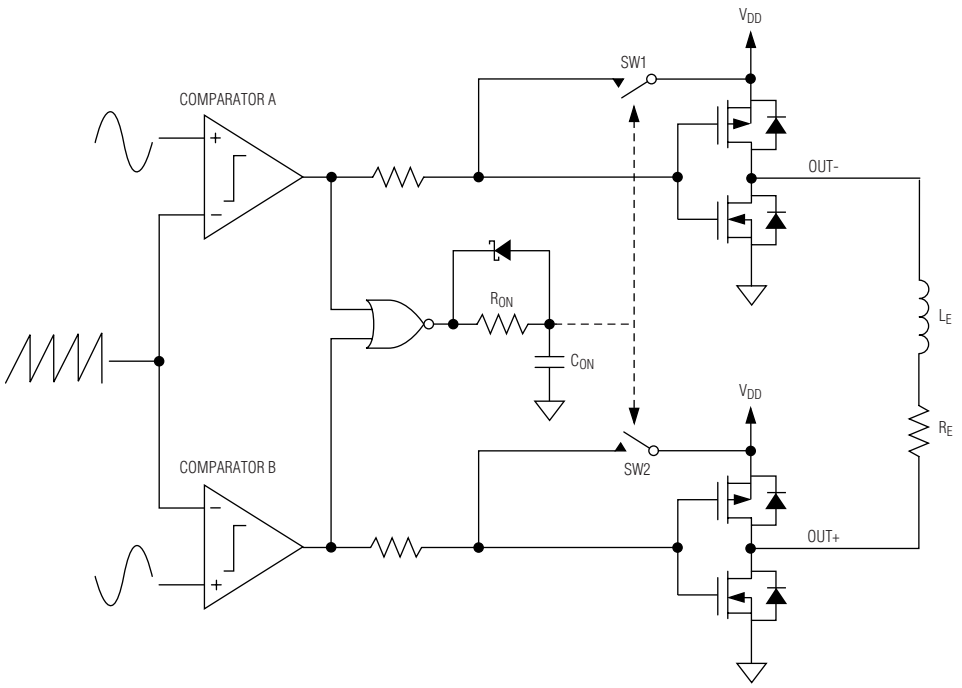
DALLAS SEMICONDUCTOR MAXIM

Engineering Journal

Volume Fifty-Nine



This simplified functional diagram shows the MAX9700's filterless Class D modulator topography. *(See page 8.)*

News Brief

MAXIM REPORTS REVENUES AND EARNINGS FOR THE FIRST QUARTER OF FISCAL 2007

Maxim Integrated Products, Inc., (MXIM) reported net revenues of $502.7 million for its fiscal first quarter ended September 23, 2006, a 1.5% decrease over the fourth quarter of fiscal 2006 and a 18.5% increase over the first quarter of fiscal 2006.

Net income for the first quarter of fiscal 2007 was $107.5 million or $0.33 diluted earnings per share including stock-based compensation. For comparison purposes, net income for the fourth quarter of fiscal 2006 was $124.3 million or $0.37 diluted earnings per share and net income for the same period a year ago was $105.4 million or $0.31 per share including stock-based compensation.

Research and development expense was $130.2 million or 25.9% of net revenue. This compares to $127.2 million or 24.9% in the fourth quarter of fiscal 2006. The increase in research and development was primarily due to additional headcount and related expenses to support future product development.

Selling, general and administrative expense was $40.1 million or 8.0% of net revenue. This compares to $37.9 million or 7.4% in the fourth quarter of fiscal 2006. The increase in selling, general and administrative expense was primarily due to $3.0 million associated with the audit of the Company's stock option program.

Total operating profit for the first quarter was $150.8 million or 30.0% of net revenues compared to $173.3 million or 34.0% for the fourth quarter and $145.8 million or 34.4% for the first quarter of fiscal 2006.

The 2 percentage point sequential increase in our tax rate was due to the old tax deduction for extra territorial income being replaced with the deduction for domestic production that is phased in over several years and the U.S. government's failure to extend the Research & Development tax credit. This resulted in a $3.3 million reduction in net income or $0.01 diluted earnings per share.

During the quarter, cash and cash equivalents increased $51.4 million to $1.4 billion after the Company repurchased 2.1 million shares of its common stock for $60.8 million, paid dividends of $50.0 million, and paid $94.9 million for capital equipment. Accounts receivable decreased $0.8 million in the first quarter to $291.7 million and inventories for the first quarter increased $10.6 million to $217.9 million and includes $15.6 million of stock-based compensation.

Mr. Gifford commented: "The Company's Board of Directors has declared a cash dividend for the second quarter of fiscal 2007 of $0.156 per share. Payment will be made on December 5, 2006 to stockholders of record on November 21, 2006."

For the complete Q107 press release, including safe harbor information, go to: www.maxim-ic.com/NewsBrief

Class D Amplifiers: Fundamentals of Operation and Recent Developments

A Class D amplifier's high efficiency makes it ideal for portable and compact high-power applications. Traditional Class D amplifiers require an external lowpass filter to extract the audio signal from the pulse-width-modulated (PWM) output waveform. Many modern Class D amplifiers, however, utilize advanced modulation techniques that, in various applications, both eliminate the need for external filtering and reduce electromagnetic interference (EMI). Eliminating external filters not only reduces board-space requirements, but can also significantly reduce the cost of many portable/compact systems.

Introduction

Most audio system design engineers are well aware of the power-efficiency advantages of Class D amplifiers over linear audio-amplifier classes such as Class A, B, and AB. In linear amplifiers such as Class AB, significant amounts of power are lost due to biasing elements and the linear operation of the output transistors. Because the transistors of a Class D amplifier are simply used as switches to steer current through the load, minimal power is lost due to the output stage. Any power losses associated with a Class D amplifier are primarily attributed to output transistor on-resistances, switching losses, and quiescent current overhead. Most power lost in an amplifier is dissipated as heat. Because heatsink requirements can be greatly reduced or eliminated in Class D amplifiers, they are ideal for compact high-power applications.

In the past, the power-efficiency advantage of classical PWM-based Class D amplifiers has been overshadowed by external filter component cost, EMI/EMC compliance, and poor THD+N performance when compared to linear amplifiers. However, most current-generation Class D amplifiers utilize advanced modulation and feedback techniques to mitigate these issues.

The Basics of Class D Amplifiers

While there are a variety of modulator topologies used in modern Class D amplifiers, the most basic topology utilizes pulse-width modulation (PWM) with a triangle-wave (or sawtooth) oscillator. **Figure 1** shows a simplified block diagram of a PWM-based, half-bridge Class D amplifier. It consists of a pulse-width modulator, two output MOSFETs, and an external lowpass filter (L_F and C_F) to recover the amplified audio signal. As shown in the figure, the p-channel and n-channel MOSFETs operate as current-steering switches by alternately connecting the output node to V_{DD} and ground. Because the output transistors switch the output to either V_{DD} or ground, the resulting output of a Class D amplifier is a high-frequency square wave. The switching frequency (f_{SW}) for most Class D amplifiers is typically between 250kHz to 1.5MHz. The output square wave is pulse-width modulated by the input audio signal. PWM is accomplished by comparing the input audio signal to an internally generated triangle-wave (or sawtooth) oscillator. This type of modulation is also often referred to as "natural sampling" where the triangle-wave oscillator acts as the sampling clock. The resulting duty cycle of the square wave is proportional to the level of the input

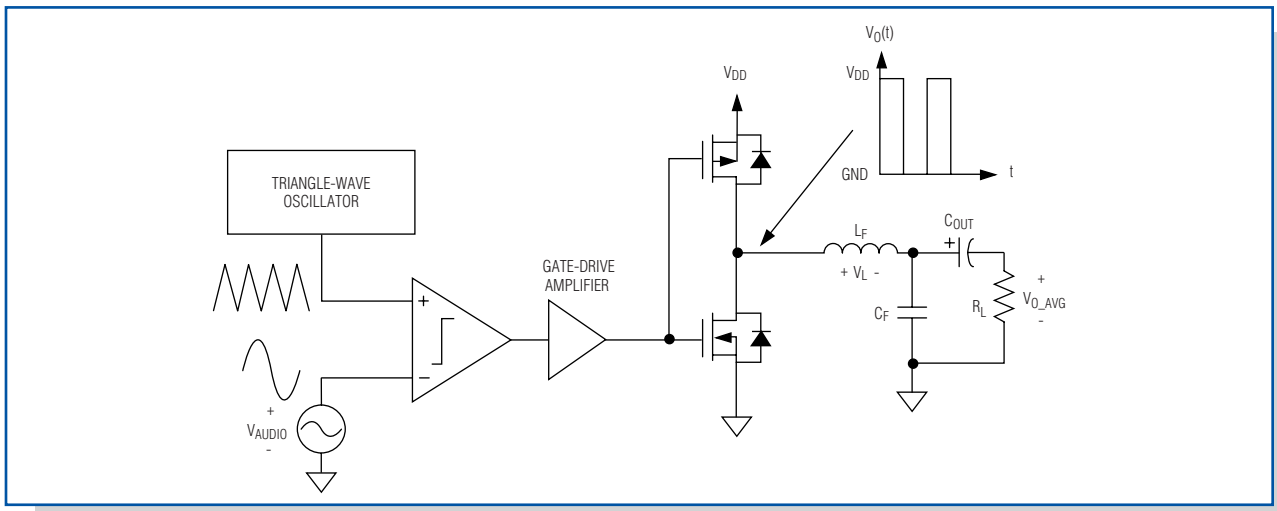


Figure 1. This simplified functional block diagram illustrates a basic half-bridge Class D amplifier.

signal. When no input signal is present, the duty cycle of the output waveform is equal to 50%. **Figure 2** illustrates the resulting PWM output waveform due to the varying input-signal level.

