio architectures no longer applies to many of today's advanced and state-of-the art radios, which use advanced digital baseband-signal processing. The rule of thumb in classical radio design suggests that smaller frequency deviations in FSK will result in better sensitivity. However, this rule no longer holds when a system uses digital-signal-processing techniques to extract data.

When working with these radio architectures, designers should carefully review datasheet information to ensure that they understand how to achieve optimal sensitivity. Taking this step during the initial radio-specification phase of development can yield tangible benefits in performance. For example, in the case of the ATA573x receiver, FSK sensitivity is optimized when F_{DEV} equals the data rate of the modulated data.

RF-Carrier Frequency

Much debate centers on the topic of whether high-band carrier frequency of 869 to 915MHz or low-band frequency of 315 to 434MHz provides optimum performance for automotive remote and passive keyless-entry systems. Insight on this debate rests in a better understanding of fundamental characteristics of each frequency band.

Output Power

Most regulatory agencies allow higher radiated transmit powers in the high band, which brings the perception of greater system range. However, an unintended consequence of the popularity of high bands is that their use results in a higher occurrence of disturbers, which can compromise RF-system performance. Power disturbers also exist in the low band. However, RF systems are more likely to encounter RF disturbers of higher amplitude because the high band is more popular and tends to be more congested with applications taking advantage of the higher allowable transmitted powers.

Path Loss

Another parameter to consider is the RF path loss, which increases with frequency. To compensate for the higher path loss, designers must increase the transmitter's effective radiated power, and they can accomplish this task only by selecting a transmitter with higher output power capability or using a more efficient antenna. When factoring path loss, transmit power and antenna efficiency into an RF-link budget analysis, designers may find that the perceived benefit of higher transmit power in the high band has only a marginal effect on the operating range of the system.

Antenna

A benefit of high-band operation is that it enables designers to implement highly efficient dipole antennas using smaller physical geometries due to wavelengths that are two to three times shorter than those in the low band. This feature is attractive not only for handheld remote-key-fob applications but also for the vehicle side. However, high-band RF tends to propagate more directionally and may provide less consistent performance than low-band systems around the contours of an automobile.

IFBW and Crystal Tolerance

When selecting and specifying a design's reference-frequency crystal and associated tolerance, it is important to understand the influence this parameter has in high- and low-band systems. For example, a typical crystal with a 150-ppm frequency tolerance will yield a high-band transmitter-output frequency of 915±137.25kHz, whereas that same crystal in a low-band transmitter will result in an output frequency of 315MHz±47.25kHz. To accommodate this frequency variation, the IFBW of the high-band receiver must be nearly three times wider than the137.25K or 47.25kHz the low band requires to capture the transmitted spectrum. Because receiver sensitivity is generally inversely proportional to its IFBW, this variation will desensitize the high-band system and reduce the operating range of the system.

Alternatively, to mitigate this effect, designers could specify a crystal with lower tolerance, such as 50ppm, in the high-band application to achieve a comparable IFBW setting—such as 915MHz×50ppm=45.750kHz versus 315MHz×150ppm=47.25MHz. However, this approach involves cost trade-offs.

Summary

This article introduces common RF-system attributes and explores their effects on the robustness and reach of automotive RF-wireless applications. It covers system requirements, such as carrier frequency, FSK frequency deviation, modulation data rate and data redundancy with single and multiple channels. It also covers receiver characteristics, such as bandwidth, sensitivity and blocking. Table 2 illustrates how trade-offs drive the design and specification of today's automotive RF-based access-and-control systems.

System	Objective	Attributes	Benefit
Remote start (RS)	Long range: 100 to 300m	Data rate: 0.5kbps Modulation: OOK Low band: 315/434MHz	• Best sensitivity • Less current in slower RF data packet • Lower path loss, less directional and less stringent crystal tolerance
Remote keyless entry (RKE)	Medium range: 10 to 30m	Data rate: 2kbps Modulation: FSK Multichannel Low band: 315/434MHz	• Fast response • High sensitivity and noise immunity • Robustness to interference • Lower path loss, less directional and less stringent crystal tolerance
Passive entry/passive start (PEPS)	Short range: 1 to 3m	Data rate: 8kbps Modulation: FSK Multichannel Low band: 315/434MHz	• Fastest response • Good sensitivity and noise immunity • Robustness to interference • Lower path loss, less directional and less stringent crystal tolerance

Table 2. Typical RF Specifications in Automotive RF Access-and-Control Systems

Automotive Passive-Entry Passive-Start (PEPS) Messaging Anticollision Principles

George Rueter

This article describes methods of arbitrating key-fob authentication and the ability to detect when multiple fobs are present in a passive-entry passive-start (PEPS) system. Stringent response-latency requirements and support for as many as eight active fobs mandate the need for efficient protocols and compromises in PEPS-system design. Considerations in the design of a PEPS system include key-fob identification and authentication, message collision avoidance and handling and minimal response time.

Passive-Entry Passive-Start Architecture Overview

The PEPS system enables hands-free vehicle functions, allowing the driver to lock and unlock doors and to start and stop the engine without pressing any buttons on the key fob and without using a mechanical key. These functions require the PEPS system to determine fob presence and its location and then authorize all actions using encrypted messaging. Figure 1 shows an overview of the internal system, which includes six low-frequency (LF) transmitting antennas.

Fob localization

The localization, or determining the location, of the key fob—inside or outside the vehicle, in the front seat or the back seat or behind the vehicle—is an important function of any PEPS system. Depending on the localization strategy, one or more LF transmitting antennas can be active to achieve this goal. The use of more than one antenna is typical and allows for a more accurate determination of the fob's location.

Designers typically accomplish this localization by using fob-reported LF RSSI (received-signal-strength-inidicator) values, indicating proximity to a transmitting coil in a known location, such as the door handle. In combination with that

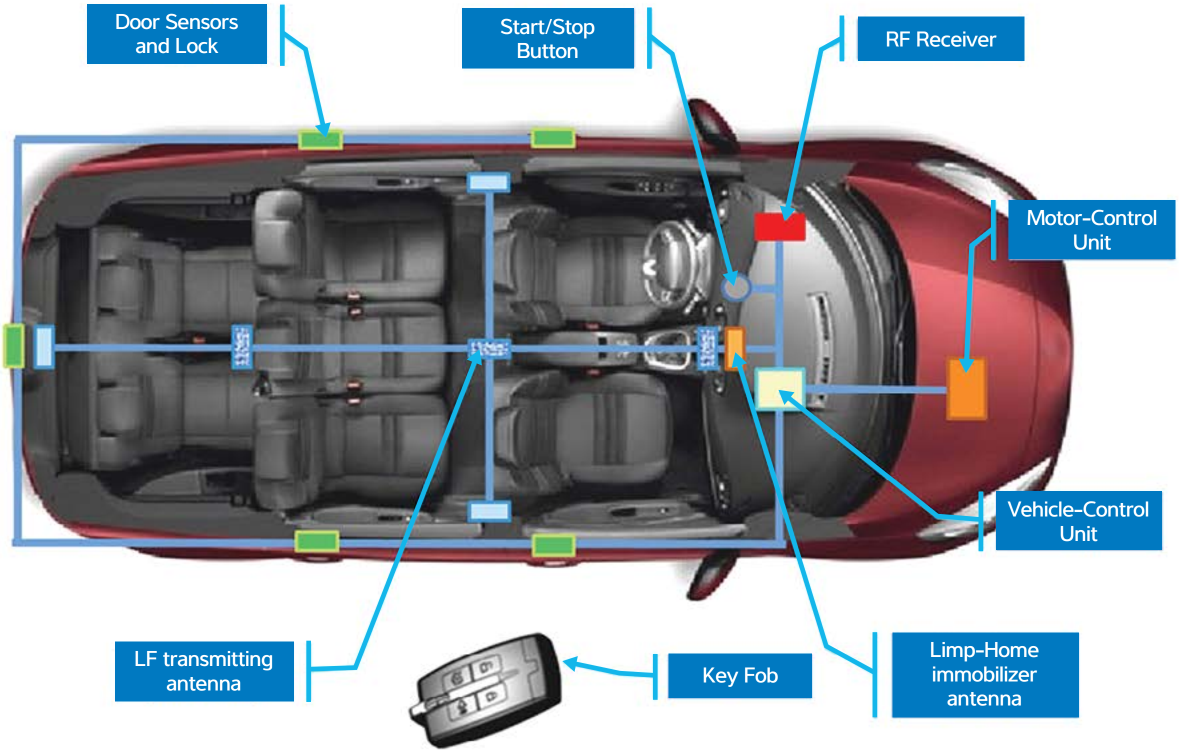


Figure 1. Typical PEPS implementation

method or as an alternative to that method, they can use fob-reported LF RSSI messages from multiple LF antennas to accurately establish fob location. For example, when the RSSI value for an LF antenna in the center stack is larger than the RSSI value from the LF antenna in the driver-side door handle, and the passenger-side door handle reports no LF signal, the fob is in the car and near the driver's seat.

Localization has significant safety ramifications. The car must not start unless someone is in inside, and the doors must not unlock when someone is inside. No PEPS-command function can occur until these localization requirements have been satisfied.Localization has significant safety ramifications. The car must not start unless someone is in inside, and the doors must not unlock when someone is inside. No PEPS-command function can occur until these localization requirements have been satisfied.

Passive-Entry Function

The passive-entry function allows the driver to unlock the vehicle's doors without any key-fob interaction. Typically, a user action triggers the system, usually when the user approaches the vehicle or touches a button on the door handle. Those actions trigger the following sequence of events to occur:

1. The vehicle transmits an LF message containing an encrypted challenge message. Multiple LF antennas may transmit this message sequentially.
2. The fob receives the LF message and responds with an RF message transmission containing the encrypted challenge response, fob ID and RSSI signal levels of the received LF message or messages.
3. The vehicle receives and authenticates the RF message and then locates the fob using RF-response-message values for the LF RSSI.
4. If the vehicle can locate the fob in a designated region, typically outside the door, the door will unlock.

Passive Start/Stop Function

The passive start/stop function allows the driver to start the vehicle without using the key fob. The operator typically initiates this function by pressing a start/stop button on the car's dashboard. This action initiates the following sequence of events:

1. The vehicle transmits an LF message containing an encrypted challenge message. Optionally, the vehicle can transmit this message sequentially on multiple LF antennas.
2. The fob receives the LF message and responds with an RF message containing the challenge response, fob ID and RSSI signal levels of the LF message or messages.
3. The vehicle receives and authenticates the RF message and then locates the fob using RF response-message RSSI values.
4. If the vehicle locates the fob in an allowed region—typically, the driver's seat—the car starts.

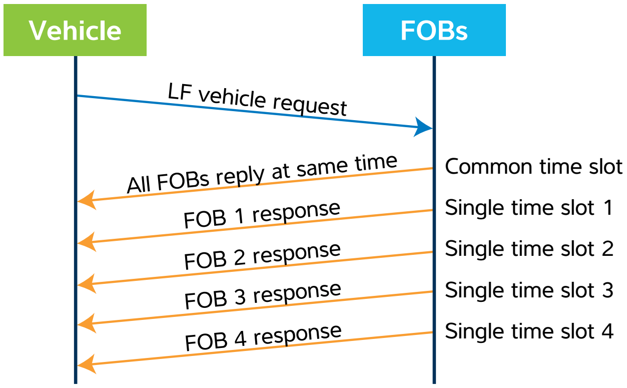
Multiple key fobs

The design of a PEPS system is complex because a vehicle can have as many as four valid key fobs. In any lock, unlock, start or stop action, as many as four fobs can respond to the same vehicle-generated LF message. If more than one key fob replies with an RF transmission, the signals become corrupted because they are transmitting simultaneously. In this case, the vehicle-side receiver cannot receive and decode the messages. This article focuses primarily on the management of these multiple fobs and their RF responses.

PEPS RF Anticollision Strategy 1: Time-Division Multiplexing

Fob RF response in allocated time slots

One strategy uses fob response in allocated time slots, which achieves the anticollision process by defining time slots for the multiple fobs to send their RF responses. However, the process starts with a common time slot in which all fobs transmit. In this way, if only one fob is present, the RF reply occurs quickly. If more than one fob is present, the common-time-slot RF messages collide, allowing the reception of the RF responses on the allocated time slots. This approach decreases the response time when only one key fob is present in the vehicle. The number of slots depends on the number of fobs a vehicle has—that is, a vehicle with four fobs will have four defined time slots.



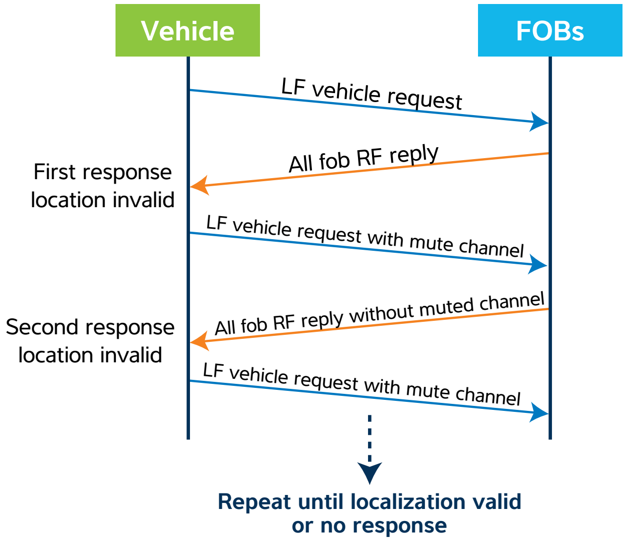
The default anticollision-time-slot order is that the single slots follow the common slot in numerically ascending order. The vehicle can also modify the fob reply order with a field in the LF command. For example, if the vehicle's main driver is using Fob 4, this fob should use Time Slot 1. Designers can accomplish this goal by setting the fob that replied during the last PEPS process as the first-priority fob because this key fob will most likely be used during the next PEPS operation. Thus, vehicle will adjust the reply order within the LF message field so that this fob replies first.

The advantages of this approach are that it requires transmitting only one LF message and that it is a traditional, well-proven practice. The disadvantage is that it requires precise timing in both the vehicle and the fob.

PEPS RF Anticollision Strategy 2: Frequency-Division Multiplexing

Fob RF response on allocated frequencies

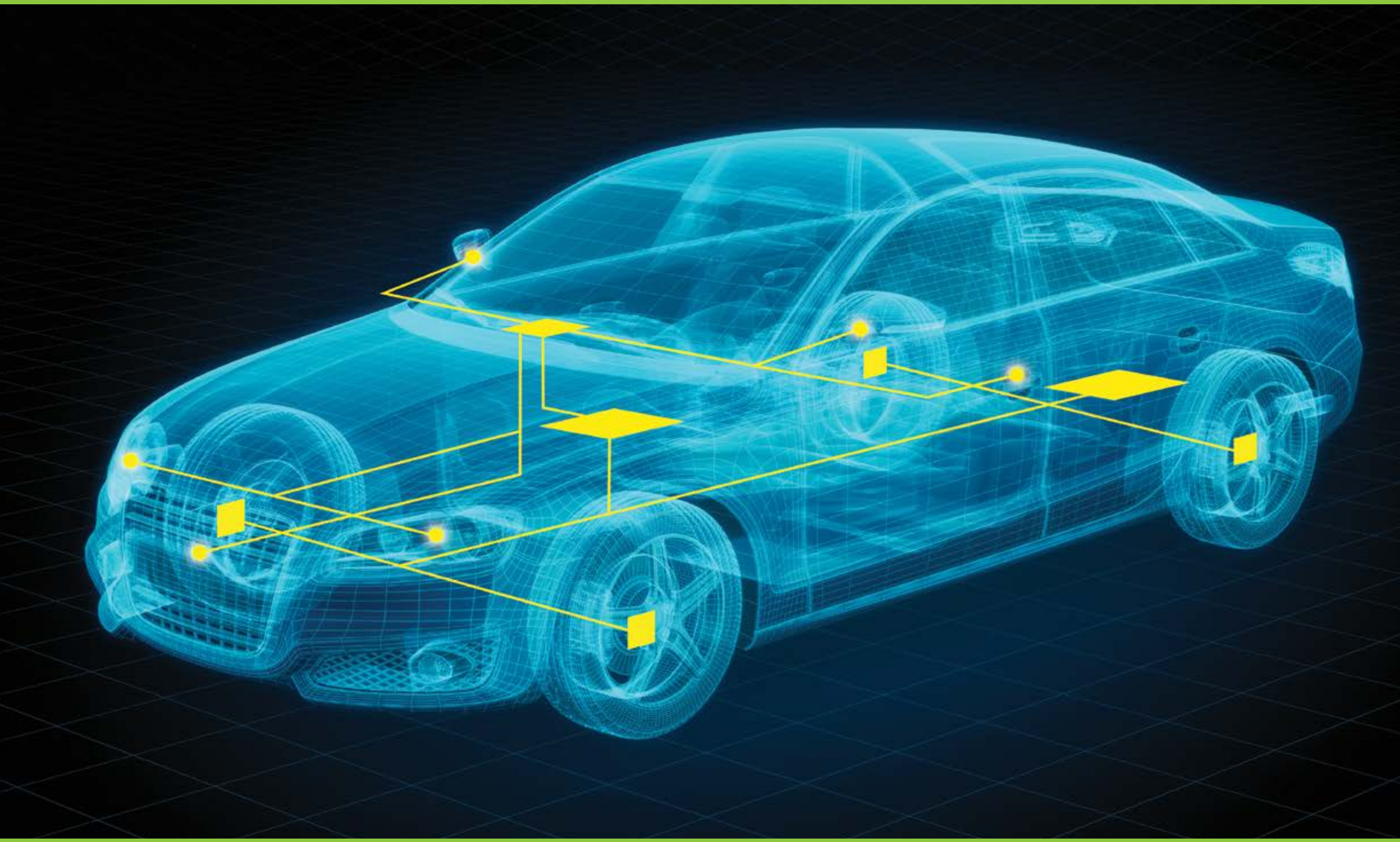
Using fob response on allocated frequency, designers can achieve the anticollision process by assigning RF frequencies for each of the fobs. The vehicle must poll all potential frequencies after the LF message transmission. The RF message preamble must be long enough—typically, no longer than a few milliseconds—to allow the vehicle to poll, or scan, all possible fob frequencies. Because all fobs may respond at once, the system must have sufficient guardband between each fob's assigned RF frequencies. After the vehicle transmits the initial LF message, it validates and localizes the first received response, but the response may not satisfy the localization requirements. In this case, the system transmits another LF message that includes a ˵mute˝ command for the fob or fobs that have communicated. The sequence repeats until one fob or all of them pass the localization test.