In order to extract the amplified audio signal from this PWM waveform, the output of the Class D amplifier is fed to a lowpass filter. The LC lowpass filter shown in Figure 1 acts as a passive integrator (assuming the cutoff frequency of the filter is at least an order of magnitude lower than the switching frequency of the output stage) whose output is equal to the average value of the square wave. Additionally, the lowpass filter prevents high-frequency switching energy from being dissipated in the resistive load. Assume that the filtered output voltage (V_{O_AVG}) and current (I_{AVG}) remain constant during a single switching period. This assumption is fairly accurate because f_{SW} is much greater than the highest input audio frequency. Therefore, the relationship between the duty cycle and resulting filtered output voltage can be derived using a simple time-domain analysis of the inductor voltage and current.

The instantaneous current flowing through the inductor is:

$$I_L(t) = \frac{1}{L}\int V_L(t)dt \qquad \text{(Eq 1)}$$

where $V_L(t)$ is the instantaneous voltage across the inductor using the sign convention shown in Figure 1.

Because the average current (I_{AVG}) flowing into the load is assumed constant over one switching period, the inductor current at the beginning of the switching period (T_{SW}) must be equal to the inductor current at the end of the switching period, as shown in **Figure 3**.

In mathematical terms, this means that:

$$\frac{1}{L}\int_0^{T_{SW}} V_L(t)dt = I_L(T_{SW}) - I_L(0) = 0 \qquad \text{(Eq 2)}$$

Equation 2 shows that the integral of the inductor voltage over one switching period must be equal to 0. Using equation 2 and examining the $V_L(t)$ waveform shown in Figure 3, it is clear that the absolute values of the areas (A_{ON} and A_{OFF}) must be equal to each other in order for equation 2 to be true. With this information, we can now derive an expression for the filtered output voltage in terms of the duty ratio of the switching waveform:

$$A_{ON} = |A_{OFF}| \qquad \text{(Eq 3)}$$

$$A_{ON} = (V_{DD} - V_O) \times t_{ON} \qquad \text{(Eq 4)}$$

$$A_{OFF} = V_O \times t_{OFF} \qquad \text{(Eq 5)}$$

Substituting equations 4 and 5 into equation 3 gives the new equation:

$$(V_{DD} - V_O) \times t_{ON} = V_O \times t_{OFF} \qquad \text{(Eq 6)}$$

Finally, solving for V_O gives:

$$V_O = V_{DD} \times \frac{t_{ON}}{t_{ON} + t_{OFF}} = V_{DD} \times D \qquad \text{(Eq 7)}$$

where D is the duty ratio of the output-switching waveform.

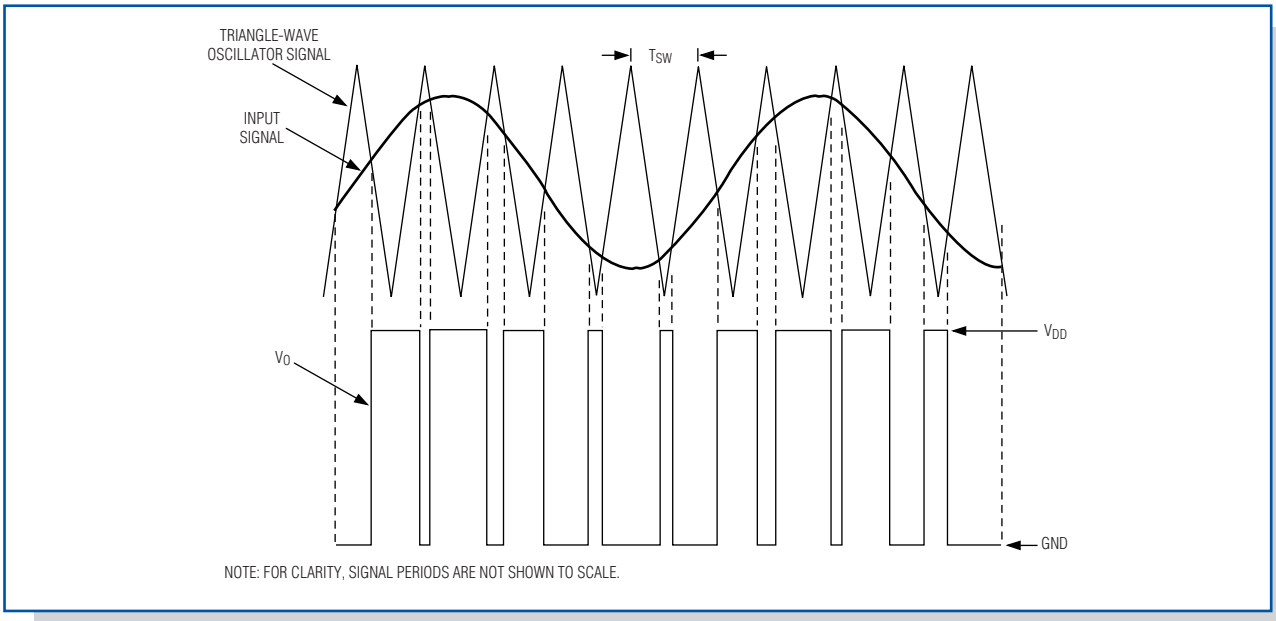


Figure 2. The output-signal pulse widths vary proportionally with the input-signal magnitude.

Using Feedback to Improve Performance

Many Class D amplifiers utilize negative feedback from the PWM output back to the input of the device. A closed-loop approach not only improves the linearity of the device, but also allows the device to have power-supply rejection. This contrasts with an open-loop amplifier, which inherently has minimal (if any) supply rejection. Because the output waveform is sensed and fed back to the input of the amplifier in a closed-loop topology, deviations in the supply rail are detected at the output and corrected by the control loop. The advantages of a closed-loop design come at the price of possible stability issues, as is the case with all systems utilizing feedback. Therefore, the control loop must be carefully designed and compensated to ensure stability under all operating conditions.

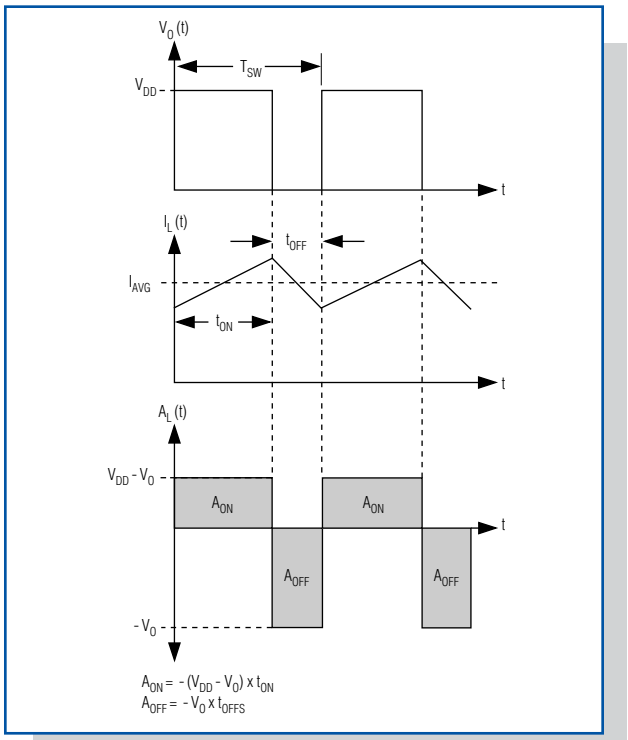


Figure 3. Filter inductor current and voltage waveforms are shown for a basic half-bridge Class D amplifier.

Typical Class D amplifiers operate with a noise-shaping type of feedback loop, which greatly reduces in-band noise due to the nonlinearities of the pulse-width modulator, output stage, and supply-voltage deviations. This topology is similar to the noise shaping used in sigma-delta modulators. To illustrate this noise-shaping function, **Figure 4** shows a simplified block diagram of a 1st-order noise shaper. The feedback network typically consists of a resistive-divider network but, for simplicity, the example shown in Figure 4 uses a feedback ratio of 1. Also, the transfer function for the integrator has been simplified to equal 1/s because the gain of an ideal integrator is inversely proportional to frequency. It is also assumed that the PWM block has a unity-gain and zero-phase-shift contribution to the control loop. Using basic control-block analysis, the following expression can be derived for the output:

$$V_O(s) = \frac{1}{1+s} \times V_{IN}(s) + \frac{s}{1+s} \times E_n(s) \qquad \text{(Eq 8)}$$

Equation 8 shows that the noise term, $E_n(s)$, is multiplied by a highpass filter function (noise-transfer function) while the input term, $V_{IN}(s)$, is multiplied by a lowpass filter function (signal-transfer function). The noise-transfer function's highpass filter response shapes the noise of the Class D amplifier. If the cutoff frequency of the output filter is selected properly, most of the noise is pushed out of band

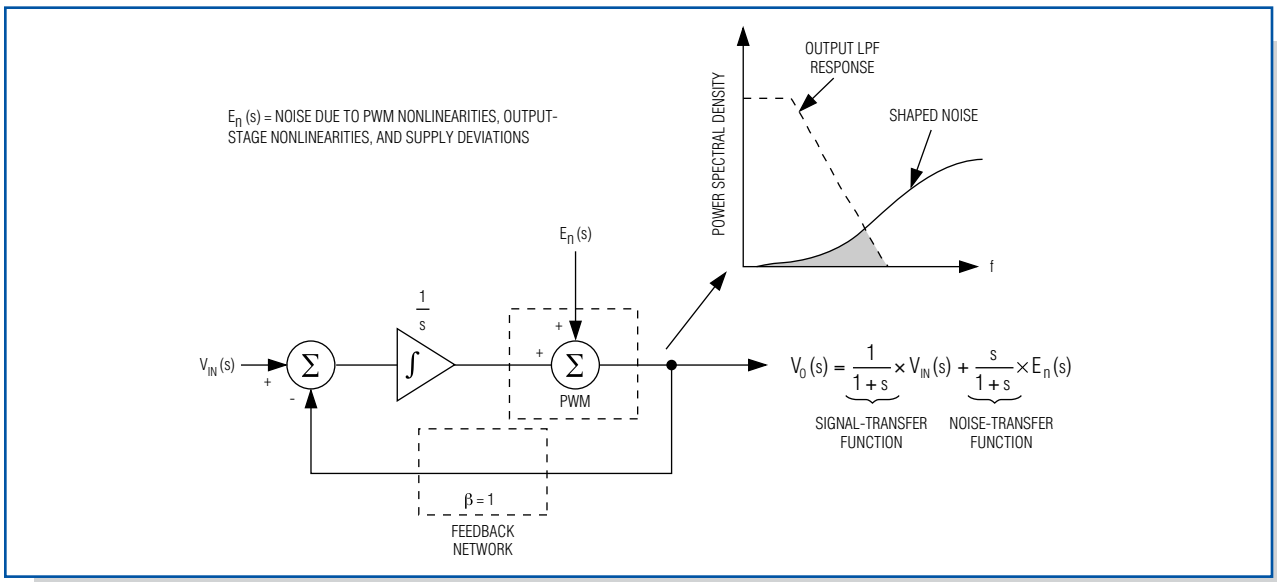


Figure 4. A control loop with 1st-order noise shaping for a Class D amplifier pushes most noise out of band.

(Figure 4). While the preceding example dealt with a 1st-order noise shaper, many modern Class D amplifiers utilize multi-order noise-shaping topologies to further optimize linearity and power-supply rejection.

Class-D Topologies—Half Bridge vs. Full Bridge

Many Class D amplifiers are also implemented using a full-bridge output stage. A full bridge uses two half-bridge stages to drive the load differentially. This type of load connection is often referred to as a bridge-tied load (BTL). As shown in **Figure 5**, the full-bridge configuration operates by alternating the conduction path through the load. This allows bidirectional current to flow through the load without the need of a negative supply or a DC-blocking capacitor.

Figure 6 illustrates the output waveforms of traditional BTL, PWM-based, Class D amplifiers. In Figure 6, the output waveforms are complements of each other, which produce a differential PWM signal across the load. As with the half-bridge topology, an external LC filter is needed at the output to extract the low-frequency audio signals and prevent high-frequency energy from being dissipated in the load.

A full-bridge Class D amplifier shares the same advantages of a Class AB BTL amplifier, but adds high power efficiency. The first advantage of BTL amplifiers is that they do not require DC-blocking capacitors on the outputs when operating from a single supply. The same is not true for a half-bridge amplifier as its output swings between V_{DD} and ground and idles at 50% duty cycle. This means that its output has a DC offset equal to $V_{DD}/2$. With a full-bridge amplifier, this offset appears on each side of the load, which means that zero DC current flows at the output. The second advantage they share is that they can achieve twice the output signal swing when compared to a half-bridge amplifier with the same supply voltage because the load is driven differentially. This results in a theoretical 4x increase in maximum output power over a half-bridge amplifier operating from the same supply.

A full-bridge Class D amplifier, however, requires twice as many MOSFET switches as a half-bridge topology. Some consider this to be a disadvantage, because more switches typically mean more conduction and switching losses. However, this generally is only true with high-output power amplifiers (> 10W) due to the higher output currents and supply voltages involved. For this reason, half-bridge amplifiers are typically used for high-power applications for their slight efficiency advantage. Most high-power full-bridge amplifiers exhibit power efficiencies in the range of 80% to 88% with 8Ω loads. However, half-bridge amplifiers like the MAX9742 achieve power efficiencies greater than 90% while delivering more than 14W per channel into 8Ω.

Eliminating the Output Filter—Filterless Modulation

One of the major drawbacks of traditional Class D amplifiers has been the need for an external LC filter. This need not only increases a solution's cost and board space requirements, but also introduces the possibility of additional distortion due to filter component nonlinearities. Fortunately, many modern Class D amplifiers utilize advanced "filterless" modulation schemes to eliminate, or at least minimize, external filter requirements.

Figure 7 shows a simplified functional diagram of the MAX9700 filterless modulator topology. Unlike the traditional PWM BTL amplifier, each half bridge has its own dedicated comparator, which allows each output to be controlled independently. The modulator is driven with a differential audio signal and a high-frequency sawtooth waveform. When both comparator outputs are low, each output of the Class D amplifier is high. At the same time, the output of the NOR gate goes high, but is delayed by the RC circuit formed by R_{ON} and C_{ON}. Once the delayed output of the NOR gate exceeds a specified threshold, switches SW1 and SW2 close. This causes OUT+ and OUT- to go low and remain as such until the next sampling period begins. This scheme causes both outputs to be on for a minimum amount of time ($t_{ON(MIN)}$), which is set by the values of R_{ON} and C_{ON}. As shown in **Figure 8**, with zero input, the outputs are in phase with pulse widths equal to $t_{ON(MIN)}$. As the audio input signals increase or decrease, one comparator trips before the other. This behavior, along with the minimum on-time circuitry, causes one output to vary its pulse width while the other output pulse width remains at $t_{ON(MIN)}$ (Figure 8). This means that the average value of each output contains a half-wave rectified version of the output audio signal. Taking the difference of the average values of the outputs yields the complete output audio waveform.

Because the MAX9700's outputs idle with in-phase signals, there is no differential voltage applied across the load, thereby minimizing quiescent power consumption without the need for an external filter. Rather than depend on an external LC filter to extract the audio signal from the output, Maxim's filterless Class D amplifiers rely on the inherent inductance of the speaker load and the human ear to recover the audio signal. The speaker resistance (R_E) and inductance (L_E) form a 1st-order lowpass filter which has a cutoff frequency equal to:

$$f_C = \frac{1}{2\pi \times \frac{L_E}{R_E}} \quad \text{(Eq 9)}$$

With most speakers, this 1st-order rolloff is enough to recover the audio signal and prevent excessive amounts of high-frequency switching energy from being dissipated