Vehicle
FOBs
LF vehicle request
All fob RF reply
First response location invalid
LF vehicle request with mute channel
All fob RF reply without muted channel
Second response location invalid
LF vehicle request with mute channel
Repeat until localization valid or no response

The advantages of this approach are that it requires no precision timing, has a rapid response time if the first response is in the correct location, and requires no waiting for time slots. The disadvantages are that it may require the transmission of multiple LF messages, requires a polling RF receiver and has increased bandwidth requirements.

Conclusion

Managing as many as four fobs in a PEPS system requires an anticollision strategy to ensure a satisfactory response time and guarantee a response from any key fob. This article presents options, including management of multiple fobs using response time slots or multiple RF frequencies. Both strategies have advantages, and both are effective at achieving the end goal of a stable system with an acceptable response time.



CAN FD (Controller Area Network with Flexible Data rate): Atmel´s new high-speed CAN transceivers perfectly serve the new trend

Daniel Yordanov, Berthold Gruber

Today´s cars are becoming increasingly complex and are undergoing the continuous addition of features. These factors have led to the need for more electronic-control units (ECUs) in vehicles, and this combination of requirements can push a CAN´s communication bandwidth to its limit. Solving this problem by using multiple CAN buses or by switching to another protocol requires a lot of system-design effort and the replacement of hardware and software. CAN FD (Flexible Data) rate extends the CAN standard and permits significantly higher data rates, enabling faster firmware upgrades and leaving most of the software and hardware, especially the physical layer, unchanged.

CAN FD improves the bandwidth usage of the CAN protocol, the dominant bus system in the automotive industry. To achieve the increase in the protocol's bandwidth efficiency, CAN FD frames support dual-bit-time capability and normal bit time during the arbitration phase. The bit time is identical to that of the current CAN protocol. This time includes those fields in which multiple devices can transmit simultaneously: at the arbitration start and acknowledgement end. Those fields are the start-of-frame (SOF) bit, the 12-bit arbitration-field, 3 control bits, the acknowledge bits, the acknowledge-delimiter bit, the 7-bit end-of-frame (EOF) field, and the 3-bit interframe space.

Further, CAN FD allows a reduced bit time in the data phase and other fields, and the timing requirements for these fields are less stringent because CAN FD guarantees that only one device is communicating on the bus. These fields are: 1 control bit; a 4-bit DLC (data length code); payload data; and CRC- field (cyclic redundancy check), which, depending on the data length, is 21 or 25 bits.

CAN FD also increases the payload capacity. The data-field length increases from 8 bytes to 64 bytes , improving the efficiency of the CAN protocol. To take advantage of this improvement, the system software also requires updating.

CAN FD Use Cases

Fast Software Downloads

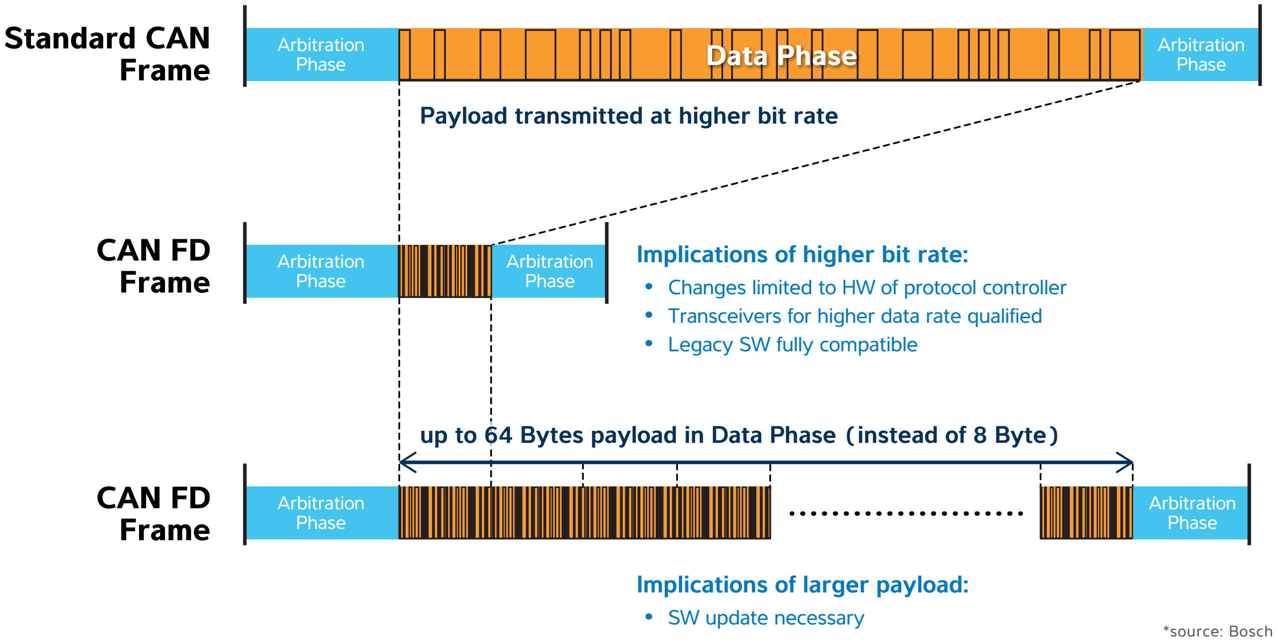
CAN FD speeds end-of-line programming of vehicles' ECUs. GM states that, with the use of CAN FD, the ECU programming time is only one-third or even one-fifth of the current programming time [1]. Likewise, diagnostics and software upgrades in repair garages are also faster.

Error Status

A transmit-node error may result in a sudden stop of the message, thus affecting safety-critical systems. Every CAN FD message includes the condition of the transmit node in the error-status-information (ESI) bit. In this way, the receiver can monitor the transmit node and take fail-safe actions before any issues occur.

Increased Data Payload

CAN FD allows messages as long as 64 bytes to avoid splitting long messages. This feature results in a simplified transport layer of the CAN stack and requires no implementation of complex flow-control mechanisms involving multiple messages.


Standard CAN Frame
Arbitration Phase
Data Phase
Arbitration Phase
Payload transmitted at higher bit rate
CAN FD Frame
Arbitration Phase
Arbitration Phase
Implications of higher bit rate:
• Changes limited to HW of protocol controller
• Transceivers for higher data rate qualified
• Legacy SW fully compatible
up to 64 Bytes payload in Data Phase (instead of 8 Byte)
CAN FD Frame
Arbitration Phase
Arbitration Phase
Implications of larger payload:
• SW update necessary

*source: Bosch

Figure 1. Comparison of Classical CAN versus CAN FD timing

Faster Communication Between ECUs

The increasing amount of automotive features leads to an increase in data exchange among the automotive ECUs. With its higher bandwidth, CAN FD can easily handle the higher amount of data, and it enables speeds similar to those of FlexRay.

Reduced Bus Loads

As a result of the higher communication speed, the ECUs can more quickly send and receive data using CAN FD frames rather than the standard CAN frames. This feature directly reduces bus loading. For example, an instrument cluster can inform a driver of many vehicle parameters. It drives three to seven gauges, controls 20 to 30 telltale devices, generates chimes, and displays signal warnings to indicate status or system malfunction.

This node receives and transmits information via many CAN messages from multiple ECUs. Because CAN is a priority-based protocol, it delays lower priority messages and increases bus loading. These issues result in reduced response time, and the CAN load on such a system can be 75 to 80%. CAN FD alleviates this problem by reducing the CAN bus load by more than 75%.

Transmission-Line Length

Networks in trucks or articulated buses can be as long as 9 to 20 meters, or approximately 3 to 6 feet. The arbitration field limits the speed of the entire network. The J1939-14 standard defines a maximum bit rate of 500kBit/s. However, CAN FD enables much higher speeds. The arbitration fields may remain at 500kBit/s, whereas the data payloads can be at much higher data rates, thus increasing the throughput of the network.

New Features in CAN FD

The FDF (FD Format) bit distinguishes between a CAN FD frame and a classical CAN frame. The classical CAN frame format is dominant, and the CAN FD frame format is recessive. Dominant means, "Do not switch to higher bit rate—that is, maintain the same bit rate in the arbitration and the data phases," and recessive means, "Switch to higher bit rate." With the ESI bit, dominant is the error-active node. The BRS (bit-rate-switch) bit allows the CAN FD rate to immediately start at the sampling point of the BRS. A recessive error indicates the passive node.

The res (reserved) bit follows the FDF bit and is reserved for future protocol expansions. In this field, dominant is the standard value. In this field, an FD-enabled receiver detects a protocol-exception event, during which it detects the res bit as recessive instead of the expected dominant value. Modified CRC maintains the same hamming distance for the longer frames as classical CAN frames. For CAN FD frames, the CRC field also contains the bit-stuff count.

Migration from CAN to CAN FD

The introduction of CAN FD will not affect today's vehicle networks, such as LIN (local-interconnect network) and MOST (media-oriented systems transport). However, migration paths are necessary to include CAN FD into current CAN networks. A CAN FD-compliant node can accept classical CAN frames and CAN FD frames without any errors, but a classical CAN node will generate an error frame on the network in the presence of CAN FD frames. OEMs can use any of several approaches to ease migration efforts to a true CAN FD network.

OEMs should note that new ECUs deployed in the network must be CAN FD-compliant, meaning that both the CAN controller and the CAN transceiver must be FD-compliant and still operate within the classical CAN communication-frame format. Also, when upgrading the software, OEMs should integrate new CAN drivers that will have only minimal or no effect on the upper layers. Further, limiting the payload to 8 bytes can restrict any software changes to the CAN driver only, and achieving higher data rates requires a software update to incorporate the CAN FD frame format.

OEMs can realize a true CAN FD-compliant network by using software updates to support payloads as large as 64 bytes for high bandwidth efficiency, by using CAN FD-qualified transceivers for much higher data rates or by implementing both of these methods.

New Generation of Atmel CAN-Transceiver Family

To serve the rapidly increasing bandwidth requirements in automotive networks, Atmel has developed the new Atmel® ATA6560 and ATA6561 high-speed CAN FD transceivers that provide an interface between a CAN-protocol controller and the physical two-wire CAN bus. The transceivers target use in automotive applications requiring speeds as high as 5Mbit/s and the ability to provide differential transmit and receive capability to a microcontroller with a CAN-protocol controller.

Due to their excellent electromagnetic compatibility (EMC), the devices guarantee operation as fast as 2Mbit/s without a common-mode-choke (CMC). Radiated-emission test passed at 2Mbit/s without a CMC.

The Atmel ATA6560 the ATA6561 provide excellent choices for all types of high- speed CAN networks, especially in nodes requiring low-power mode with wake-up capability via the CAN bus. They provide:

- improved electrostatic-discharge (ESD) performance;
- low quiescent current;
- ideal passive behavior to the CAN bus when the supply voltage is off;
- the ability to directly interface with microcontrollers with voltages of 3 to 5V (ATA6561);
- three operating modes; and
- dedicated fail-safe features.

Figures 2 and 3 show the typical application circuits for the new CAN transceivers, which are available in SO8 and DFN8 packages with wettable flanks, allowing automatic optical inspection of the solder joints.

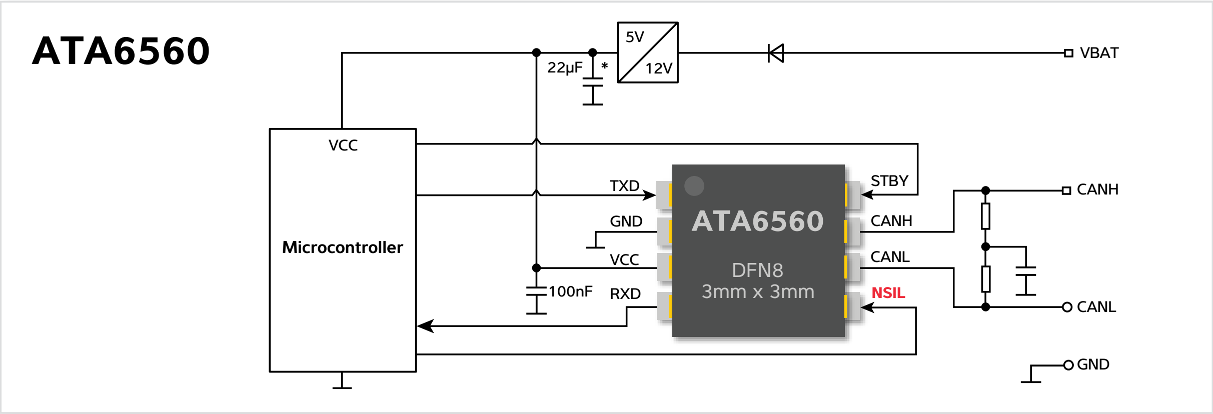
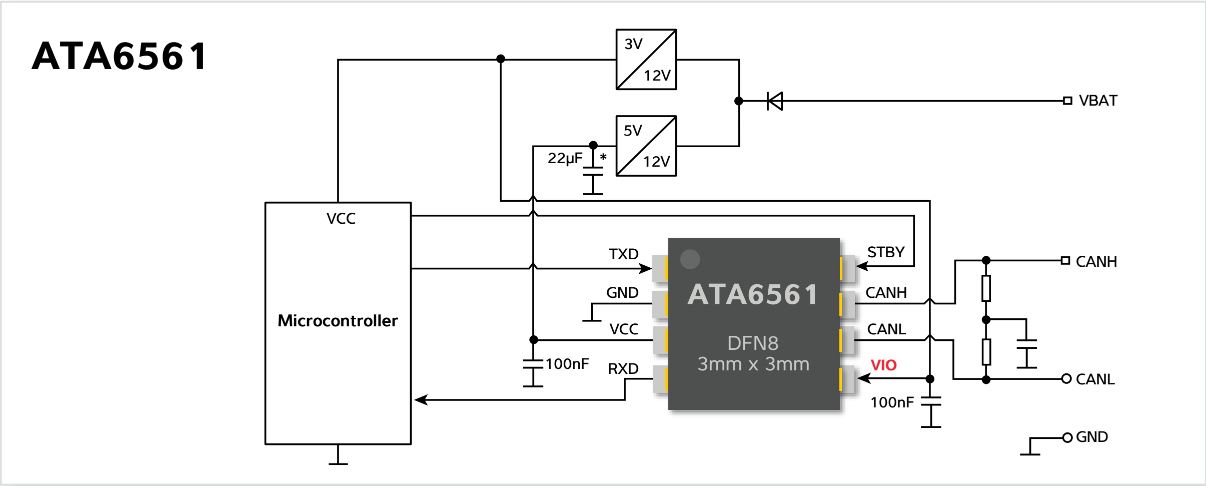


Figure 2. Typical Application Circuit of the ATA6560



*The size of this capacitor depends on the selected external voltage regulator.

Figure 3. Typical Application Circuit of the ATA6561

Summary

- CAN FD provides increased throughput at costs comparable to those of currently available CAN networks.
- CAN FD provides additional bandwidth and higher speeds. For automotive applications, CAN FD targets an average data rate of 2Mbit/s with currently available CAN transceivers, resulting in the ability to carry the same effective payload as a low-speed FlexRay network.
- CAN FD maintains the reliability of the classical CAN due to changed CRC polynomials.
- ATA6560 and ATA6561 perfectly suit the new CAN FD world and classical CAN applications
- The devices provide an easy migration path from classical CAN systems to CAN FD systems because there is no need to change CAN application software, except for configuration software.

Outlook: Auto Compilation 2016

A second new trend in the CAN world, for which Atmel also provides a solution, is partial networking for CAN-bus systems. The following is just a short overview; the next edition of Atmel's Automotive Compilation will describe it in more detail.

Carbon dioxide (CO2) is the primary component of greenhouse gases, and one of the larger sources of emissions. Cars that use fossil fuels, such as gasoline and diesel, contribute about 12% to these emissions. Governments around the world set mandatory emission-reduction targets for new cars. This legislation is the cornerstone of the strategy to improve the fuel economy of cars.

Vehicle manufacturers face a dilemma: On the one hand, regulations continuously are calling for massive reduction of CO2 emissions, and, on the other hand, the use of electronics in vehicles is increasing incrementally, in turn increasing electrical power consumption. Today's complex vehicles require more features, and the number of necessary ECUs is increasing significantly. Many of the ECUs—even if they are not in use—are permanently active, consuming around 2W. A modern car can have more than 70 ECUs, and many of them are not in use during approximately 95% of the time a car is operating. The potential waste of energy and fuel and increase in CO2 emissions are considerable.

With partial networking, one ECU or a cluster can remain in selective sleep mode without wasting energy when the vehicle does not require it. Partial networking enables the use of dedicated and predefined CAN messages, rather than bus activity, to wake up a node or a cluster.

With partial networking, all vehicle functions remain available at any time, and the approach requires no modification of network architecture and no additional components or external crystals.

From a CAN-transceiver manufacturer's point of view, a big change is necessary, and this change will bring more complexity to the simple CAN transceiver.

References

1. “CAN FD Positioned for Success,” *The Hansen Report on Automotive Electronics,* Vol. 25, No. 10, December 2012/January 2013,Portsmouth, New Hampshire.
2. Hartwich, Florian, “CAN with Flexible Data-Rate,” Robert Bosch GmbH, www.can-cia.org/fileadmin/cia/files/icc/13/hartwich.pdf.
3. Hammerschmidt, Christoph, “Ethernet succeeds in automotive environments,” *EETimes Automotive Europe,* Oct. 14, 2011, www.automotive-eetimes.com/en/ethernet-succeeds-inautomotive-environments.html?cmp_id=7&news_id=222901844.
4. “Ethernet to gain ground in automotive applications, Bosch predicts,” *EETimes,* Feb.5, 2011, www.eetimes.com/electronics-news/4212870/Ethernet-to-gain-ground-in-automotive-applications--Bosch-predicts.
5. Butzkamm, Cornelius, and David Bollati, “Partial Networking for CAN bus systems: Any saved gram CO2/km is essential to meet stricter EU regulations,” C&S group GmbH, iCC 2012.

A New Generation of Atmel LIN Devices

Daniel Yordanov, Berthold Gruber

The Local Interconnect Network (LIN) is a serial protocol used for in-car communications. LIN systems are typically used throughout the automobile in comfort, powertrain, sensor and actuator applications, where a maximum data rate of 20kBit/s is sufficient and where safety is not critical.

The rapid growth of the LIN market parallels continually increasing needs for greater system efficiency, higher integration and lower costs. The next generation of LIN devices must deliver the flexibility to adapt to evolving requirements such as these.

Atmel® supports a wide range of in-car applications with a new generation of modular LIN devices. These products range from simple voltage regulator ICs to complex system basis chips (SBCs). Using this new Atmel LIN device family gives designers the flexibility to develop a single-board design serving various applications. A single package footprint across the entire family also makes it easy to upgrade designs using various devices. In addition, to meet the needs of space-saving applications, Atmel ATA663x devices are available in the DFN8 package (ATA6632xx) and the DFN16 package (ATA6633xx and ATA6634xx). All devices respectively all packages have wettable flanks that allow optical inspection of the soldering.

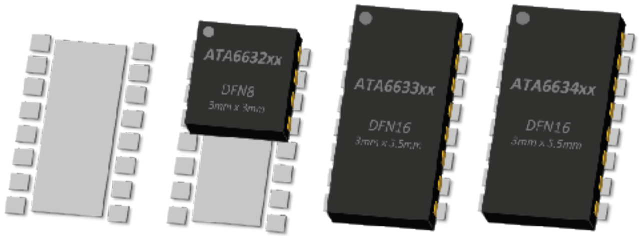


Figure 1. Single footprint for the complete SBC family.

The Atmel **ATA663x** device family includes five sub-families:

- The Atmel **ATA6632xx** device sub-family includes three basic products: a LIN system basis chip (SBC), a LIN transceiver and a low-drop voltage regulator
- The Atmel **ATA66323x/5x** system basis chip is a fully integrated LIN transceiver—designed according to the LIN specification 2.2 and SAEJ2602-2—together with a low-drop voltage regulator (3.3V/5V/85mA)
- The Atmel **ATA663211** transceiver is a fully integrated LIN transceiver designed in compliance with the LIN specification 2.2 and SAEJ2602-2. It interfaces the LIN protocol handler and the physical layer
- The Atmel **ATA66320x** voltage regulator is a fully integrated low-drop voltage regulator, with 5V output voltage and 85mA current capability
- The Atmel **ATA6633xx** is a new generation of system basis chips with a fully integrated LIN transceiver designed in compliance with LIN specifications 2.2 and SAEJ2602-2, a low-drop voltage regulator (3.3V/5V/85mA), two low-side drivers, and one high-side driver. With its two low-side drivers, this device can control two relays that form a H- bridge, so that a motor can be driven easily in both directions
- The Atmel **ATA6634xx** is a new generation of system basis chips with a fully integrated LIN transceiver designed in compliance with LIN specifications 2.2 and SAEJ2602-2, a low-drop voltage regulator (3.3V/5V/85mA), a window watchdog with Limp Home output and a high-side driver

All ATA663x devices are designed to handle low-speed data communication in vehicles (such as in convenience electronics). Improved slope control at the LIN driver ensures secure data communication up to 20kBit/s. The bus output is also designed to withstand high voltages without additional protection circuitry.

The improved sleep mode and silent mode guarantee minimized current consumption even in the event of a floating or short-circuited LIN bus, or at undervoltage conditions.

The new linear low-drop voltage regulator—whether standalone or integrated into the SBCs—is especially designed for the automotive environment. A key feature is that the current consumption always remains below 170µA (without load) even if the supply voltage drops below the regulator's nominal output voltage. The improved design allows the usage of multilayer chip capacitors (MLCC) with a very low ESR value, which delivers a cost advantage compared to tantalum capacitors.

The following pictures show how a single layout and board design can address various applications. It is just a matter of using different mounting options. In the same application the level of the integrated devices will be different, depending on the end customer's desired add-on features. However, using different boards for every configuration would drive the cost of the given application beyond an affordable level. Take the simple example of a car door application: the window lift can be electrically driven or not; it can have electrical or mechanical lock/unlock; it can integrate ambient lighting into the door; or it can have an electrical or mechanical adjustable rearview mirror. The end customer can select some, all or none of these features, which means the car manufacturer requires a highly flexible platform.

The Atmel ATA663x device family is specifically designed to meet demands such as these, thus offering a more competitive price for Atmel customers. Additionally, a single board for various applications means a significant reduction of the qualification, and therefore the production costs.

Typical Applications Using the Different Derivatives

Typical application with the ATA663211 standalone LIN-transceiver

Unlike other devices in the Atmel LIN family, the standalone ATA663211 LIN-transceiver has no integrated voltage regulator. Consequently, its applications typically require an external logic supply voltage and an external pull-up resistor between the RXD-output pin and the external logic supply voltage. The logic supply voltage usually supplies the connected microcontroller in the application. Also an INH high-side output is available that allows the control of an external voltage regulator. Using this approach, the complete LIN node can be activated if a valid wake-up signal occurs at the bus or at the WKin pin. The schematic is depicted in the figure 2.

Usually, the logic supply voltage is generated by a voltage regulator that also supplies the connected microcontroller in the application. Since the output pin RXD of the Standalone LIN transceiver is an open drain output an external pull-up resistor is required. With this approach, the RXD output is compatible to a 3.3V and a 5V supply.

The thresholds at the TXD input pin also allow the ATA663211 device to work with a 3.3V and 5V logic supply voltage. The TXD pin provides an internal pull-down resistor in order to have a defined level when the TXD pin is disconnected.

The high-voltage WKin input pin is used to wake up the ATA663211 device from Sleep Mode. It is usually connected to an external switch or a transistor to generate a local wake up.

Typical application with the ATA66320x voltage regulator

The ATA663205 voltage regulator is the only device in the family without a LIN transceiver. Only four pins of the DFN8 package are connected, so the application circuit is quite simple. In addition to the voltage regulator, the ATA663205 device provides also an undervoltage circuit that switches the NRES output to GND when the VCC output voltage falls below the corresponding undervoltage threshold. At power-up, the NRES output remains at low level for typically 4ms after the VCC voltage has exceeded its undervoltage threshold.

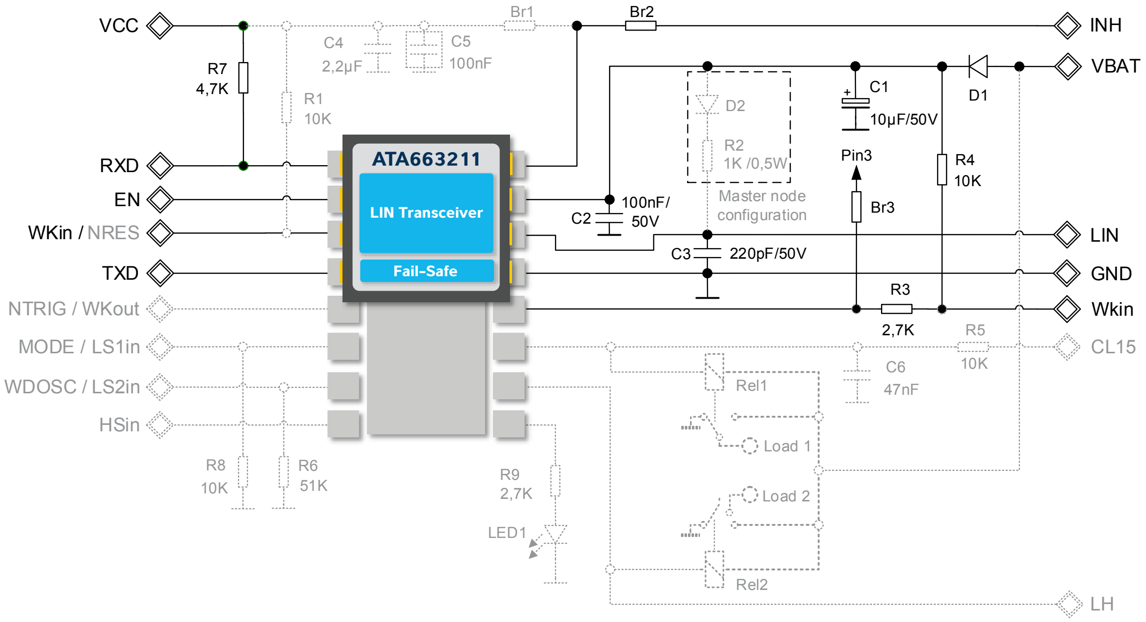


Figure 2. Mounting option for the typical application with the ATA663211 standalone LIN transceiver

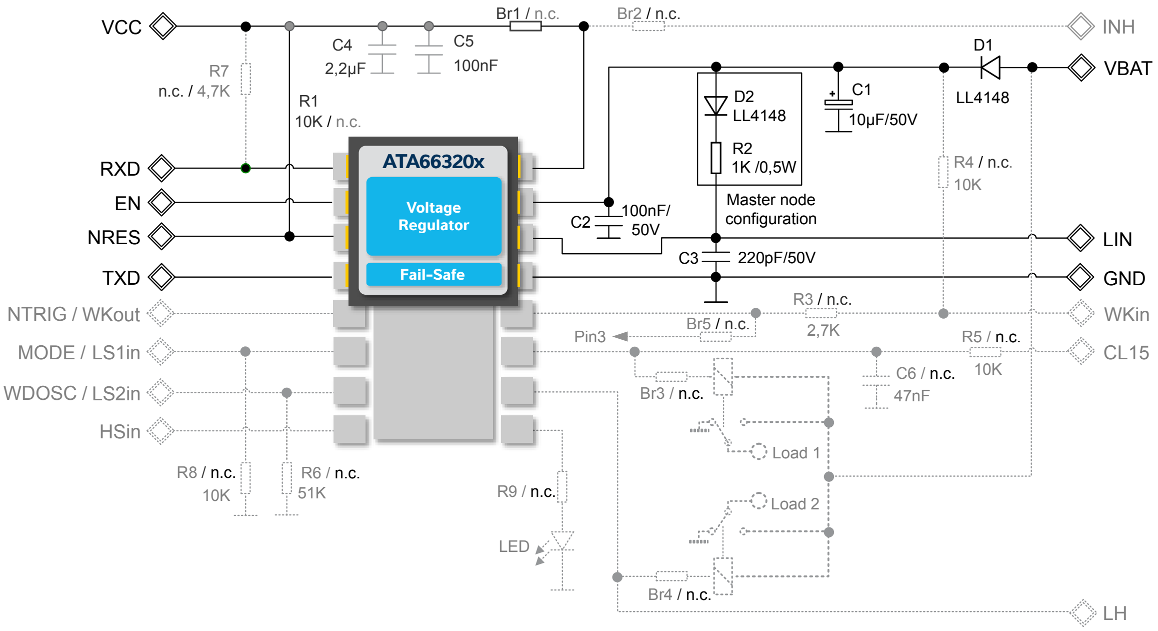


Figure 3. Mounting option for the typical application with the ATA66320x voltage regulator

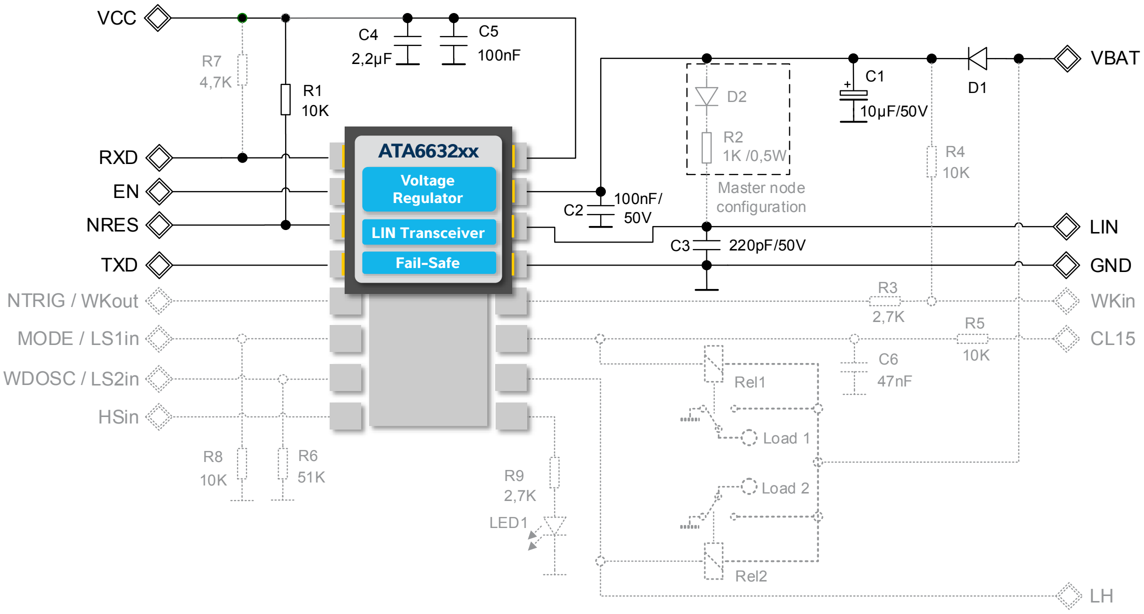


Figure 4. Mounting option for the typical application with the ATA6632xx SBC (LIN transceiver with LDO)

This 8-pin configuration is the base for the ATA6633xx and the ATA6634xx, which are 16-pin extensions of this LIN SBC. The upper eight pins are equal at all three devices.