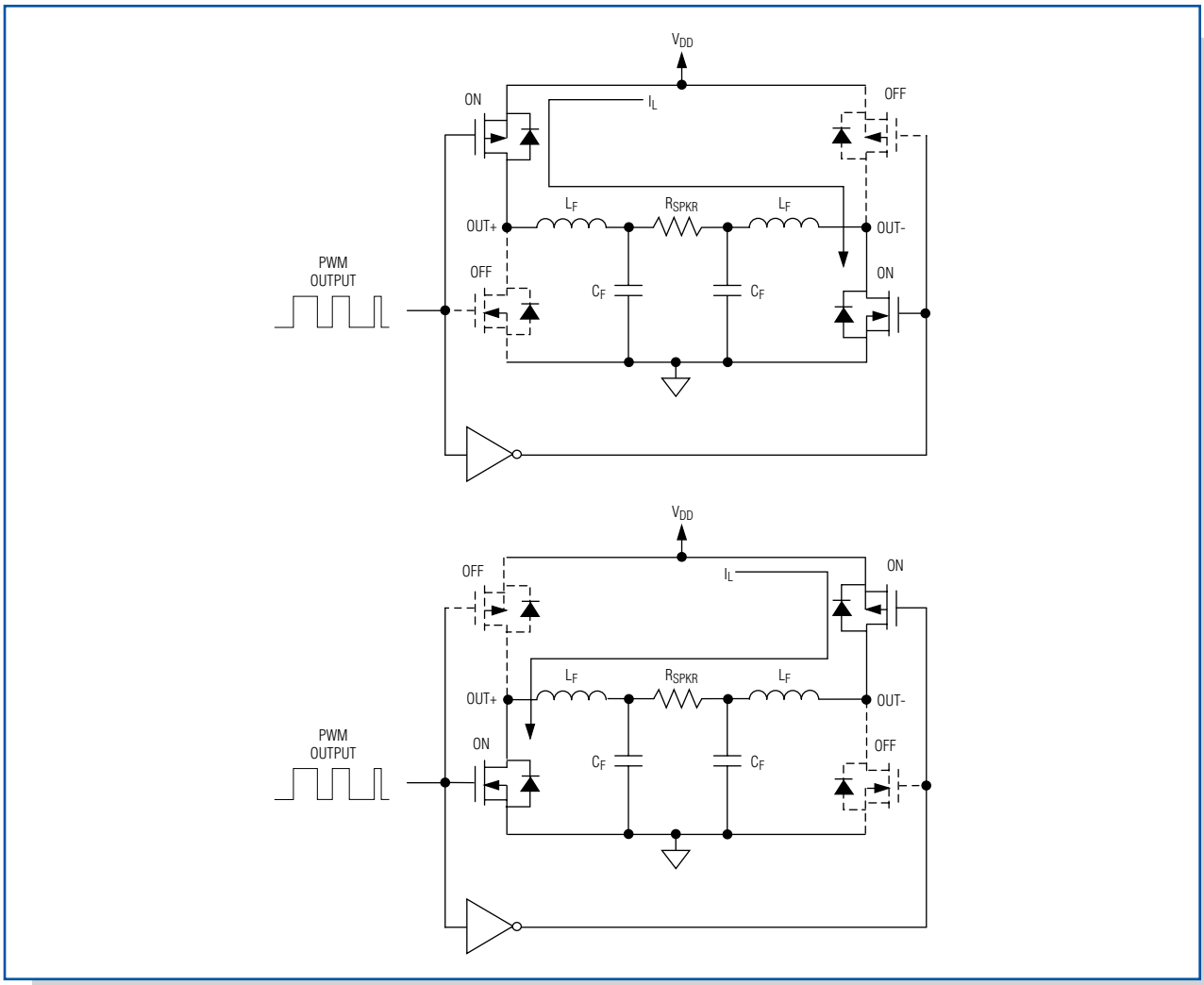


Figure 5. A traditional full-bridge Class D output stage uses two half-bridge stages to drive the load differentially.

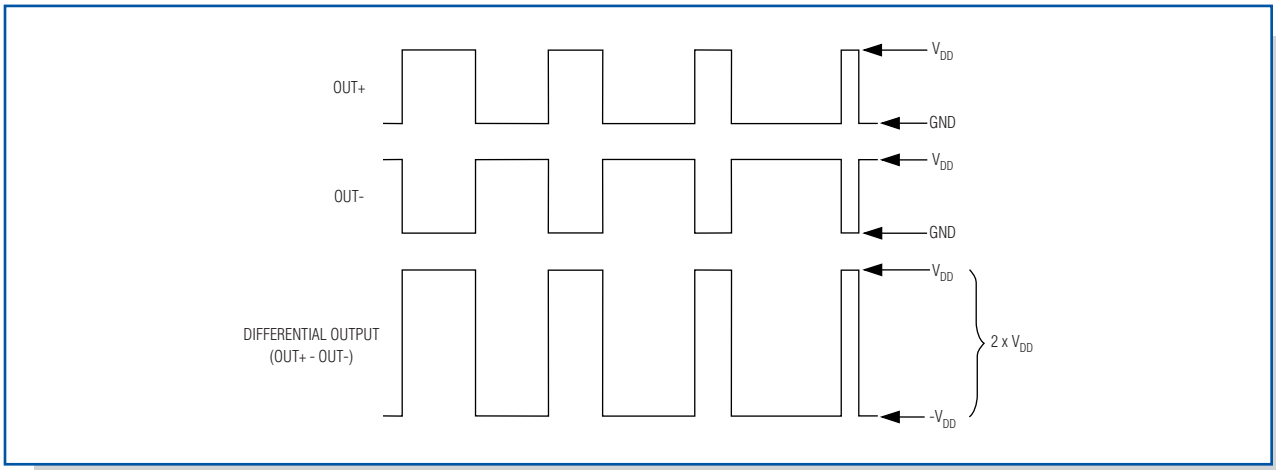


Figure 6. Traditional full-bridge Class D output waveforms complement each other, thus creating a differential PWM signal across the load.

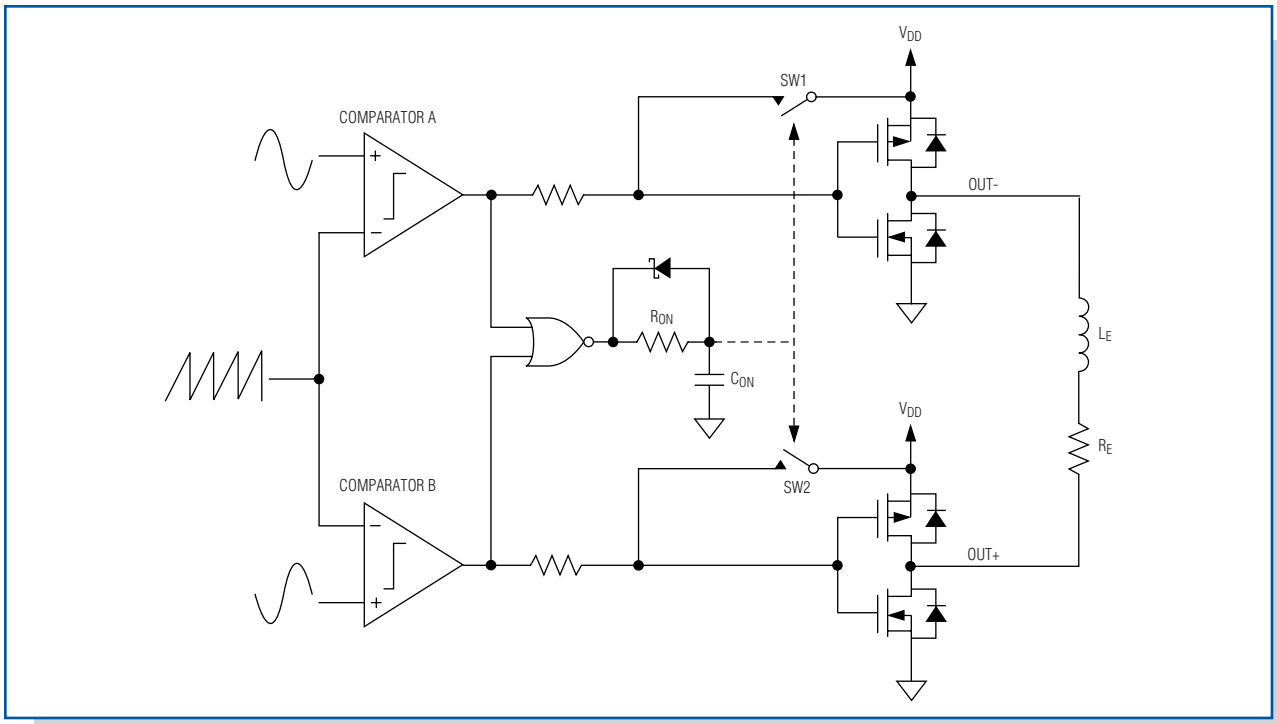


Figure 7. This simplified functional diagram shows the MAX9700's filterless Class D modulator topography.