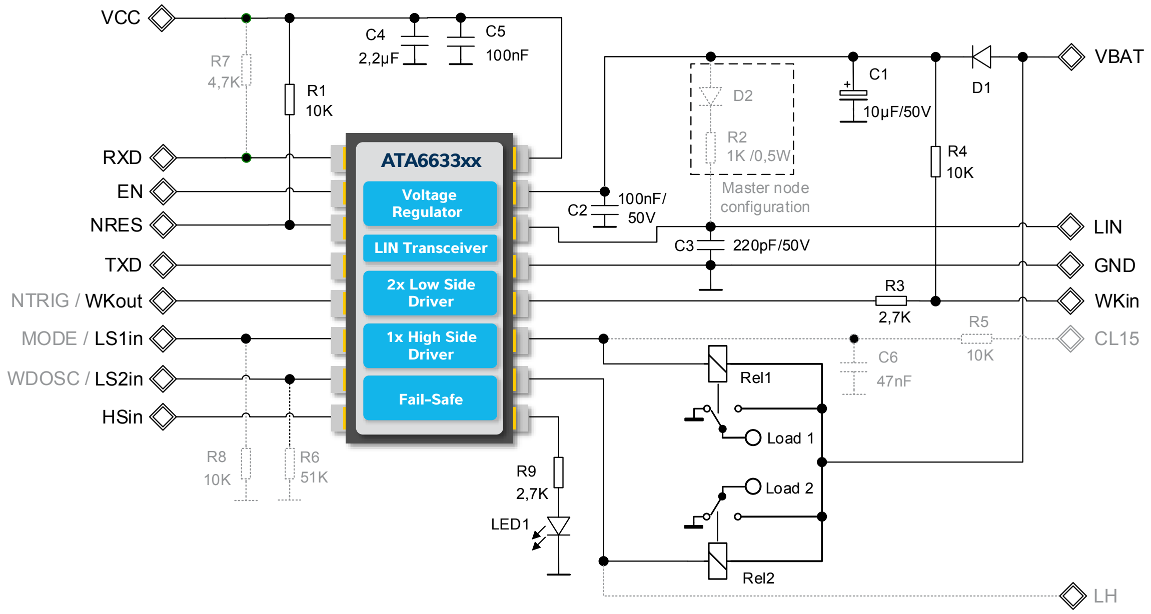


Figure 5. Mounting option for the typical application with the ATA6633xx SBC (LIN transceiver, LDO, two low-side drivers and one high-side driver)

Typical application with the ATA6632xx LIN-SBC (LIN transceiver + voltage regulator)

The combination LIN transceiver + voltage regulator allows the realization of cost-effective LIN nodes and delivers a broad range of flexibility, because these parts are always needed in a LIN node. The devices are available with VCC = 5V and VCC = 3.3V.

The ATA6632xx LIN-SBC has four different operation modes:

1) Normal Mode (transceiver and voltage regulator active)
2) Fail-safe Mode (voltage regulator active, this mode is entered after the supply voltage ramp-up and after a wake up request)
3) Silent Mode (only the voltage regulator is active)
4) Sleep Mode (voltage regulator is switched off, only the wake up function is activated)

The device can be switched into the current saving Sleep-respectively Silent Mode by setting the EN input pin to low. If the TXD pin is at high level during this falling edge the device enters Silent Mode; if it is at low level, the device enters Sleep Mode.

Typical application with the ATA6633xx LIN SBC (LIN SBC with two low-side drivers, one high-side driver)

In addition to the functionality provided by the ATA6632xx LIN SBC, the ATA6633xx device provides a high-voltage wake-up input pin with a low-voltage status output, two low-side drivers and one high-side driver.

The low-side drivers are usually used to drive relays (see schematic below). They are only functional in Normal Mode and are short circuit and overtemperature protected. They include an active clamping circuitry to provide a freewheeling path that is needed for inductive loads. The clamping voltage is typically > 44V. Each of the low-side drivers is directly controlled via a low-voltage input pin.

If an overload condition is detected, the appropriate driver stage is shut down. This shutdown is latched, which means the corresponding input pin has to go low first before the output can be restarted.

The high-side driver is designed for low-power loads such as with LEDs, sensors or a voltage divider for measuring the supply voltage. It is functional in all operation modes with the exception of the Sleep Mode and is protected against short circuits and overheating. A low-voltage input pin controls the high-side output driver.

All low-voltage input pins provide an internal pull-down resistor that keeps the corresponding driver OFF in the case of a disconnection at the input pins.

Typical application with the ATA6634xx LIN SBC (LIN SBC with watchdog, one high-side driver)

In addition to the functionality provided by the ATA6632xx LIN SBC, the ATA6633xx device provides two high-voltage wake-up input pins (one for a positive edge, and one for a negative edge), a window watchdog with Limp Home output and a high-side driver.

The window watchdog anticipates a trigger signal from the microcontroller at the NTRIG input within a specific time window, which can be adjusted via an external resistor at the WDOSC pin. If no trigger signal or a trigger signal with the wrong timing is received, a Reset signal is generated at the NRES output.

The watchdog is only active in Fail-Safe and Normal Mode.

The Limp Home output (LH) is a high-voltage NMOS open drain output that signals watchdog failures.

It works independent from the VCC voltage and the microcontroller. The LH output switches ON after power up or after a wake-up and could only be switched OFF again if three correct consecutive trigger pulses occur at the NTRIG pin. If a watchdog Reset occurs, it will be switched ON immediately.

The Limp Home function gives the user an additional security feature for its application. The high-side driver is the same as in the ATA6633xx.

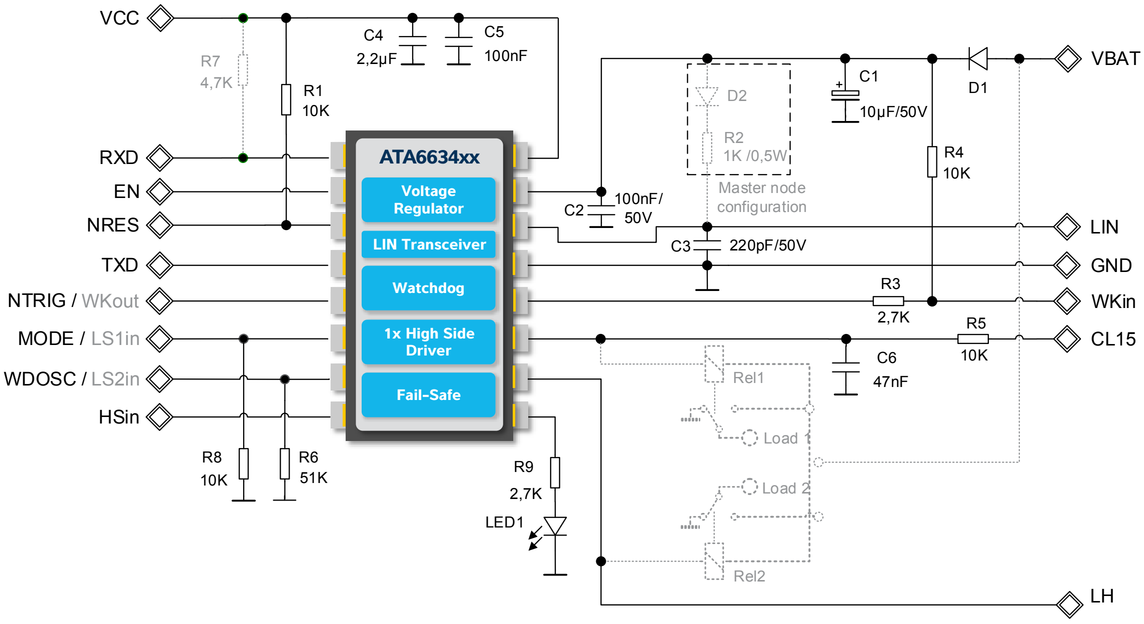


Figure 6. Soldering option for the typical application with the ATA6634xx SBC (LIN transceiver, LDO, watchdog and 1x high-side driver)

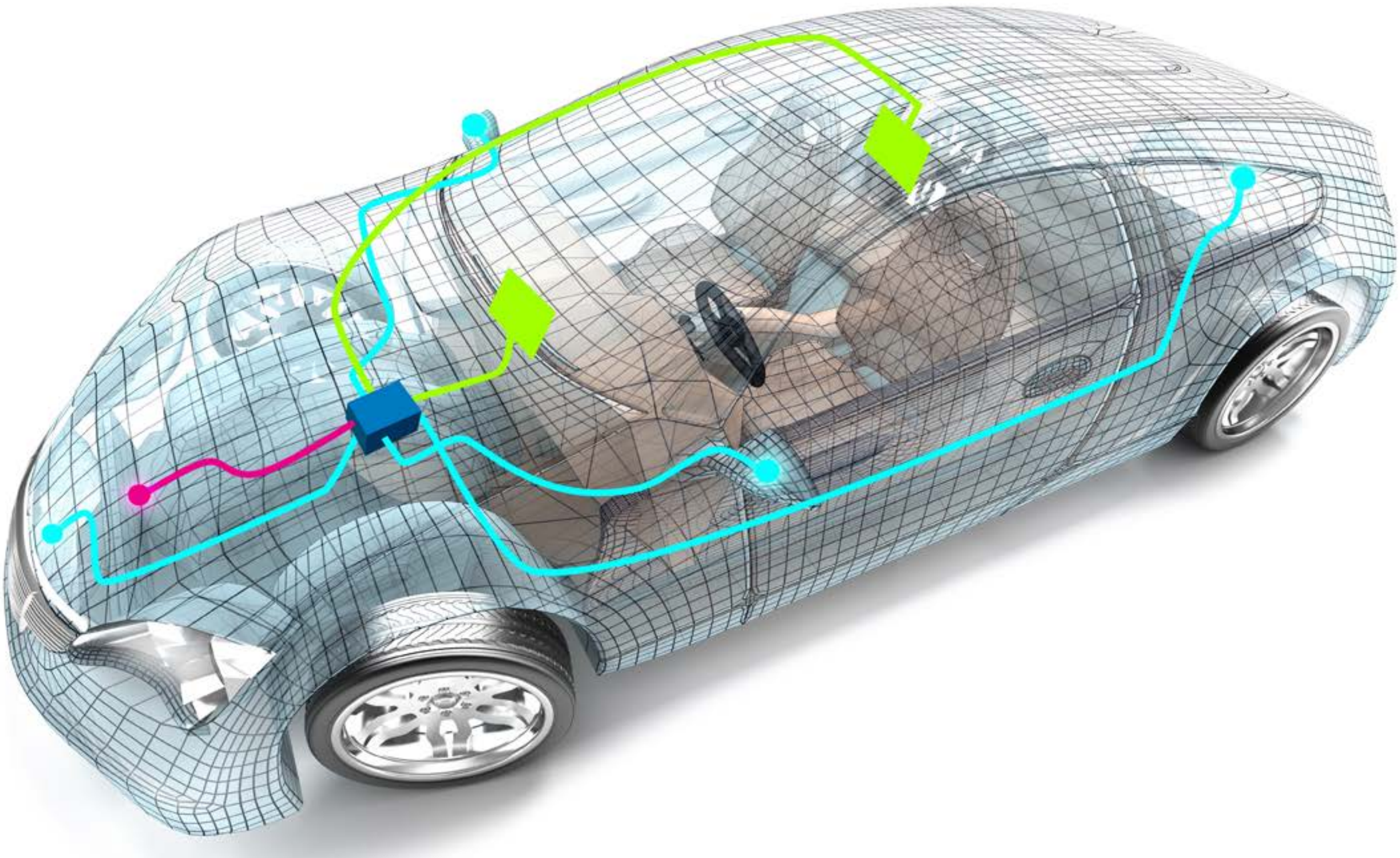
The new Atmel device family comes with various fail-safe features to ensure secure functioning of the application:

- The bus pin is short circuit and overtemperature protected vs. GND and battery
- TXD time-out timer to prevent the bus line from being driven permanently in the dominant state
- Wake-up source recognition between LIN, WKin or CL15
- VCC undervoltage detection with open drain reset output (NRES, 4ms reset time)
- Voltage regulator is short circuit and overtemperature protected
- Interference and damage protection according to ISO7637
- The watchdog always generates Resets when the WDOSC pin is short circuited or open
- Limp Home output for indication or enabling an external safety circuitry in case of watchdog failures

Summary

The new modular ATA663xxx LIN device family gives users the ability to use one board for many different applications with the ability to use every part from this family. So a standalone LIN transceiver, a voltage regulator, and a LIN SBC with LIN transceiver and voltage regulator can be realized in a small DFN8 package with a size of just 3x3mm. Additionally, as an extension of the 8-pin LIN SBC, the ATA6633xx device in the small DFN16 3x5.5mm package with its two additional relay drivers, a high- voltage Wake input and a high-side driver represents another part of the family. And finally, the ATA6634xx device with its watchdog, two high-voltage Wake pins and a high-side driver complete the modular device family.

With all these devices, this flexibility to use only one board as a platform for many different applications gives users a significant cost advantage in the highly competitive LIN market.



Ethernet AVB for Automotive Streaming Applications

Pradeep Yale, Tim Grai

Advanced driver-assistance systems using cameras, infotainment systems, rear-seat entertainment systems and mobile phones have dramatically increased the availability of audio/video (AV) content in vehicles. Ethernet is emerging as the automotive network of choice to cater to these bandwidth-intensive and latency-sensitive applications. Standard Ethernet protocols cannot ensure timely delivery of AV content.

The audio-video-bridge (AVB) collection of extensions to IEEE 802.1 specifications enable local Ethernet networks to stream time-synchronized, loss-sensitive data, including AV data. In an Ethernet network, the AVB extensions help differentiate AVB traffic from non-AVB and legacy traffic that can also flow through the network.

The extensions that define the AVB standard achieve this task by

- Reserving bandwidth for AVB data transfers, thus avoiding packet loss due to network congestion from talkers to listeners;
- Queuing and forwarding rules for AVB packets, thus avoiding packet bunching, and the use of intermediate switches to guarantee delivery of packets with a bounded latency from talkers to listeners;
- Offering time synchronization to a global clock, allowing all network nodes to precisely align their time bases to the network's master clock; and
- Including "presentation time" in every packet, which specifies when AV data in packet must be played.

Atmel's new SAMV71 ARM®-M7 core microcontrollers implement Ethernet AVB products. Atmel® SAMV71 microcontroller offers features to reduce software loading in implementing the Ethernet AVB stack.

This article summarizes the AVB standard and its use in streaming AV data over Ethernet. It also highlights SAMV71 features that facilitate Ethernet AVB implementation.

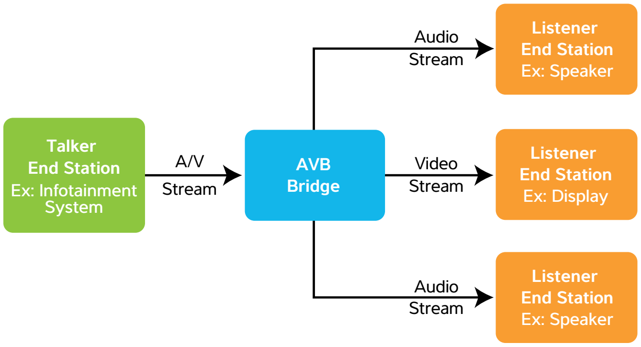


Figure 1. An Ethernet AVB network includes talker and listener end stations to stream audio and video data.

AVB Standards

The AVB extensions to the IEEE 802.1 standards are

- 802.1AS™ Generalized Precision Timing Protocol (gPTP), providing timing and synchronization for time-sensitive applications;
- 802.1Qat Stream-Reservation Protocol (SRP); and
- 802.1Qav Forwarding and Queuing for Time-Sensitive Streams (FQTSS) Protocol.

802.1AS

IEEE Standard 802.1AS-2011 specifies protocol and procedures for establishing and maintaining one time reference—a synchronized "wall clock"—for all the nodes in a local network. The gPTP protocol is based on IEEE1588 and synchronizes and "syntonizes" all network nodes to submicrosecond accuracy. Nodes are synchronized if their wall clocks show the same time. Nodes are syntonized if their clocks increase at the same rate.

The major functions of this protocol are to:

- Select the grand-master clock;
- Propagate the current time from the grand-master clock to all network end stations; and
- Correct for clock offset and clock drift by measuring path delays and frequency offsets in the clock.

Grand-Master-Clock Selection

- Any end station with clock-sourcing capability announces its ability to become a grand-master clock. This method uses the best-master-clock algorithm (BMCA) to select the grand master that all nodes will use when more than one clock source capable node exists in the network. The protocol also defines procedures to switch grand-master clocks.

Delay-Measurement Determination

This protocol defines procedures to determine the

- Time offset from the grand-master clock;
- Path delay between peers;
- Frequency offset from grand-master clock and peers; and
- Messages and their encapsulations to calculate the above delays.
  - Event messages are those whose time stamps must be captured when they are transmitted or received, and they include SYNC, DELAY_REQ, PDELAY, and PDELAY_RESPONSE.
  - Management messages are follow-up messages that may carry the time stamps of the event messages, and they include FOLLOW_UP, DELAY_RESPONSE, and PDELAY_RESPONSE_FOLLOWUP.

The grand-master clock periodically broadcasts the current time using the SYNC and FOLLOW_UP messages. PDELAY and PDELAY_RESPONSE messages determine peer capability, link delay and neighbor-clock-rate ratio (neighborRateRatio). Nodes at both ends of a link use these messages, regardless of whether they contain a master clock or a slave clock.

Step 1: Peer-Rate-Clock Determination

- The initiator schedules PDELAY message for transmission.
- Time Stamp t1 is captured as it passes from the media-access-control (MAC) layer to the physical (PHY) layer.
- Time stamp t2 is captured as it passes from the PHY layer to the MAC layer at the responder.
- The responder then sends PDELAY_RESPONSE PDELAY_RESPONSE_FOLLOWUP messages with time stamps of t2 and t3 to the initiator.

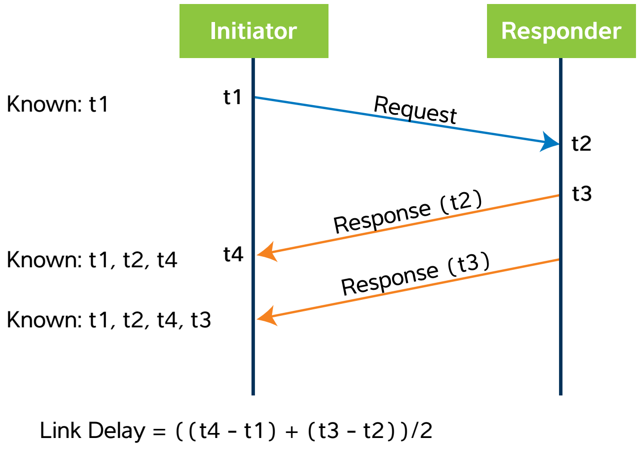


Figure 2. The peer-link-delay calculation does not require the clocks to be synchronized. If the link delay is fixed, regardless of the message type, and symmetric in message direction, the above equation applies.

Step 2: Grand-Master-Clock Offset

- The grand-master clock schedules a SYNC message.
- A slave time-stamps t2 when a SYNC message passes from the PHY layer to the MAC layer.
- The grand master schedules a FOLLOW_UP message with time stamp t1.

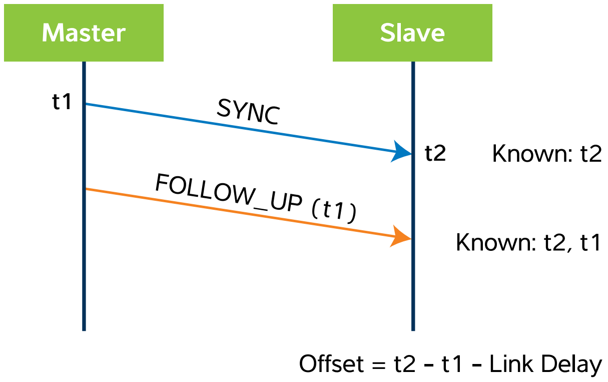


Figure 3. the slave corrects its clock using Offset = t2 – t1 – Link Delay.

This offset synchronizes the node with the grand-master clock. Periodic exchanges also enable the computation of the frequency ratio of the grand master relative to the local clock. Intermediate switches in the network adjust the correction field in FOLLOW_UP to account for switch-residency time and switch-measured upstream-path delay.

Computing syntonized time requires the use of the frequency ratio of the grand-master clock relative to the local clock, and correcting propagation-time measurement requires the use of the frequency ratio of the neighbor clock relative to the local clock.

The Atmel SAMV71 hardware time-stamp unit automatically detects and captures time stamps when the gPTP event messages crosses media-independent-interface (MII) layer. The gPTP messages can be transported over raw Ethernet in Internet Protocol Version 4 or 6 (IPv4 or IPv6). SAMV71 micro-controllers can automatically recognize 10 such encapsulations of gPTP event messages.

Thus, the Atmel SAMV71 hardware-recognition feature helps to accurately calculate clock offset and link delay with a minimal software load.

802.1Qat

The SRP uses other signaling protocols, including the Multiple MAC Registration Protocol (MMRP), Multiple VLAN (virtual-local-area-network) Registration Protocol (MVRP) and Multiple Stream Registration Protocol (MSRP), to dynamically establish bandwidth reservations for AV streams.

Talkers "advertise" streams and their characteristics. Listeners use these advertisements to determine which streams are available. Listeners request talkers to start or stop stream transmission. Talkers respond to these registrations and deregistration events.

Switches process these announcements from talker and listeners to:

- Register and prune streams path through network;
- Reserve bandwidth and prevent oversubscription of available bandwidth;
- Establish the forwarding rules for incoming packets;
- Establish the SRP domain; and
- Merge multiple listener declarations for the same stream.

The standards stipulate that AVB data can reserve only 75% of total available bandwidth. For example, in a 100Mbps link, the maximum AVB data is 75Mbps. Designers of automotive systems can preconfigure streams and provide for statically reserved bandwidth at system start-up. Hence, automotive designs do not need SRP, which in turn allows for a faster network start-up time.
SRP guarantees end-to-end bandwidth reservation for all streams and ensures that switches do not drop packets due to congestion on the LAN.

802.1Qav

This specification guarantees that time-sensitive AV streams will arrive at listeners within a bounded latency. This specification covers procedures for priority regenerations and the credit-based shaper (CBS) algorithm to shape traffic in accordance with stream reservations.

AVB-Traffic Classes

The priority-code-point (PCP) field of the VLAN tag in an Ethernet packet is encoded with the priority value of the frame. Each frame is mapped to a traffic class using this priority and a port's traffic-class table. The frames separate into queues, each corresponding to a traffic class. The switch at the SRP domain boundary remaps traffic entering an SRP domain to a lower priority. There is no means of mapping these priority values back to their original values as frames exit from an SRP domain.

The AVB standard can support as many as eight traffic classes, designated A through H. SR Class A has the highest priority in the network. Typically, nodes support at least Class A and Class B traffic. AVB uses traffic classes to determine the quality of service (QoS) a stream receives. Class A traffic QoS stipulates, a class-measurement interval of 125 µsec, an upper bound for latency of 2msec through seven hops and a buffering time of 2msec for data.

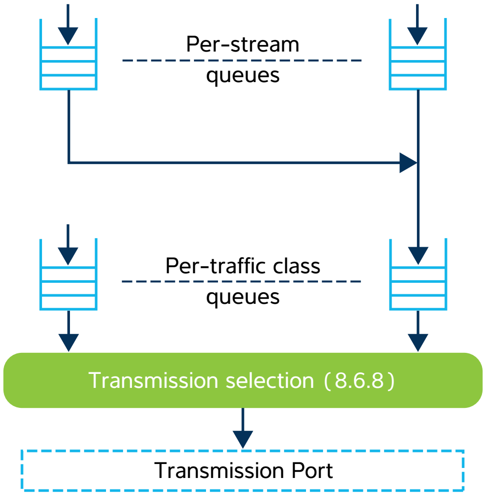


Figure 4. In the talker-queuing model, each frame is mapped to a traffic class using this priority and a port's traffic-class table[2]

Class B traffic QoS stipulates a class-measurement interval of 250 µsec, an upper bound for latency of 50msec through seven hops and a buffering time of 50msec for data. The CBS shaper shapes the frames in per-traffic-class queues.

SAMV71 has features that help manage receiver and transmitter data and supports as many as three priority queues for transmission. Hence, the two priority queues can have at least two SR classes, while the default queue can send "best-effort class" non-AVB data.

SAMV71 supports as many as three queues to route received data, can be configured to reject all frames except VLAN tagged frames, and has "screeners" that act as filters and route data to specific queues. The screeners allow the SAMV71 to filter as many as three 16-bit fields. It routes a frame that passes the filters to a specific queue and can route AVB data to one queue and non-AVB data to another queue.

The screeners can match a combination of any of the following fields:

- Enabled VLAN priority;
- Ethernet type; and
- Three 16-bit compare fields specifying an offset, mask and value, in which a 16-bit word at bit offset from frame start is masked and compared against value.

Credit Based Shaper (CBS)

All talker end stations must shape outbound frames to reduce bursting and bunching. AVB's CBS suits this purpose.

Each queue that supports the operation of the CBS algorithm includes the following parameters:

- The **portTransmitRate** parameter is the link bandwidth, or the transmission rate in bits per second.
- The **idleSlope** parameter is the bandwidth in bits per second that this queue is currently reserving and is the rate of change of credit in bits per second when the value of credit is increasing. This rate cannot exceed the portTransmitRate.
- The **sendSlope** parameter is the rate of change of credit in bits per second when the value of credit is decreasing: sendSlope=portTransmitRate–idleSlope;
- The **hiCredit** parameter is the maximum value of credit that the queue has accumulated.
- The **loCredit** parameter is the minimum value of credit of a queue.

The CBS traffic algorithm performs the following functions:

- Transmits frames in a queue only if the frame has a non-negative credit;
- Initializes each queue's credit to zero;
- Decreases credit at the rate of sendSlope when a frame from the queue is transmitted;
- Increases credit at the rate of idleSlope on completion of transmission;
- Continues to increase credit at the rate of idleSlope when a queued frame waits for the port to become available;
- Queues no more frames if the frames are too small to consume all of the available credit and reduces credit to zero on completion of the transmission; and
- Completely transmits all frames, regardless of value, once a transmission has started.

SAMV71 microcontrollers support traffic shaping in hardware, greatly reducing the load on software and allows traffic shaping on the two highest-priority queues, thus supporting two traffic classes.

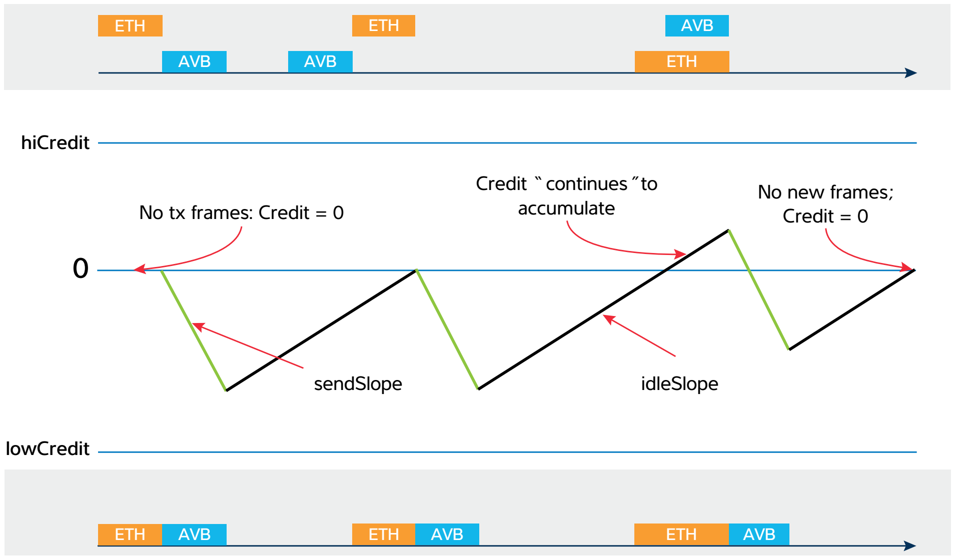


Figure 5. CBS ensures that traffic classes honor but do not exceed bandwidth guarantees on each network link.

Transporting AV over the AVB network

The AVB Transport Protocol (AVBTP) provides a high-level encapsulation that defines the formatting of AV data in a frame. AVBTP encapsulates the frames containing AV data into Ethernet frames in which the EtherType field is 0X22f0 for transportation across the network. The IEEE 1722.1-2013 standard allows AVB discovery, enumeration, connection management and control (AVDECC) of devices using IEEE 1722-2011.

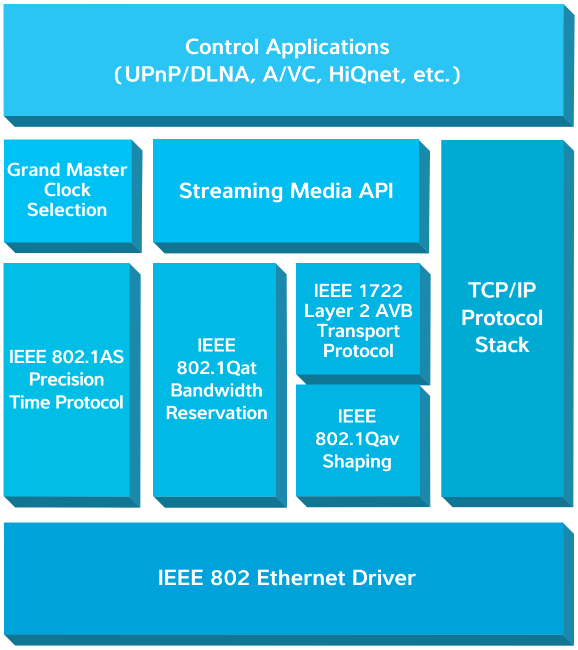

Control Applications
(UPnP/DLNA, A/VC, HiQnet, etc.)
Grand Master Clock Selection
Streaming Media API
TCP/IP Protocol Stack
IEEE 802.1AS Precision Time Protocol
IEEE 802.1Qat Bandwidth Reservation
IEEE 1722 Layer 2 AVB Transport Protocol
IEEE 802.1Qav Shaping
IEEE 802 Ethernet Driver

Figure 6. In the Ethernet AVB Protocol stack, AVBTP is transparent to its data payload because it defines its own header.[3]

The AVBTP header includes a subtype field that specifies the streaming protocol. Its value can range from 0x00 to 0x7F. The 0x00 IEC 61883/IIDC streaming protocol can transmit a variety of media formats, including raw and compressed AV formats. Formats based on IEC 61883 include:

- IEC 61883 – 2 SD DVCR
- IEC 61883 – 4 MPEG2-TS Compressed video.
- IEC 61883 – 6 Uncompressed Audio
- IEC 61883 – 7 Satellite TV MPEG.

The 64-bit 0x7F proprietary/experimental field can transmit any digital data. The stream-ID field uniquely identifies streams by all nodes. It comprises:

- A 48-bit MAC address associated with the talker and
- A 16-bit unsigned integer value, or unique ID, to distinguish among multiple streams from the talker.

The 802.1AS presentation-time field finds use when the data must be played. Talkers sample the 802.1AS clock relevant for an AV data block and then add the worst-case transport delay to the sample time to get a presentation time, which is inserted into the AVBTP packet. This presentation time is always for the first sample in the packet. Subsequent samples are played at media-clock frequencies. The presentation-time field can synchronously reproduce media for multiple listeners, accounting for variable latencies and path delays. This scenario could occur, for example, when front and rear speakers in a vehicle are playing audio or when a movie is transmitting both audio and video streams.

A talker samples analog AV media at a standardized frequency, or media clock, to produce raw digital samples, such as 44.1 or 48kHz audio. The application then packs these samples into an AVBTP frame. The number of samples in an AVBTP frame depends on the media-clock frequency.

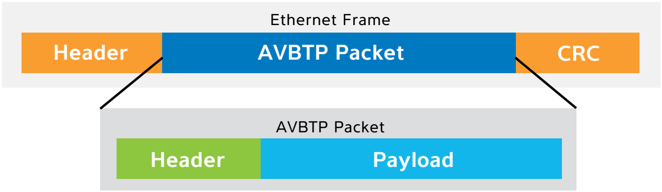


Figure 7. The AVBTP provides a high-level encapsulation that defines the formatting of AV data in a frame.

Porting Media Clocks

The Ethernet AVB network supports multiple media formats with different media clocks. For example, it can support a vehicle's cameras and center display with media clocks that correspond to video data and support amplifiers and speakers that connect to the same network with media clocks that correspond to audio data. The AVB standards do not cover media-clock recovery. When an AVB talker sends media to an AVB listener, a mechanism must be in place to guarantee that the media clock is operating at the same frequency between the endpoints of the same stream.

Use of Clock Streams and Cross-Time Stamping

Each sampling frequency requires a clock stream to distribute media-clock time stamps to all network nodes. Alternatively, the AVBTP time-stamp field in the data packets can embed the time stamp. Network-bandwidth limitations make it impractical to send time stamps at the media sampling rate. Instead, times stamps correspond to every nth sample to minimize network-bandwidth requirement.

Listeners compare the received time stamps with their internal 802.1AS wall clocks. The rate at which the time stamps match the wall clock re-creates a scaled-down (in frequency) media clock. Listeners generally use a phase-locked loop (PLL) to generate a media clock. This media clock triggers processing on the media sample. The scaled-down media clock acts as the reference and correction signal to syntonize the PLL's output with the talker.

The clock stream should supply time stamps at sufficient frequency to allow interpolation at the listener to reconstruct the media clock. This interpolation can account for lost packets of the media-clock stream and changes in global-clock frequency.

The SAMV71 can generate an interrupt when the internal 802.1AS timer count value matches a programmable comparison value. The microcontroller can write this media-clock time stamp to this compare register. This timer-compare interrupt can use the event system to trigger a pulse-width-modulated (PWM)-timer peripheral without any software intervention. The PWM-timer peripheral in turn toggles an output pin for every compare event. Media-clock time stamps received in a stream transform into square outputs at the same frequency. The SAMV71 can thus use this clock to correct an external PLL output to re-create the media clock with minimal software intervention from time stamps.

Buffering in AVB Networks

Talkers advertise the worst-case latency that a stream can encounter in its path from a talker to a listener. The latency does not increase during the life of the reservation. If some event occurs that would increase the latency beyond the original guarantee, the system reports a failure.