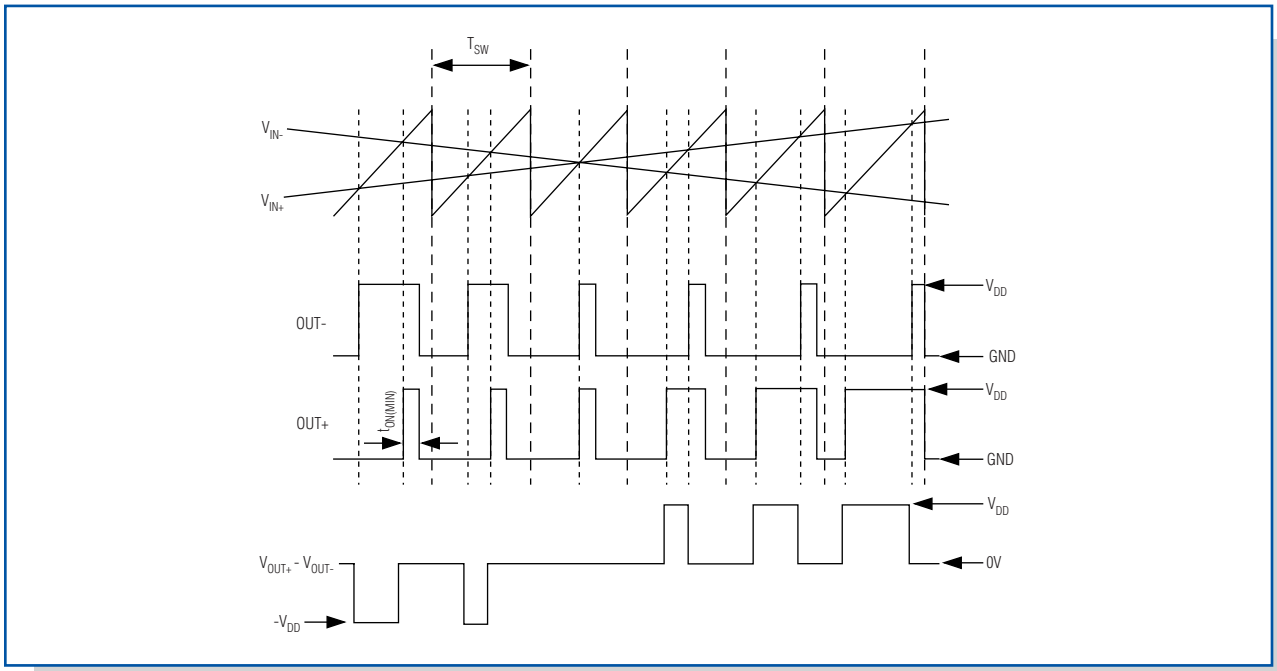


Figure 8. The input and output waveforms are shown for the MAX9700's filterless modulator topography.

in the speaker resistance. Even if residual switching energy results in speaker movement, these frequencies are inaudible to the human ear and will not adversely affect the listening experience. When using filterless Class D amplifiers, the speaker load should remain inductive at the amplifier's switching frequency to achieve maximum output-power capabilities.

Minimizing EMI with Spread-Spectrum Modulation

One disadvantage of filterless operation is the possibility of radiated EMI from the speaker cables. Because the Class D amplifier output waveforms are high-frequency square waves with fast-moving transition edges, the output spectrum contains a large amount of spectral energy at the switching frequency and integer multiples of the switching frequency. Without an external output filter located within close proximity of the device, this high-frequency energy can be radiated by the speaker cables. Maxim's filterless Class D amplifiers help mitigate possible EMI problems through a patented modulation scheme known as spread-spectrum modulation.*

Spread-spectrum modulation is accomplished by dithering or randomizing the switching frequency of the Class D amplifier. The switching frequency is typically varied up to ±10% of the nominal switching frequency. While the period of the switching waveform is varied randomly cycle-to-cycle, the duty cycle is not affected, thereby preserving the audio content of the switching waveform. **Figures 9a** and **9b** show the wideband output spectrum of the MAX9700 to illustrate the effects of spread-spectrum modulation. Rather than having the spectral energy concentrated at the switching frequency and its harmonics, spread-spectrum modulation effectively spreads out the spectral energy of the output signal. In other words, the total amount of energy present in the output spectrum remains the same, but the total energy is redistributed over a wider bandwidth. This reduces the high-frequency energy peaks at the outputs, therefore minimizing the chances of EMI being radiated from the speaker cables. While it is possible that some spectral noise may redistribute into the audio band with spread-spectrum modulation, this noise is suppressed by the noise-shaping function of the feedback loop.

Many of Maxim's filterless Class D amplifiers also allow the switching frequency to be synchronized to an external clock signal. This allows the user to manually set the switching frequency of the amplifier to a less-sensitive frequency range.

While spread-spectrum modulation significantly improves EMI performance of filterless Class D amplifiers, there is typically a practical limit on the length of the speaker cables that can be used before the device begins to fail FCC or CE radiated-emissions regulations. If a device fails radiated-emissions tests due to long speaker cables, an external output filter may be needed to provide additional attenuation of the high-frequency components of the output waveform. In many applications with moderate speaker cable lengths, ferrite bead/capacitor filters on the outputs will suffice. EMI performance is also very layout sensitive, so proper PCB-layout guidelines should be strictly followed to guarantee compliance with applicable FCC and CE regulations.

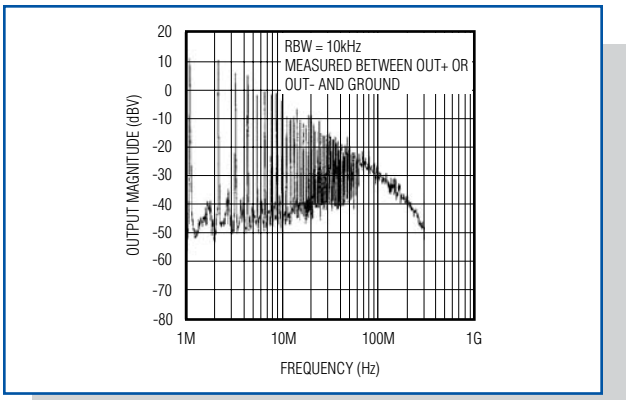


Figure 9a. The wideband output spectrum is shown for the MAX9700 using a fixed switching frequency.

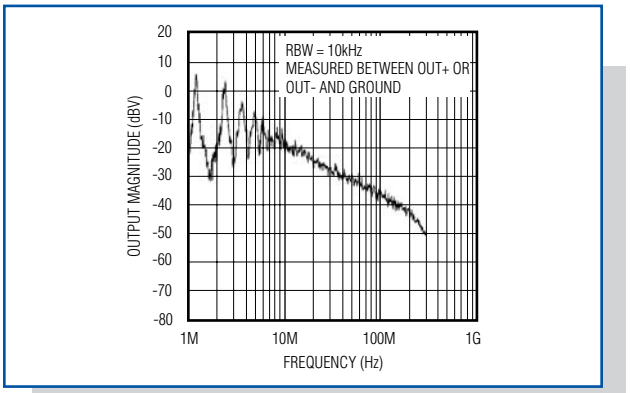


Figure 9b. Spread-spectrum modulation redistributes the spectral energy of the MAX9700 over a wider bandwidth.

Conclusion

Recent advancements in Class D modulation techniques have allowed Class D amplifiers to flourish in applications where linear amplifiers once dominated. Modern Class D amplifiers include all of the advantages of Class AB amplifiers (i.e., good linearity and minimal board-space requirements) with the added bonus of high power efficiency. Currently, there are a wide variety of Class D amplifiers available, thus making them suitable for numerous applications. These applications range from low-power portable applications (e.g., cell phones, notebooks) in which battery life, board-space requirements, and EMI compliance are of utmost importance, to high-power applications (e.g., automotive sound systems, or flat-panel displays) where minimizing heatsinking requirements and heat generation is vital. Having a fundamental understanding of Class D amplifiers and their recent technological advances will aid designers in selecting the correct amplifier for their application and allow them to successfully weigh the advantages and disadvantages of specific features.

*US Patent #6,847,257.

Embedded Security Going Forward

With the rapidly growing concerns of security in nearly every aspect of electronic system design, manufacturers and circuit designers will soon face challenges that never before existed. In the past, security within electronic equipment was something only faced by a limited and very selective audience consisting mostly of software-related technologies or specialized hardware used in financial, military, and access-control markets. This is all about to change as designers will soon be given a host of new standards to meet, certifications to obtain, and technical knowledge to learn that will seem foreign to many seasoned designers of embedded electronic systems. Understanding this technological trend, as well as its design and manufacturing cost ramifications, is of growing importance to equipment manufacturers of embedded systems.

Because ensuring software/firmware integrity is an extremely complex issue, the burden is placed upon hardware to maintain security and not become the weakest link in a complex security implementation (see *Appendix 1—Classification Taxonomy* on page 11). With the formation of new standards bodies like the Trusted Computing Group™, as well as various digital rights management (DRM) proponents, the issue of security is rapidly affecting a broad range of devices, including consumer, media, industrial, medical, automotive, and telecommunication equipment. Of course, this issue also includes governmental or homeland security system upgrades and the increased proliferation of electronic banking and e-commerce applications.

However, for any security solution to be effective, physical tamper protection and the methods to achieve it must be addressed. Even the most sophisticated secure microprocessors, FPGAs, smart cards, and other security components still remain vulnerable to certain attack scenarios. This vulnerability leads to the requirement of maintaining a suitable portion of active circuitry, which remains "alive" during system downtime to sense a potential attempt to extract or steal sensitive information or intellectual property. To accomplish this, devices must use extremely low power. They also must be housed in tamper-reactive packages that include suitable interfaces for the variety of sensors used to create this security fence around content-sensitive circuitry.