Before sending the presentation time, the talker adds an offset to it that should account for the maximum delay, or latency, through the network. The actual delay to each

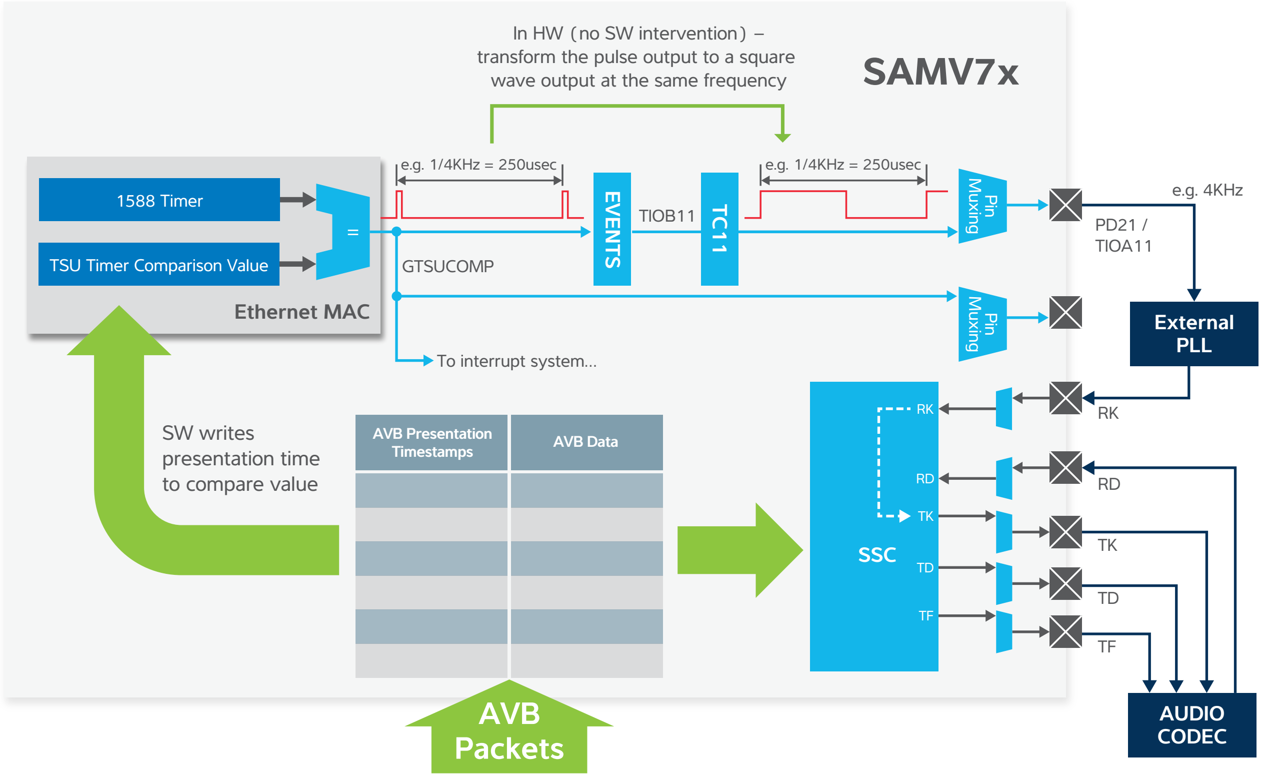


Figure 8. SAMV71 hardware supports reconstructing the media clock from the AVBTP timestamps.

listener can vary, depending on the number of hops on the network path to the listener. Hence, the buffer size at a listener is dynamic and depends on the latency. The listener can use this information to decide whether the latency is too large for an acceptable presentation of the stream.

Buffer-Size Calculation

Consider that a system designer calculates the worst-case delay from a talker to Listener A as 49msec through seven hops. The designer would then set the delay time, or offset, at 50msec. However, Listener B is only one hop away and has a delay of 7msec. A listener that receives packets with lower latency continues to buffer until the listener with the worst-case latency receives data from the same stream. Hence, Listener B buffers data for 43msec, whereas Listener A buffers data only for 1msec.

Consider a five-channel, 16-bit Class B audio-stream data sample at 48kHz frequency. The buffer would require a sampling frequency of 48kHz, a class-measurement interval of 250μsec, a 2-byte sample and five channels. Thus, it would require 12 audio samples per Ethernet packet. Listener A, at 1msec, would require four 250μsec Ethernet frames. Listener B, at 50msec would require 200 250μsec frames.

In mono audio, Listener A would require five channels at 2 bytes per channel; 12 audio samples per Ethernet frame, four Ethernet frames and a 480-byte buffer. Listener B would require five channels at 2 bytes per channel, 12 samples per Ethernet Frame, 200 Ethernet frames and a 24,000-byte buffer. These specs are critical in automotive networks in which the end devices may have limited buffer space.

Typically, an automotive system may have multiple streams, with each stream having more than one channel in it. The buffer size increases for every additional channel in a stream and for every additional stream. The buffer sizes, hence, depend highly on the configuration.

The presentation time in each AVBTP frame also requires buffering. The buffer size for holding presentation time depends on the number of streams supported and the worst-case latency time of the stream.

Automotive requirements

Automotive Ethernet networks are typically closed networks where many aspects of the system can be pre-configured as part of the system definition. For example, the BCMA algorithm fixes the best clock master at the network-definition phase with dynamic selection and without the need for a master-clock algorithm. Further with the 802.1Qat SRP, all streams, their contents and their characteristics are known at system definition, and no new streams are dynamically created or destroyed.

The bandwidth reservation to ensure proper reservation of data is also known at the system definition phase. Hence, switches, talkers and listeners can have their configurations loaded at system start-up from preconfigured tables rather than requiring dynamic negotiations.

Low latency is often not extremely critical, but delivery is always critical. Automotive networks are small and have only a few nodes between a talker and a listener. It is more important that a system does not drop packets due to congestion.

Conclusion

Vehicles increasingly require the transmission of a high volume of time-sensitive AV content. Ethernet is a widely adopted standard, and AVB extensions enable it to deliver AV to distributed devices on the network with microsecond accuracies or better. In addition, AVB standardization has resulted in the development of interoperable end-devices that can efficiently handle A/V traffic.

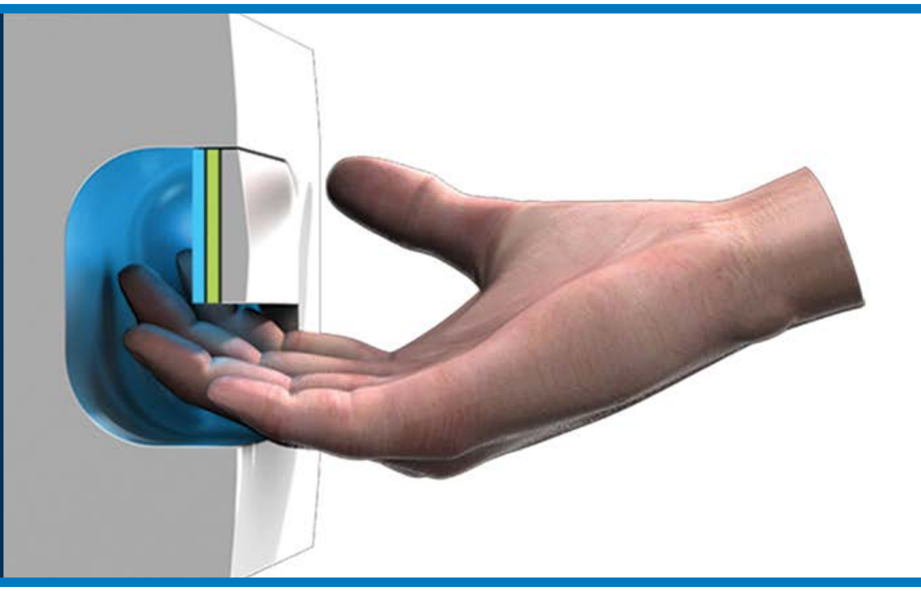
References

1. http://www.ieee802.org/1/files/public/docs2009/avb-rboatright-p1722-explained-0903.pdf

2. http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf

3. http://www.embedded.com/design/connectivity/4008284/3/Understanding-IEEE-s-new-audio-video-bridging-standards

Capacitive Proximity-Sensor Shielding



Darius Rydahl

Introduction

A typical unshielded capacitive proximity sensor can detect an approaching finger or hand from almost any orientation—top, bottom, left or right. In some situations, this "360-degree" field of detection is undesirable, and the sensor application may require specific localization with regard to the region of detection. For example, it may need to limit detection of a finger to only one region or one side of the sensor. To restrict this type of detection, the sensor requires a shield. This is accomplished by placing a secondary electrode, the shield, beneath the primary sensing electrode, the sensor. Shield termination is important because it determines how well the shield will perform in the end application.

Electric-Field Generation and Shielding Basics

In essence, the copper track on a printed-circuit board (PCB) that forms the proximity sensor is simply one plate of a virtual capacitor that comprises a dielectric, or free space air gap, and an earth return to ground.

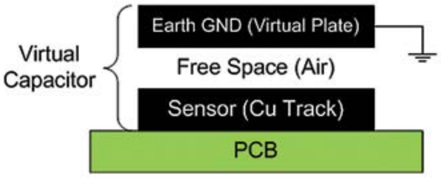


Figure 1. Touch-Sensor Virtual Capacitor

An electric field is generated when charge is transferred into the proximity sensor during the acquisition phase of sensor measurement. If the sensor is unshielded, the resulting electric field radiates outward from both sides of the sensor. The field takes the path of least resistance to reach earth ground through free space (air).

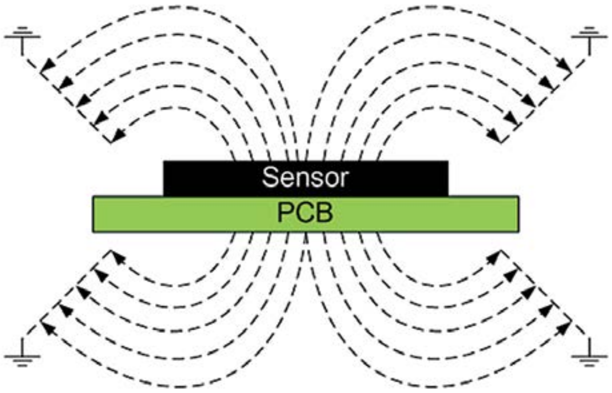


Figure 2. Electric Field of an Unshielded Sensor

The approach of a finger or hand to the sensor changes the capacitive load the sensor sees and provides a more direct path to ground. The closer the finger is to the sensor, the greater the effective capacitance, which in turn indicates closer proximity between the sensor and the finger. This change in capacitance determines the strength and intensity of sensor detection.

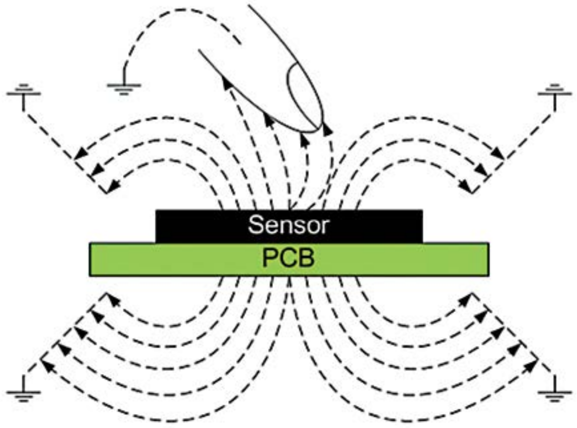


Figure 3. Electric Field of an Unshielded Sensor in Detection

The finger in the figure above could just as easily approach the sensor from the bottom as it does from the top because the electric field radiates outward from both sides of the sensor. In most instances, this additional region of detection is not an issue. By default, sensor detection can occur in only one direction due to sensor placement within the application. In these cases, only one side of the sensor is accessible to the outside world. In other instances, the sensor may be exposed on both sides; the designer may not care about the expanded region of detection. This feature can make the application more robust in detection.

Consider a scenario in which sensor activation from the rear or bottom side would be undesirable. The application might dictate this situation to isolate the sensor from other sensitive circuitry and from ground or to control the direction from which detection occurs. In this situation, designers must place a shield beneath the sensor as Figure 4 shows.

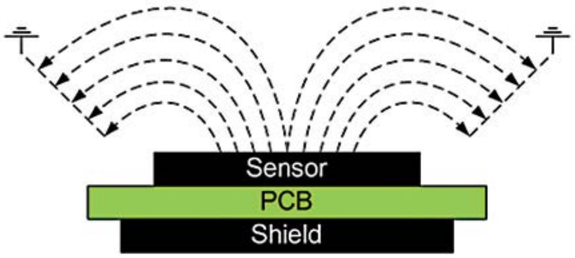


Figure 4. Electric Field of a Shielded Sensor Not in Detection

In this configuration, the electric field radiates only from the top side of the board. The shield absorbs the field that would normally radiate from the bottom side of the sensor. With the shield in place, the sensor can detect in only one direction: from the sensor side.

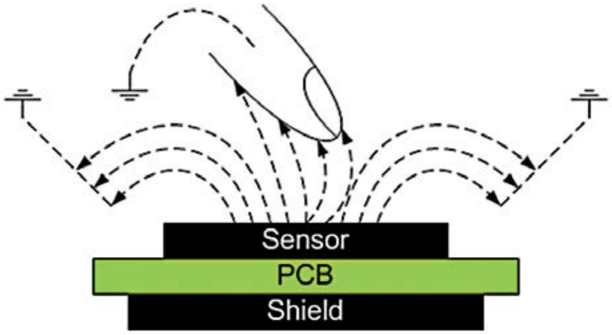


Figure 5. Electric Field of a Shielded Sensor in Detection

Terminating the Shield

When terminating the shield, the designer has three options:

- Leave the shield floating
- Connect the shield to ground
- Modulate the shield with a voltage potential

Let´s look at these options in further detail.

Floating Shield

A floating shield is actually no shield at all. If the shield electrode remains unconnected, it simply creates the second plate of the sensor/PCB dielectric capacitor. By default, this plate allows another path to earth ground through free space for the electric field. When charge is added to the sensor during the acquisition phase, the electric field will again radiate outward from the top and bottom sides of the PCB, just as it does with an unshielded sensor. The sensor detects the approaching finger from either side of the board.

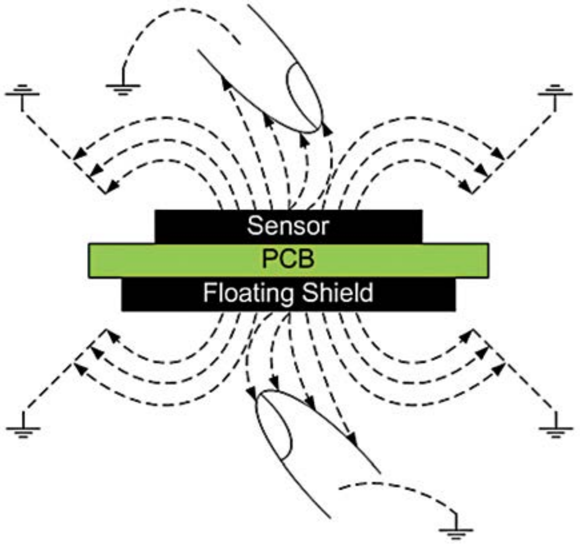


Figure 6. Sensor: Floating Shield in Detection

Grounded Shield

A grounded-shield electrode makes a shield that is almost too good. Connecting the shield electrode directly to the circuit ground provides the radiated electric field a more direct path to ground than that of the field radiated through free space. The grounded shield attenuates the electric field on the top side of the board and acts as a shunt to ground for the field on the bottom side. Bottom-side detection is not possible in this instance. Conversely, detection is still possible from the top side of the sensor, but the electric field strength is greatly reduced, which in turn reduces the sensitivity and overall detection range of the sensor. This reduction in range may be acceptable for a standard touch sensor but is probably undesirable for a proximity-sensing application.

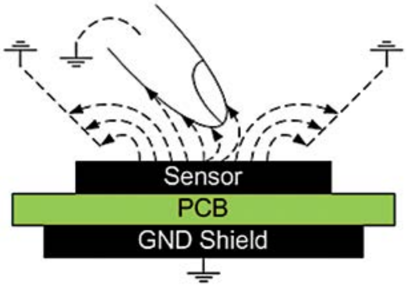


Figure 7. Sensor: Grounded Shield in Detection

Driven Shield

A driven shield—one that is driven by some voltage potential—provides the best shielding of the three configurations. Ideally, this voltage should be identical in amplitude and phase to that of the driving source on the sensor. Driving the shield in this manner reflects the radiated electric field that would normally exit through the bottom side of the board back toward the top side. Reflection of the field results in an increase in sensitivity and the overall detection range of the sensor.

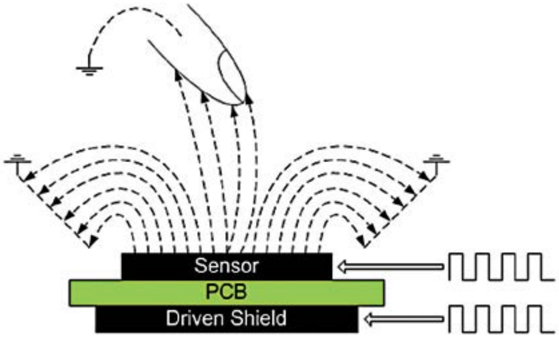


Figure 8. Sensor: Driven Shield in Detection

Any mismatch between the sensor and the shield-driving sources will result in a decrease of sensitivity and detection range. Designers should take care to match the signals as closely as possible.

Shield Overview

Figure 9 shows a side-by-side comparison of the relative field strengths for the three sensor-shield configurations. The figure illustrates the attenuation effect that the grounded shield has on the electric field, followed by the nonshielding performance of the floating shield and the amplified electric field of the driven shield.