It is important to realize that the strength of an encryption algorithm is no longer the target of an attack. It is much easier and far more beneficial to simply devise clever ways to steal the keys. Therefore, an increasing amount of attention is being placed upon physical hardware protection requirements.

Emerging Security Standards

Most newly evolving security standards stem from specifications set forth by the National Institute of Standards and Technology (NIST) in the US and from the Communications-Electronics Security Group (CESG) in the UK. These organizations provided standards known as FIPS 140-1 and ITSEC, respectively.

Because of the many new standards emerging and increasing level of security required, these and other multinational groups are adopting a new single standard that combines the best of these standards, known as "Common Criteria" (see *Appendix 2—Common Certifications/Standards* on page 12). For example, NIST has now updated its FIPS specification to 140-2 and will soon be moving solely to Common Criteria.

With the increasing proliferation of devices capable of conducting financial transactions, other standards now come into play. Among the most recognized is EMV (European MasterCard® Visa®) and PCI PED (payment card industry; PIN entry device), which was established by MasterCard and Visa. One can expect these certification standards to become increasingly more stringent due to the newly evolving trends associated with DRM, the ability for mobile platforms to conduct financially related transactions while protecting a user's or system's identity, and new government initiatives such as FIPS 201 Personal Identity Verification (PIV).

All of the aforementioned standards outline the physical security requirements that must be met for certification for various end-equipment categories. Generally, this requires security to be addressed in multiple layers beginning at the silicon-processor level and ending at the packaging that surrounds the processor, memory, or data path exposed to sensitive content or algorithms. For an end product to achieve certification, it must undergo extensive testing by an approved laboratory and be accompanied by a security target document that outlines how specific physical security threats are mitigated. In the case of some standards (PCI, for example), the manufacturer must show what security improvements have been made over their existing products to meet newly updated criteria. In many instances, the vague nature of exactly how security must be designed into a product can be very frustrating to manufacturers and design teams who have not yet had to face these types of requirements.

The requirements that determine what level of security certification is needed vary considerably; nonetheless, the demands placed upon physical tamper protection are becoming increasingly more stringent. These demands are

driven by the availability of sophisticated analysis tools and the technical expertise necessary to launch a sophisticated attack.

DS3600 Family of Security Controllers

To assist designers' ever-increasing need for physical security while reducing size, cost, and power consumption, Maxim/Dallas Semiconductor announced the first in a series of security controllers that specifically addresses the needs of increased physical hardware protection. The DS3600 product family gives embedded-systems designers the ability to add the additional layers of security required for present and emerging certification requirements.

These devices have sophisticated temperature monitoring for extremely low-leakage current comparators, protection against cryogenic attacks, time-keeping and tamper-logging functions, and a host of other functions required by cryptographic subsystems (**Figure 1**). At the hub of this array of functionality lies a unique memory-cell structure intended to further protect top-level encryption keys and security certificates. Traditional memory-cell technology is subject to phenomena called data imprinting, which refers to a memory cell's trait of leaving remnants of previously stored information. These remnants can be extracted through a variety of attack scenarios. The DS3600's internal nonimprinting memory is the first device of its kind to eliminate this common point of attack. Additionally, the entire memory array can be erased with a single hardware command instantaneously. This security controller's combination of functionality dramatically reduces power consumption and no longer requires host processor intervention for the protection of encryption key memory.

In many cases, the highly integrated features found in this family of controllers have replaced the functionality of over 40 discrete components. While reducing size and cost at a fraction of the power traditionally required, the DS3600 family can virtually eliminate the need for other expensive components such as secure microprocessors. This allows manufacturers of embedded systems based upon non-secure processor architectures to achieve certification and retain large intellectual property software assets. Because these devices have been designed to meet certification, they provide the most assistance for designers who must now produce the necessary documentation for product certification.

Appendix 1—Classification Taxonomy

To determine the level of security required, IBM® presented a classification taxonomy over a decade ago that is still used today to describe potential attack classifications.

Class I (Clever Outsiders)

- Often very intelligent
- Have insufficient knowledge of the system
- May have access to moderately sophisticated equipment
- Typically attack a weakness in the system, rather than create one

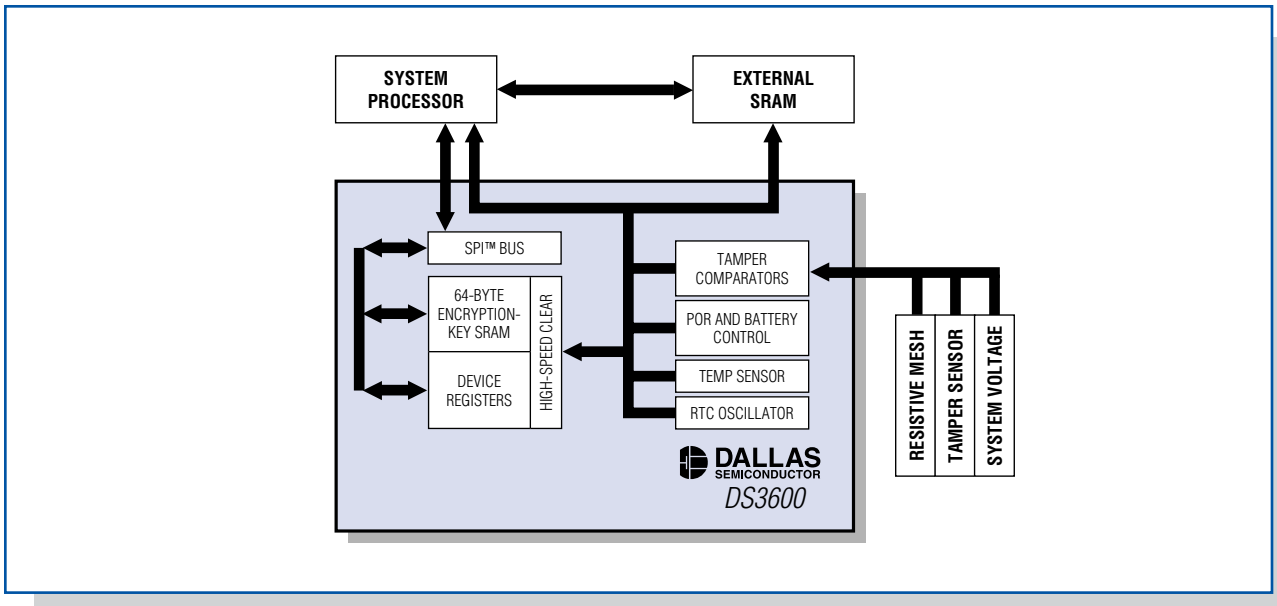


Figure 1. The tamper-resistant DS3600 controller features extremely high-impedance comparators to provide continuous low-power system monitoring and meet the highest level Common Criteria requirements.

Class II (Knowledgeable Insiders)

- Have substantial specialized technical education and experience
- Have some system knowledge, but potential access to most of it
- Often have access to sophisticated tools and instruments for analysis

Class III (Funded Organizations)

- Possess nearly unlimited funding resources
- Able to assemble teams of specialists
- Able to acquire or gain access to the most advanced analysis tools
- Capable of in-depth analysis and design of sophisticated attacks
- May recruit Class II knowledgeable insiders as part of the attack team

At a minimum, a system designer seeking to achieve certification should be able to describe the threats associated with at least the following common attack scenarios.

Physical Attacks

- Package intrusion
  - Cutting, etching, and ion or laser drilling
  - Reverse engineering (requires several sample devices)
    - Generating circuit schematics
    - Extracting ROM code
    - Identifying physical location of key circuit elements (i.e., memory)
  - Gaining Access to Memory
    - Alter circuitry with an FIB workstation
    - Alter the state of specific transistors with ionizing radiation
    - Microprobing
    - Advanced spectrographic analysis of memory-cell oxides

Noninvasive Attacks

- Ionizing radiation and thermal/cryogenic
- Induced voltage fluctuations and clock disturbance
- Differential power analysis

Appendix 2—Common Certifications/ Standards

NIST FIPS 140-2 Levels 1 to 4

- CESG ITSEC E1 to E6
- Common Criteria EAL1 to EAL7
- EMV 4.1 Levels 1 to 2 (Primarily Used in Banking/POS)
- ZKA (Primarily Used in Banking/POS)
- PCI PED (Primarily Used in Banking/POS PIN Entry

Industry Moving Towards "Common Criteria" Unification

- Various protection profiles, security targets, and schemes can exist
  - UK EN45011:1998
  - ISO 15408
  - Trusted computer group provides additional protection profiles
  - IBM Trusted Mobile Platform security

These and other standards bodies are summarized below along with a brief description of related security levels.

NIST FIPS 140-2

FIPS 140-2 defines four levels of security assurance, from lowest to highest, with each level building on the previous one.