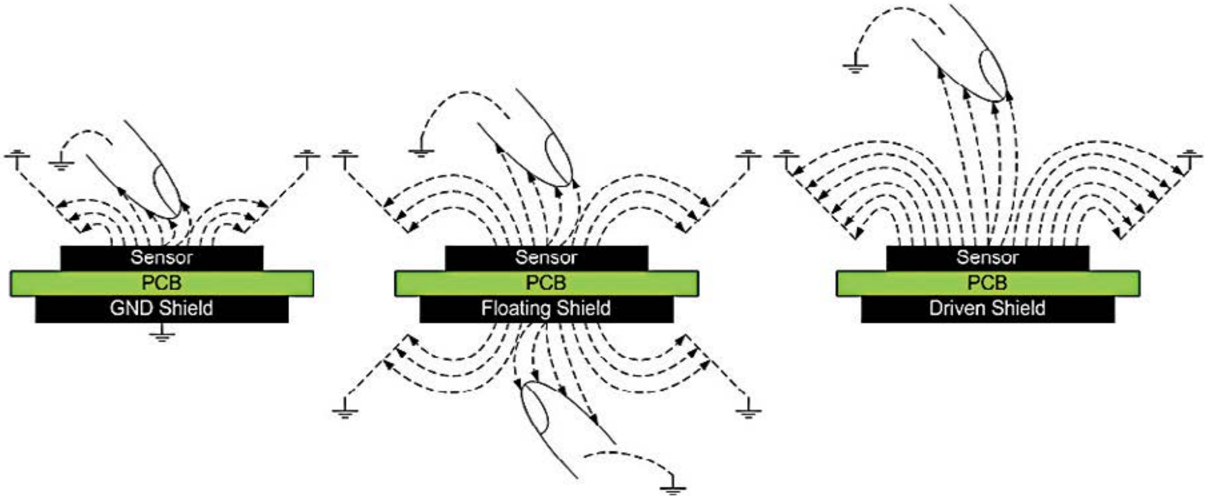


Figure 9. Shielded Sensor Comparison

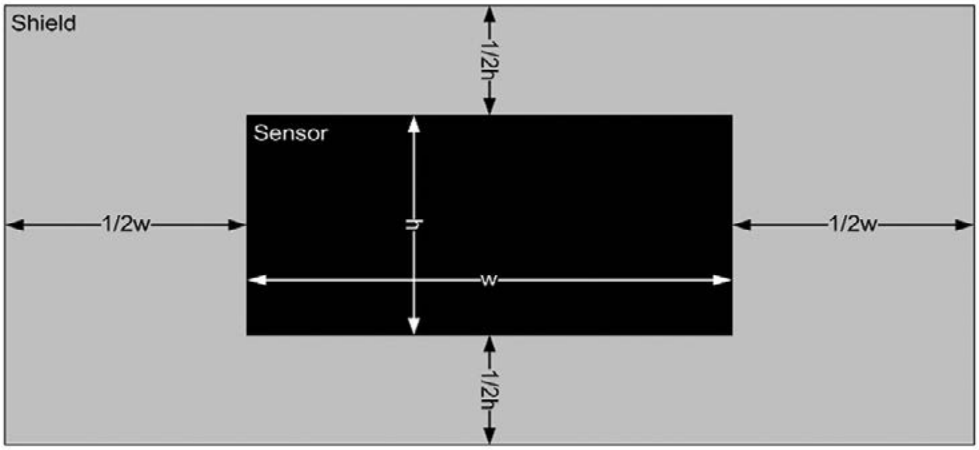


Figure 10. Shield Size and Geometry Recommendations

Shield Size and Geometry

To be effective, the shield should be larger than the sensor that it is shielding. If the shield is the same size as or smaller than the sensor, the electric field will radiate and wrap around the sensor, which will reduce the overall effectiveness of the shield. A good rule of thumb is to ensure that the shield extends beyond the perimeter of the sensor by one-half the width and one-half the height. Figure 10 illustrates this relationship.

Designers should also construct the shield as one solid plane, not hatched, which leaves holes at evenly spaced intervals throughout the shield. Tests have shown that a hatched shield reduces its overall performance.

Summary

Of the three sensor-shield configurations, the floating shield provides no shielding of the sensor whatsoever from the outside environment. It simply provides another path, similar to that of the unshielded sensor, for the electric field to reach earth ground. The grounded shield does a good job of shielding the sensor, but it suffers from a reduction in sensitivity and detection range because it provides a low-impedance path to ground through the shield plate. The driven shield, in contrast, does everything and more than the other two shields combined. It adequately shields the sensor from unwanted touch on one side and provides the added benefit of boosting the sensor sensitivity and detection range. Clearly, the driven shield should be the implementation of choice for a sensor that requires shielding from its operating environment.

Introducing Atmel | SMART ARM® Cortex®-M Core Automotive Microcontrollers

Tim Grai

The new Atmel | SMART SAMV7x and SAMDAx families of ARM® Cortex®-M core-based microcontrollers bring the benefits of industry-standard 32-bit processing performance, improved accuracy, increased power efficiency and higher levels of system integration to automotive applications. These new families leverage Atmel's 17-year history as an ARM-core licensee along with more than two decades of experience with 8-bit embedded-flash microcontrollers to create powerful systems for tomorrow's demanding automotive networking, touch interface and connectivity applications. The new families combine the best elements from this extensive experience (Figure 1).

For real-time embedded automotive applications, a powerful CPU core is not enough; the other elements of the device architecture must empower the core, and this empowerment requires the use of powerful peripherals that can autonomously perform functions with little CPU interaction. System architects must also include features that allow efficient—and, in many cases, deterministic—cooperation among the peripherals and the core. Such features include the event system, a feature that Atmel borrows from the AVR® XMEGA® family, which allows peripherals to communicate without using any CPU or bus resources. The new Atmel families also feature ease of use, accessible tech support and a strong tool offering.

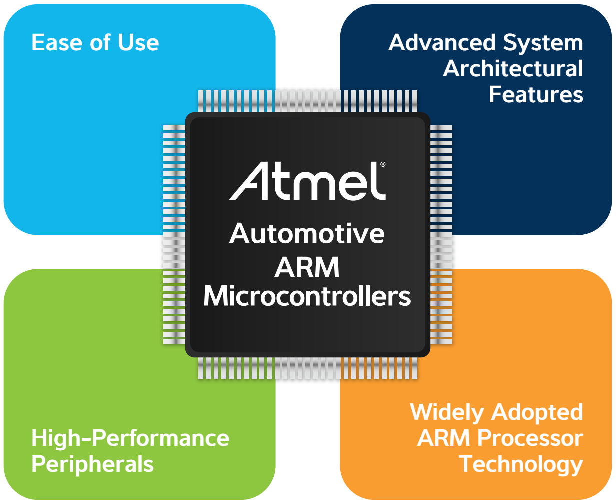

Ease of Use
Advanced System Architectural Features
Atmel
Automotive ARM Microcontrollers
High-Performance Peripherals
Widely Adopted ARM Processor Technology

Figure 1. The new automotive ARM core-based microcontrollers are part of Atmel's expanding portfolio of microcontrollers and related products that address the emerging trends in the automotive industry.

Industry Trends

Fuel Efficiency: Improving fuel efficiency is a priority in the automotive industry. "Efficiency" refers not only to conserving fuel in gas-fueled cars but also to conserving battery charge in electric vehicles. To achieve these goals, designers are networking vehicles' microcontrollers to make cars "smarter." Designers achieve this goal by implementing vehicles' ability to share sensor data and other information, thus maintaining or even reducing the power budget. These new car designs are also seeing the continued electrification of pumps and other mechanical loads to allow the selective shutdown of loads when the vehicle does not require them. For instance, a vehicle can use electric-motor-driven water pumps that turn off when the vehicle does not need continuous flow rather than belt-driven pumps which drain precious energy even when flow is not needed.

Connectivity, Safety and Security: The previously closed network of computers that compose a car's electrical system will become a more open system as cars of the future connect to the Internet and to the environment around them: the road and other cars. This trend includes the use of an advanced driver-awareness system (ADAS), which will combine onboard camera and sensor information with information the vehicle's electronics gather from the road and other cars to alert drivers to potential hazards. A set of safety and security challenges come with that connectivity; as such, the entire vehicle will require cryptologic technology.

Bringing the Consumer Experience to the Car: Drivers and passengers will increasingly demand the same audio and entertainment experience in the car that they enjoy with their consumer-electronics devices. This feature will greatly enhance the human interface, the most outwardly visible portion of the audio and entertainment experience.

ARM-Core Advantages

Each of Atmel's new automotive-microcontroller families uses a processor from the ARM Cortex-M family. ARM Cortex-M processor family members are upwardly binary compatible, allowing for software reuse and easy migration as performance needs increase, and allowing customers to make platform decisions for new products on a processor-core level. Using industry-standard ARM processors also provides customers with easy access to a range of expertise, support, information and tools. The use of industry-standard processor cores allows Atmel to focus on creating superior microcontroller systems, using its experience to bring the right mix of peripherals and system architectural features to demanding automotive applications.

The 32-bit ARM Cortex-M processors have 32-bit-wide internal registers; arithmetic and logical operations can operate on 32-bit-wide operands. The 32-bit ARM Cortex-M processors provide substantially better computational efficiency on a CPU-clock-cycle basis than do 8- and 16-bit processors. This computational efficiency is necessary to support the increasing complexity of automotive algorithms. For example, a generic 32-bit multiply/accumulate requires four multiplications and four additions on a 16-bit processor versus only one cycle on a 32-bit processor.

Using the 32-bit ARM Cortex-M core does not necessarily mean that "code bloat" will accompany the transition from 8- and 16-bit applications to 32-bit machines because the ARM processors use a high-density instruction set focusing on achieving more per byte of flash than 8- and 16-bit architectures can achieve.

The Atmel | SMART SAMV7x products use the higher-end Cortex-M7 processor, which integrates a floating-point unit (FPU), providing computational efficiency and simplifying application development. The FPU eases the implementation of complex mathematical algorithms; for example, it does not need to handle scaling variables. The wide dynamic range of floating-point numbers, especially in the supported double-precision format, maintains the highest precision. These features accelerate software development and achieve improved numerical results from the algorithms. A variety of applications, including many audio applications and those that require digital-signal-processing (DSP) computations, can benefit from the use of an FPU.

To address the need for increased system safety, the new Atmel devices integrate a memory-protection unit (MPU) that monitors and controls accesses to a number of configurable regions within the memory map. Designers can dynamically assign access-permission rules for various application tasks during runtime. With this mechanism, the design can prevent an application task from corrupting memory space that other tasks and the operating-system kernel are using.

To enable safe and secure flash updates through a boot loader, the Cortex-M processors supports vector-table relocation.

Additional features in the ARM Cortex-M processors enable efficient real-time operation. For example, the Cortex-M0+ processor in the Atmel | SMART SAMDAx microcontrollers supports a separate I/O-port interface that allows single-cycle access to I/O-port operations. Single-cycle I/O access is important in many real-time applications for achieving deterministic operation. Furthermore, many customers deploy bit banging and other schemes in which fast and predictable latency-pin access is vital. Because the I/O-port interface is part of the system's memory map, customers can access the I/O-port register on this interface in C, but it does not require C-language-extension features, such as special data types. Because the processor can concurrently access both the separate I/O-port interface and other memories, it can fetch the next instructions while accessing the I/Os. Single-cycle I/O accesses can thus continue for as long as necessary.

All these processor features and capabilities are of no use unless designers can efficiently and quickly debug their software to get an application up and running, and the ARM Cortex-M processors include extensive debugging features to achieve that goal. They implement a serial-wire-debug (SWD) connection that requires only two pins to access debug functions, thereby making more pins available for application functions.

Even the lower-end products provide trace capability. For example, the Cortex-M0+ processor in the SAMDAx supports a microtrace buffer (MTB), which provides simple instruction-trace capability. The programmer allocates a small part of the system SRAM as a trace buffer, and the MTB stores instruction-flow information to the reserved SRAM as a circular buffer. After the processor stops—when it hits a breakpoint, for example—the debugger can then retrieve the trace information and subsequently reconstruct the recent execution history. The MTB can also support one-shot triggering. The higher-end processor in the SAMV7x provide trace functions through the embedded trace macrocell (ETM), which includes the Coresight-embedded trace buffer and trace-port-interface unit.

Automotive Peripherals

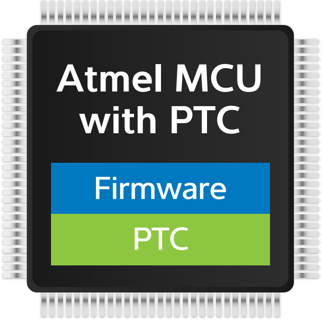
Atmel devices include a variety of state-of-the-art peripherals to meet the demanding functional needs of automotive electronic-control modules and ensure reliable operation across the entire automotive temperature range in compliance with the AECQ100 specification. For example, they include multiple timer channels, each with a variety of clock sources and a rich feature set, including counter, capture, up/down counter and pulse-width modulation (PWM). They also support multiple serial-communication interfaces, including a two-wire interface (TWI) for I^{2}C, master or slave serial-peripheral interface (SPI), UART-based protocols and local-interconnect-network (LIN).

The SAMDAx products implement these serial functions through the use of the innovative SERCOM peripheral (Figure 2). The primary benefit of the SERCOM module is that it enables designers to configure each device with four to six SERCOM instances to fit various applications' needs. For example, an application can have two I2C channels and four UART channels or three SPI channels and and one UART channel. To simplify circuit-board design, designers can choose the SERCOM module with the pin options that best fit the application's routing requirements—to avoid long signal paths, for example.

The devices also include an analog-to-digital converter (ADC) that converts from multiple input channels with 12-bit resolution, supporting differential- and single-ended measurements, with a set of reference voltages. The ADC includes hardware support for oversampling and digital averaging that can enhance resolution to as much as 16 bits. An analog comparator features selectable input from multiple input channels, and the comparator's output can generate an interrupt or find use in the event system.

USB functions support device or embedded-host modes, with an integrated USB physical layer and the option to run the USB using the internal RC oscillator, eliminating the need for and expense of an external oscillator. The devices also include a digital-to-analog converter (DAC) and specialized peripherals, such as a peripheral touch controller (PTC), CAN FD (controller-area network with flexible data), a Gigabit Ethernet media-access controller (GMAC), Media LB, an image-sensor interface and security.

The PTC is among the most innovative new peripherals available on Atmel's lower-end SAMDAx products (Figure 3). Designers can use it, along with Touch Library firmware, to implement buttons, sliders, wheels and proximity sensing, and it supports as many as 256 channels in a matrix configuration; the number of available channels varies with the device pinout and the aquisition algorithm in use. The PTC supports both self-capacitance and mutual capacitance and can perform in both modes without the need for external components, resulting in a lower-cost design. With superb sensitivity, noise tolerance and self-calibration, the PTC requires no user tuning, resulting in faster time to market. The PTC's low power consumption enables capacitive-touch technology as a feasible replacement to mechanical buttons, even in applications that require minimal power consumption. For example, the PTC can perform a 0.25-second scan using less than 10μA of current and wake up the device on a touch event.



- The PTC autonomously runs data acquisition.
- The CPU can idle with the PTC is working.
- Compensation and oversampling occur automatically in the PTC.

Figure 3. The PTC is among the most innovative new peripherals available on SAMDAx products.

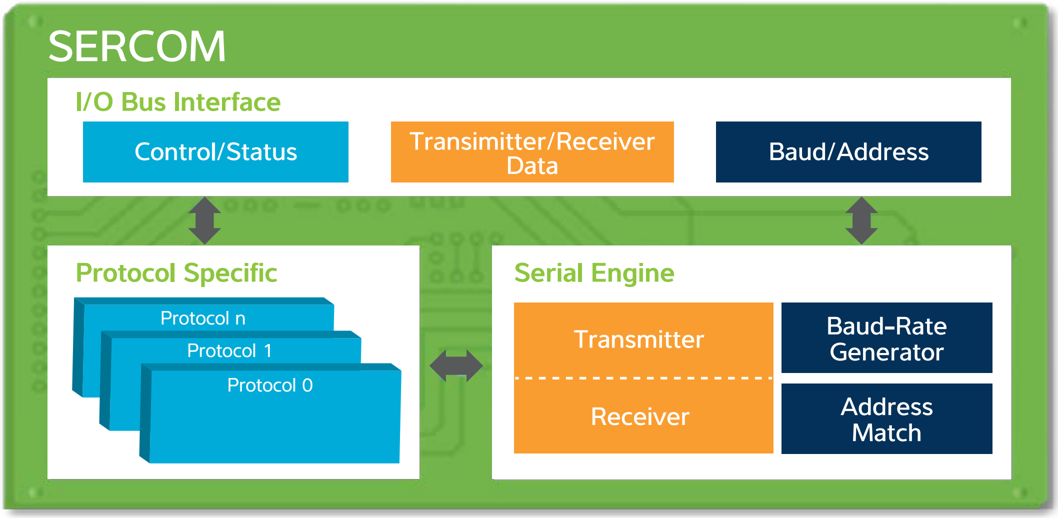


Figure 2. The SAMDAx products implement these serial functions through the use of the innovative SERCOM peripheral.