Level 1 means that the product properly implements the NIST standardized cryptographic algorithms, including data encryption standard (DES), triple DES (3DES), and advanced encryption standard (AES).

Level 2 means that the product has tamper-evident coatings to ensure that any corruption of the device would be noticeable.

Level 3 is for cryptographic modules that delete stored keys if the modules detect a physical attack on circuit components. At Level 3, the product must require authenticated access.

Level 4 requires that a product provide protection from attacks that attempt to thwart physical access controls, such as supercooling.

Most security products receive FIPS 140-2 Level 2 or Level 3 certification, either of which is sufficient as long as the modules are contained in a controlled environment.

Common Criteria

Common Criteria uses a scale called evaluation assurance level (EAL). This is an assessment that says that the product meets the functional requirements stated in the security target and protection profile documents. These documents are prepared by the vendor and evaluated by the Common Criteria evaluator. EAL levels range from EAL1 to EAL7, with most products receiving Common Criteria certification of EAL4 and below.

EAL1 Product meets the basic requirements.

EAL7 Product meets the requirements for exceptionally secure environments.

EAL5, 6, and 7 certifications are extremely stringent, requiring evaluation of the development process and theoretical framework, as well as functional tests.

An EAL rating is meaningless without first evaluating the security target and protection profile documentation.

A similar article appeared in the October 2006 issue of Embedded Systems Europe.

Selecting a Serial Bus

The heart of today's advanced electronic products is a microcontroller (µC) that communicates with one or more peripheral devices. Initially, µC periphery was memory mapped and connected to the data and address bus. Chip-select signals were decoded from address lines to give each component its unique location in the limited address range. This type of interface determined the minimum number of pins (in addition to power and ground) to 8 (data) plus 1 (R/$\overline{W}$) plus 1 ($\overline{CS}$) plus n address lines [n = log2(number of internal registers or memory bytes)]. A 16-byte device, for example, needed 8 + 1 + 1 + 4 = 14 pins for communication. The access time was short, but the high pin count increased the package size and the overall cost. The obvious alternative to decrease cost and package size is a serial interface.

Defining a serial bus is not a trivial task. Besides data rate, bit sequence (most or least significant bit first), and voltage, one needs to consider the following:

- How the peripheral device gets selected (by hardware through the chip-select input, or by a software protocol).
- How the peripheral device stays synchronized with the µC (through a hardware clock line, or through clocking information embedded in the data stream).
- Whether data is transmitted on a single line (switching between "high" and "low") or a two-line differential connection (both lines changing their voltage simultaneously, but in opposite direction).
- Whether both ends of the communication line are electrically terminated with a matching impedance (typical with differential signaling), or whether they are left unterminated or terminated at one end only (typical with single-ended buses).

Table 1 shows the matrix of variations using popular bus systems. Only 4 of the possible 16 combinations are currently known commercial products.

Beyond these parameters, the application can add further requirements such as the method of power delivery, isolation, noise immunity, the maximum distance between the µC (master) and the peripheral device (slave), or the structure of the cabling (linear, star, insensitive to reversal of wires). These requirements lead to applications such as building automation, industrial control, and reading of utility meters for which special standards have been developed.[1, 2]

Requirements for Applications from Circuit Board to Backplane

A serial bus system for peripheral functions must not add any significant burden on the system. In particular,

- The connection must be easy to route (the fewer signals the better).
- The protocol must be easy to implement in software (or natively supported by the chosen µC/µP).
- There should be an adequate selection of device functions.
- The bus must be easy to expand.

The fewest number of signals is required with single-ended self-clocking systems that use a software protocol for addressing. As shown in Table 1, 1-Wire®, LIN bus, and SensorPath™ meet these criteria. Within this group there are additional factors to consider (see **Table 2**).

Table 1. Serial Bus Systems Overview

<table>
<tr><td></td><td colspan="4">ADDRESSING (SELECTION)</td><td></td></tr>
<tr><td>SYNCHRONIZATION</td><td colspan="2">PROTOCOL</td><td colspan="2">CHIP-SELECT LINE</td><td>IMPEDANCE</td></tr>
<tr><td rowspan="3">SELF-CLOCKING</td><td>1-Wire,
LIN bus,
SensorPath</td><td></td><td></td><td></td><td>NOT MATCHED</td></tr>
<tr><td></td><td>RS-485, LVDS,
CAN, USB 2.0,
FireWire®</td><td></td><td></td><td rowspan="2">MATCHED</td></tr>
<tr><td rowspan="2">CLOCK LINE</td><td></td><td></td><td></td><td></td></tr>
<tr><td>I²C, SMBus™</td><td></td><td></td><td>SPI™,
MICROWIRE™</td><td>NOT MATCHED</td></tr>
<tr><td></td><td>SINGLE-ENDED</td><td>DIFFERENTIAL</td><td></td><td>SINGLE-ENDED</td><td></td></tr>
<tr><td></td><td colspan="4">TRANSMISSION MODE</td><td></td></tr>
</table>

Table 2. Further Distinctions Among 1-Wire, LIN Bus, and SensorPath Bus Systems

	1-Wire[3]	LIN Bus[4]	SensorPath[5]
Physical Network Size	Board or backplane, can be expanded up to ~300m	~40m	Board
Network Drivers (Hardware)	Drivers are available for RS-232, I^2C, USB, and general µP port pins[6, 7]	Drivers are available for µP port pins	Super-I/O chips, µP port pins
Network Drivers (Software)	Available free for various platforms, including µCs[8]	Available free for Freescale™ µCs	Not available
Power Supply	Through the data line (typical case), local V_{CC} (some devices)	Through the data line	Local V_{CC}
Data Rate	Up to ~15kbps (standard) or ~125kbps (overdrive)[9]	Up to ~20kbps	Data dependent, up to ~20kbps
Network Inventory	Through the "search ROM" network function	Not applicable, message-based addressing	Not supported
Choice of Device Functions	Large variety of device functions, including serial number, instrumentation, secure memories, etc.	Limited to functions needed in automotive applications	Limited to temperature sensors and voltage ADCs

Physical Network Size

Only SensorPath is limited to board-size applications. Under certain conditions and using appropriate hardware and software network drivers, the size of a 1-Wire bus can be expanded significantly.

Network Drivers

For protocol-based networks, one needs software drivers to generate the communication waveforms (link layer), to identify and address an individual slave/node in the network (network layer), and to transmit/receive data to or from a device (transport layer). Software drivers are specific for an operating system and communication port. There are 1-Wire hardware driver chips (masters) and adapters for ports such as COM, LPT, USB, and I^2C. For large unterminated networks, reflections from cable ends, connectors, and stubs can limit the performance.

Power Supply

Each device in a network must be powered for operation. Most cost effective is a remote supply accessed through the data line. This method, also called "parasite power," makes it possible to read system diagnostic information (e.g., in power-down mode). For an example, refer to Figure 3 and the related text in Application Note 178: *Printed Circuit Board Identification Using 1-Wire Products*.[10] Parasite power, however, reduces the achievable data rate, as time must be set aside for power delivery.

Data Rate

Generally, a higher data rate is associated with a reduced network size and vice versa. In a 1-Wire system, due to the power-delivery feature, the maximum data rate depends on the number of slave devices in a network and the overall length (capacitance) of the cable.

Network Inventory

This feature allows the master to identify the number, type, and addresses of slave devices in a network. It is a prerequisite for networks with a dynamic (changing) population. Refer to page 22 of the *Dallas Engineering Journal* (vol. 2)[11] for an example.

Choice of Device Functions

The best interface is useless if the device functions required for an application are not available. Compared to LIN bus and SensorPath, 1-Wire has by far the largest selection of functions.

I²C/SMBus vs. 1-Wire

If the application can support a clock line, then the choice can be extended to I²C[12] and SMBus[13] devices. In its initial specification, the SMBus was mostly a variation of the original 100kbps I²C bus specification with a timeout feature added. This timeout prevents the bus from becoming inoperable from a node that has lost synchronization with the bus driver; an I²C system requires a power-on reset to recover from this situation. In 1-Wire systems, the reset/presence-detect cycle resets the communication interface to a defined starting condition. Besides the clock line, I²C/SMBus uses an acknowledge bit for every byte that is communicated on the bus. This reduces the net data rate by 12%. Transactions begin with a start condition followed by a device address and a data-direction bit (read or write), and they end with a stop condition. In 1-Wire systems, the requirements of the network layer must first be met (i.e., selecting a particular device or search ROM or broadcast); subsequent communication begins with a device-specific command code, which also affects the data direction (read or write).

A serious issue of the original I²C and SMBus is the limited 7-bit address space. With more than 127 different device types available, one cannot deduct the device function from its slave address. In addition, many I²C devices allow the user to set one or more address bits arbitrarily to have several equal devices on the bus. This feature also reduces the available address space. The standard method to work around address conflicts is splitting a bus into several segments and activating one segment at a time under software control. This segmentation requires more hardware and complicates the application firmware. The lack of an inventory function or enumeration makes it difficult for an I²C system to handle a dynamic population. This issue is solved with the Address Resolution Protocol of *SMBus Specification Version 2.0*.[13] However, there are only few SMBus devices available that support this feature.