The most recent enhancement to the widely deployed CAN protocol, CAN FD, includes support for both bit rates higher than 1Mbps and a data payload as large as 64 bytes. These enhancements aim to extend the use of CAN in the face of ever-increasing network traffic. The CAN controller on SAMV7x products fully supports the CAN FD protocol and previous versions of CAN: CAN 2.0 A/B. Each CAN controller supports as many as 64 SRAM-based mailboxes, with as many as two available controllers, depending on product version.

Available on the SAMV71, the Ethernet GMAC efficiently interfaces with the system through a dedicated direct-memory-access (DMA) channel. To support emerging automotive Ethernet audio-video-bridging (AVB) applications, the GMAC includes support for IEEE1588 PTP frames, IEEE802.1AS time-stamping, priority queues, and IEEE802.1Qav credit-based traffic shaping in hardware.

The MediaLB peripheral on the SAMV7x provides efficient access to a three-wire MediaLB bus, through which the microcontroller can ultimately establish connection to a MOST (media-oriented systems transport) 25 or 50 network for in-vehicle audio-streaming applications.

The 12-bit ITU-R BT. 601/656 image-sensor interface on the SAMV7x products provides connectivity to a CMOS-type image sensor and provides for image capture in several formats.

The SAMV7x products include features to address emerging security needs, including a true random-number generator; 256-, 192- and 128-bit AES (Advanced Encryption Standard) support; and an integrity-check monitor supporting Secure Hash Algorithm (SHA) 1.

System-Architecture Features

An exceptional core and high-performance peripherals alone are not sufficient to address the needs of complex automotive real-time embedded systems. A coherent system architecture—one that manages common real-time events in embedded systems and minimizes processing latency—must connect the core and peripherals. Atmel's new automotive ARM Cortex-M processor-based microcontrollers include features to accomplish these tasks.

Multilayer Bus

A high-speed multilayer bus matrix is at the heart of the system architecture. The multilayer bus matrix connects the elements of the system—the core, the RAM and the flash memory, for example—through multiple master and multiple slave ports. This arrangement allows for concurrent accesses from masters to slaves. For example, the CPU can access the flash memory while transferring data from a peripheral to the SRAM.

Event System

The CPU's ability to manage peripherals can cause a major system bottleneck, especially as the number of peripherals and their operating frequencies increase. With high update and sampling rates across multiple serial interfaces, timer channels and analog inputs, interrupt overhead and data processing can consume a large percentage of the processor's available clock cycles. These problems affect CPU efficiency and worst-case interrupt latency; these problems can also introduce jitter.

The new automotive ARM core-based products use an event system that allows CPU-independent handling of interperipheral signaling through an internal communication fabric (Figure 4). In essence, the event system is a routing network directly between peripherals and independent of the traditional data paths, such as the internal buses. It can transfer events generated at one peripheral without any CPU involvement for use as trigger activities at another peripheral.

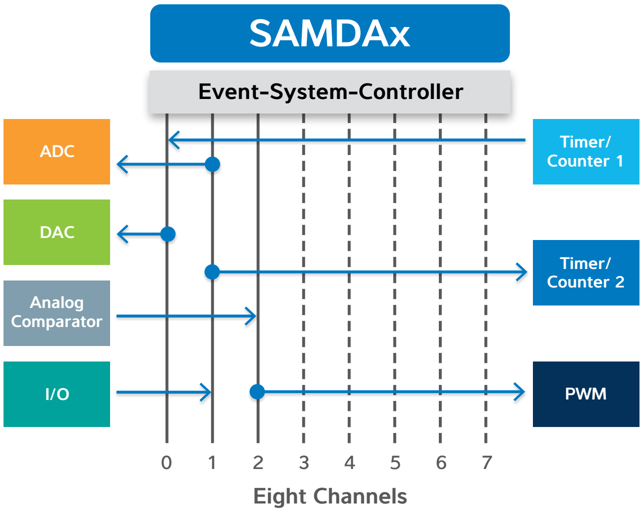


Figure 4. The new automotive ARM core-based products use an event system that allows CPU-independent handling of interperipheral signaling through an internal communication fabric that interconnects peripherals.

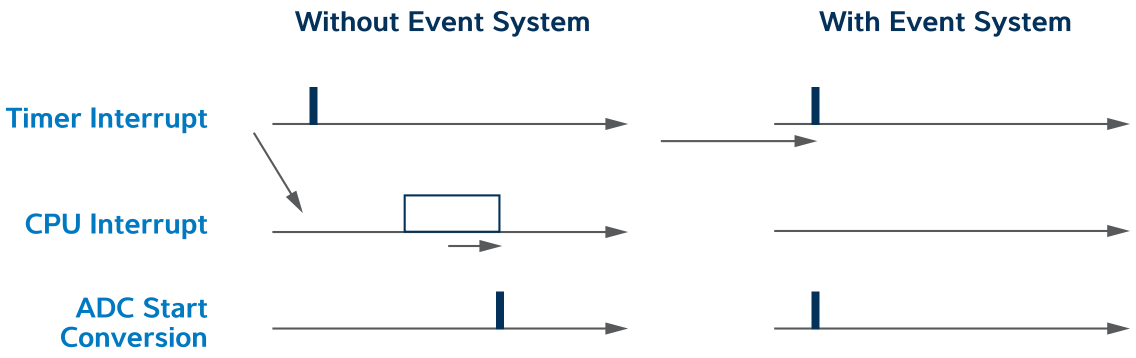


Figure 5. A timer-compare event generated at a timer peripheral can automatically trigger an ADC conversion without any action from the processor.

For example, a timer-compare event generated at a timer peripheral can automatically trigger an ADC conversion (Figure 5) without any action from the processor. To conserve power, the processor could remain in a low-power mode not executing any code during the entire sequence. Alternatively, the processor is free to execute application code during the sequence, without the need to divert cycles away from the application code to handle the ADC triggering.

In addition to eliminating CPU cycles for servicing peripherals, the event system is an independent and direct connection between peripherals, so it also guarantees a deterministic fixed latency response. This feature enables precise timing of activities without jitter; it provides, for example, constant jitter-free sampling of ADC and DAC channels. Using the event system also ensures that the system never loses events due to high CPU loading. In other words, the next event cannot happen before the interrupt for the current event executes. These characteristics make the event system a predictable and perfect fit for real-time embedded applications.

Designers typically use interrupts to handle data or actions for power-limited applications. For example, an interrupt would wake up the CPU to request a data transfer, an action or a computation. For example, to drive a motor at a steady pace would require a slight adjustment of the PWM at regular intervals to make sure the motor runs at the right revolutions-per-minute spec. An interrupt would wake the CPU on a regular basis, and the CPU would have to retrieve the current speed from the ADC, compare it with the offset and then adjust the PWM period before the CPU could go back to sleep. The event system automates all these tasks. A real-time-clock (RTC) event can wake the ADC and request a conversion. The ADC then sends an event to the analog comparator requesting a comparison between the current speed and the previously set threshold. In turn, the analog comparator would send an action to the PWM to increase or decrease the period. The new Atmel devices accomplish all these tasks without using the CPU.

Direct-Memory Access

The automotive ARM products also include a multichannel direct-memory access (DMA) controller to further reduce the processor load to service peripherals. DMA allows for transfers between peripherals and memories or among memories without CPU involvement. It performs these transfers over traditional data buses, but the DMA controller, rather than the processor, manages these transfers. Hardware or software automatically triggers these DMA transfers.

The higher-end SAMV7x products provide not only the multichannel central DMA controller but also a dedicated DMA controller on each of several of the high speed peripherals, including the GMAC, CAN, and USB.

Tightly Coupled Memory

Atmel's high-end SAMV7x microcontrollers include instruction and data caches and an innovative, flexible SRAM architecture. This architecture allows the partioning of SRAM between system memory and tightly coupled memory to suit various configurations under software control, according to the needs of the system. The partition allocated as system memory is shared with the entire system though a direct connection to the multi-layer bus matrix. On the other hand, the partition allocated as ″tightly coupled″ memory has a direct connection to both the data and instruction buses of the processor, allowing simultaneous access to data and memory with no wait states. The multilayer bus matrix allows the ability to access the tightly coupled memory partition at lower priority through a slave port. The no-wait-state nature of the tightly coupled memory makes it ideal for functions that must operate on data at high frequencies and with tight latency requirements, such as DSP functions operating on audio or video streams. Applications with a high percentage of such high-frequency, time-critical operations would configure the available SRAM with more tightly coupled memory and, therefore, less system memory than applications that have fewer of these types of operations.

Clocking Options

All the automotive ARM core devices include multiple clock options, ranging from external crystals to high-frequency, highly accurate internal RC oscillators to low-power internal RC oscillators. The RTC and calendar has a dedicated low-power, 32kHz crystal oscillator. Phase- or frequency-locked loops multiply the selected clock source to the needed operating frequency. Designers can individually gate the clock source to each peripheral. The combination of all these features allows the device to meet the performance and power-consumption trade-off an application requires.

Summary

Atmel´s new ARM-core based microcontroller families combine industry-standard 32-bit ARM M-core processing performance with innovative peripherals and system-architecture features to create products that meet the challenging real-time performance demands of automotive applications.

Driving Futuristic Human-Machine-Interface Concepts for Automotive Applications

Stephan Thaler

The automotive industry is making great strides in alternative driving technologies, with ever more efficient gas and diesel engines, hybrid variants and pure electric-drive options. The industry is also increasingly using new materials, such as carbon fiber, to help make cars lighter and more energy-efficient. With ubiquitous always-on data, vehicles can now provide passengers with unique digital experiences on their journeys.

These new advanced technologies are increasingly becoming part of the persona of the vehicle and the underlying brand. As such, they require a human-machine interface (HMI) that is fit for the future.

Gone are arrays of backlit, gray switches with confusing iconography, clunky segmented LCDs and mechanical rotary dials. Instead, new vehicles include an array of new technologies that provide clearer views of maps, better status updates of vehicles' onboard systems and deep integration with the devices that drivers use in the vehicle. Furthermore, these technologies provide both drivers and passengers with the ability to choose options, such as ambient lighting, to suit their moods and personalities.

With more than 30 years of experience in body electronics and power-train designs, Atmel® has a pedigree in automotive electronics. The company's design and manufacturing processes are in place to meet the demands of AEC-Q100 qualification and the automotive industry's quality target of zero defects. It should come then as no surprise that Atmel has managed to successfully apply this experience to capacitive-touch technology.

Since the launch a decade ago of the first MP3 players with capacitive-sensor-based scroll wheels as part of the HMI, Atmel has pursued a position of technical dominance in this area. Millions of people worldwide now interact with such technology on a daily basis through a host of devices and appliances, including their smartphones; their coffeemakers; and their washers, dryers, and refrigerators. But one question remains: What effect will capacitive-touch sensing have on the user experience in automobiles? The AvantCar™ center stack represent Atmel's vision of future vehicle interiors. It uses a broad array of in-house, commercially available technologies that could now find use in vehicles.

AvantCar Concept

The AvantCar concept pushes the boundaries of the possible to the extreme. The most eye-catching design element is the glossy, flowing line of the center stack, with its curved surface, which begs to be touched. The navigation system takes up the uppermost section of the stack, and a similarly sized section below it has large, clear buttons, allowing users to control and set music and other comfort options. AvantCar uses no traditional mechanical buttons; everything works through touch. Two touchscreens, each about the size of a large tablet, dominate the curvaceous expanse of the navigation system. Together, they provide an empty canvas to cater to the whims and desires of those designing the user interface. For example, the bottom screen splits into groups of touch zones providing access to in-car comfort controls, such as ambient lighting and climate control, and multimedia options for radio, MP3 and other technologies.

To minimize clutter, touch zones use clear iconography to provide access to a more expansive user interface. Thus, for example, selecting the climate-control button opens a new collection of options that provide the expected granularity of control. This collection of buttons can then move to a free area of the screen or recede completely when a user selects an alternate control interface, such as multimedia.

By providing a blank canvas as a starting point for the HMI, the AvantCar concept opens many new possibilities for interaction with an automobile's systems. The technology enables an easily realized element of user customization, common in smartphones and PCs. Users can also add a new vehicle feature or a model update at a modest level of investment.

Perhaps the most striking and cleverest capability, however, is the user interface's dependence on the person who most recently interacted with the console.

If the driver were to adjust his or her seat-heating setting, the appropriate collection of menu options would appear on the driver's side of the screen. However, if the front-seat passenger were to do the same, the same collection of menu options slide across to the passenger's side of the screen. This feature helps to simplify user control, reduces the amount of time the driver must take his or her eyes off the road and decreases driver distraction from a passenger who tries to activate a function that is on the driver's side of the console. Drivers can also easily integrate a wide array of media in the vehicle, such as that available on smartphones or tablets, along with notification from apps.

maXTouch Touchscreen Controllers

Although the function of the electronics that evaluate all the nodes of a touch sensor for touches and gestures is simple to describe, the challenge lies in the implementation. A typical touchscreen has several hundred nodes that require rapid and repeated evaluation. This requirement alone is more complicated than it sounds; each node has a capacitance of a few picofarads, and the application of a finger results in a change of only fractions of picofarads. The touch-detection subsystem must also, in a few milliseconds, successfully differentiate an actual touch from a false or an unwanted touch. Furthermore, it must—in a few hundred milliseconds—evaluate changes in signal across several related nodes for a possible gesture, such as a zoom or a swipe motion. Only after reliably meeting all these criteria is the system ready for integration into an automotive environment without concern that poor system response to inputs might detract from usability. Atmel's automotive-qualified maXTouch® devices, with their unparalleled analog sensing technology and integrated postprocessing, suit such applications.

The implementation of a touch interface has such demanding real-time processing requirements that the only serious solution is one that is dedicated to the task. The maXTouch analog front end ensures that the incoming signal is of the highest possible quality, providing high-quality data to the digital postprocessing blocks. The digital back end is also highly configurable, and designers can reconfigure it on the fly. The devices handle filtering of various noise sources; detection of gloved versus gloveless use; and the suppression of unintended touches, such as a resting palm. Once the system recognizes a valid touch, maXTouch then characterizes the touch or gesture type, with any related pertinent parameters, such as speed or direction. It then transfers this compressed description of the user's intent to the host CPU, thus improving total system responsiveness and simplifying user-input processing.

Many of today's premium vehicles include rotary push dials to input, for example, the characters of a street name or a town into the navigation system. Many users consider these dials cumbersome and nonintutitive. In contrast, the maXTouch products offer a scan rate of up to 280Hz that enables, with suitable external postprocessing, the recognition of characters input onto a built-in touchpad built on the center stack. Thus, drivers can access novel input method that would have been impractical before the introduction of capacitive touch.

QTouch Technology

Drivers would sometimes benefit from a haptic, or touch-based, experience similar to that of a mechanical interface. Such an interface would be helpful for drivers when they are attempting to control a vehicle´s temperature or fan speed. Atmel´s QTouch® technology makes it possible to implement items such as sliders and rotary wheels to complement the larger touchscreen interface. The AvantCar concept implements two capacitive touch sliders below the lower touchscreen. In this case, they provide an alternative control input, complementing a multiple-button-press control on the touchscreen menu. To ease usability, the curved console implements a subtle groove, allowing a user´s finger to naturally find the area of control.

Atmel's QTouch software library simplifies designers´ ability to integrate capacitive buttons, sliders, wheels and proximity sensors. The software library supports as many as 64 capacitive channels, with sliders and wheels requiring three channels per instantiation and delivering a resolution as high as 256 bits. Designers can implement QTouch on a wide array of Atmel´s 8- and 32-bit automotive-qualified AVR microcontrollers. Those looking for a simpler approach will find a range of fixed-function products that also meet the automotive standards.

LIN-Based Ambient Lighting

Vehicle manufacturers are well-aware of drivers´ desire to configure personal electronics to suit their moods and personalities. The AvantCar concept provides a view of the possibilities in the form of a string of linked RGB LED modules and uses a LIN (local-interconnect-network) bus as the control interface. Designers can string together tens of modules requiring only power, ground and LIN connections, minimizing cabling weight and complexity. Atmel´s latest generation of system-based chips (SBCs) pairs with an 8-bit, automotive-grade, 16kB microcontroller and lies between the system bus and the LEDs. The SBC handles the signaling element of the LIN-bus communication with its robust analog circuitry and provides a 5V, 80mA regulator, watchdog and eight high-voltage current sources with switches. The SBC, AVR microcontroller, and a handful of passive components come in a 7-by-7mm QFN package, and designers can compress it onto a circuit board about the size of a thumbprint.

The menu system enables drivers and passengers to use the touchscreen to select a lighting ambiance that suits their moods. Installation and any necessary replacement of the RGB modules are simple, requiring only a branch from a three-wire cable loom for each ambient-light module.

The future is closer than you think

Motor shows and concept vehicles tend to show ideas of future mobility that are just out of arm´s reach. The AvantCar concept, however, uses proven technology that manufacturers are installing in vehicles today and provides a vision of how the center console of all vehicles could look in just a few years´ time.

Atmel® | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T :** (+1)(408) 441. 0311 **F :** (+1)(408) 436. 4200 | **www.atmel.com**

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.