SPI and MICROWIRE

SPI[14] and MICROWIRE[15], a subset of SPI, require an additional chip-select line for each device. Due to the chip-select signal, the SPI protocol only defines commands such as read and write for memory addresses and the status register. It does not use an acknowledge function. Typically, SPI devices have different pins for data input and data output. Because the data output is tristated (disabled) for anything except read functions, the two data pins can be tied together to form a single bidirectional data line. SPI is chosen for functions that are not available in other bus systems or for its fairly high data rate, which may be 2Mbps or higher. A downside of SPI and MICROWIRE is the decoder that generates the $\overline{CS}$ signal to address an individual chip. However, there are no address conflicts. As with I²C, there is no inventory function. The master cannot deduct the device function from its logical address, which makes it difficult to manage a network with a dynamic population.

RS-485, LVDS, CAN, USB 2.0, and FireWire

These standards are discussed here as examples for differential signaling. The two fastest systems in this group, FireWire[16] and USB 2.0[17], are electrically point-to-point connections. Using sophisticated nodes or hubs, they implement a virtual bus of a tree-like topology where data packets are transmitted from source to endpoint (USB) or peer-to-peer (FireWire) at a burst data rate of up to 480Mbps (USB 2.0) or 1600Mbps (FireWire). The limited packet size and the receive/buffer/retransmit communication concept add latency, which in turn reduces the achievable data throughput. Topology and protocol permit a maximum of 126 nodes for USB and 63 nodes for FireWire with a maximum distance of 4.5m between nodes using passive cable. Designed for applications such as PC periphery, multimedia, industrial control, and aviation (FireWire only), USB and FireWire devices can be plugged in without powering down the system (hot-swapped). This allows the network's population to change dynamically.

LVDS[18], RS-485[19], and CAN[20] implement a true linear bus structure with masters and slaves or even multiple masters. The fastest of these standards, low-voltage differential signaling (LVDS), can operate at 100Mbps if the bus size does not exceed 10m. Depending on the network size, the achievable data rate and throughput can be higher or lower. Designed as the electrical standard for backplane applications, LVDS allows hot-swapping, but does not specify any protocol.

RS-485 also specifies only the electrical parameters. Instead of nodes, RS-485 defines loads and the maximum number of loads per bus, which is 32. One electrical node can have a load of less than 1. Typical data rates are up to 35Mbps at 12m and 100kbps at 1200m network size, which are adequate for data acquisition and control applications. The protocol of RS-485 equipment is often based on components originally designed for RS-232.

The controller area network (CAN), in contrast, defines a serial communications protocol for distributed real-time control with a very high level of security, geared towards automotive applications and industrial automation. The data rate ranges from a network size of 1Mbps at 40m down to 50kbps at 1000m. The addressing is message-based without any protocol-inherent limitation to the

number of nodes. CAN nodes can be hot-swapped for dynamic change of the network's population.

Summary

In the group of simple, low-cost bus systems, 1-Wire has the largest variety of device functions and network drivers as compared to LIN bus and SensorPath. I^2C and SMBus require a clock line and V_{CC} power in addition to data and ground reference, but offer an impressive choice of device functions. SPI and MICROWIRE need an additional chip-select line, but communicate at significantly higher data rates.

With its parasitic power supply and network inventory function, the 1-Wire interface and protocol support hot-swapping, a feature that is otherwise only found in high-speed systems that use differential signaling and in SMBus 2.0-compliant products. The best-known examples of hot-swapped 1-Wire devices are iButton® products, in which hot-swapping is the normal way of operation. 1-Wire devices have proven to be very efficient for functions such as global identification[21], circuit boards/accessory identification and authentication[10], temperature sensing, and actuation. Other very successful products are 1-Wire devices with secure memory and challenge-and-response functionality that protect intellectual property at a minimal cost through two-way authentication.[22, 23]

A similar article appeared in the September 2006 issue of Electronic Products.

References

1. Interbus Club. www.interbusclub.com/ (industrial automation)
2. The valid M-Bus standard. www.m-bus.com/ (meter reading)
3. "Overview of 1-Wire Technology and Its Use." www.maxim-ic.com/AN1796 (intro to 1-Wire)
4. LIN Local Interconnect Network. www.lin-subbus.org/ (LIN specification)
5. National Semiconductor. "Cost Effective Partitioning of IO and Management Functions in PCs - Introduction of SensorPath™ Technology." www.national.com/nationaledge/jan04/article.html (SensorPath)
6. "Advanced 1-Wire Network Driver." www.maxim-ic.com/AN244 (hardware driver)
7. "Guidelines for Reliable 1-Wire Networks." www.maxim-ic.com/AN148 (1-Wire networks)
8. "1-Wire Software Resource Guide." www.maxim-ic.com/AN155 (software drivers)
9. "Determining the Recovery Time for Multiple-Slave 1-Wire Networks." www.maxim-ic.com/AN3829 (recovery time)
10. "Printed Circuit Board Identification Using 1-Wire Products." www.maxim-ic.com/AN178 (board identification)
11. "Dallas Engineering Journal," vol. 2. pdfserv.maxim-ic.com/en/ej/DallasEJ2.pdf (dynamic network)
12. "The I^2C-Bus Specification, Version 2.1, January 2000." www.nxp.com/acrobat_download/literature/9398/39340011.pdf (I^2C)
13. "SMBus Specifications." www.smbus.org/specs/ (SMBus)
14. "M68HC11E Family." www.freescale.com/files/microcontrollers/doc/data_sheet/M68HC11E.pdf (SPI)
15. "MICROWIRE™ Serial Interface." www.national.com/an/AN/AN-452.pdf (MICROWIRE)
16. The Air Power Australia Website. "Firewire." www.ausairpower.net/OSR-0201.html (FireWire)
17. "USB 2.0 Specification." www.usb.org/developers/docs (USB specification)
18. National Semiconductor. "LVDS Owner's Manual: Low-Voltage Differential Signaling." www.national.com/appinfo/lvds/files/ownersmanual.pdf (LVDS)
19. Lammert Bies' Website. "RS485 serial information." www.lammertbies.nl/comm/info/RS-485.html (RS-485)

20a. Robert Bosch GmbH. "CAN Specification, Version 2.0." www.semiconductors.bosch.de/pdf/can2spec.pdf (CAN specification part A)

20b. CAN in Automation (CiA). "CAN Specification 2.0, Part B." www.can-cia.org/downloads/ciaspecifications/?269 (CAN specification part B)

21. "Creating Global Identifiers Using 1-Wire Devices." www.maxim-ic.com/AN186 (global identifier)
22. "Protecting the R&D Investment—Two-Way Authentication and Secure Soft-Feature Settings." www.maxim-ic.com/AN3675 (two-way authentication)
23. "Xilinx® FPGA IFF Copy Protection with 1-Wire SHA-1 Secure Memories." www.maxim-ic.com/AN3826 (FPGA protection)

Add Control, Memory, Security, and Mixed-Signal Functions with a Single Contact

Overview

The Dallas Semiconductor 1-Wire bus is a simple signaling scheme that performs half-duplex bidirectional communications between a host/master controller and one or more slaves sharing a common data line (**Figure 1**). Both power and data communication for slave devices are transmitted over this single 1-Wire line. For power delivery, slaves capture charge on an internal capacitor when the line is in a high state and then use this charge for device operation when the line is low during data transmission. A typical 1-Wire master consists of an open-drain I/O port pin with a resistor pullup to a 3V to 5V supply. More sophisticated masters, including dedicated line-driver solutions, are available from Dallas Semiconductor. This clever communication scheme also allows you to add memory, authentication, and mixed-signal functions at any time, easily and efficiently.

64-Bit Serial Numbers

There is an important, fundamental feature in every 1-Wire system: each slave device has a unique, unalterable (ROM), 64-bit, factory-lasered serial number (ID) that will never be repeated in another device. Besides providing a unique electronic ID to the end product, this 64-bit ID value allows the master device to select a slave device among the many that can be connected to the same bus wire. Part of the 64-bit ID is also an 8-bit family code that identifies the device type and functionality supported.

Data-Bit-Level Communication

The bus master initiates and controls all 1-Wire communication. As illustrated in **Figure 2**, the 1-Wire communication waveform is similar to pulse-width modulation, because data is transmitted by wide (logic 0) and narrow (logic 1) pulse widths during data-bit time periods or time slots. A communication sequence starts when the bus master drives a defined length "Reset" pulse that synchronizes the entire bus. Every slave responds to the Reset pulse with a logic-low "Presence" pulse. To write data, the master first initiates a time slot by driving the 1-Wire line low, and then either holds the line low (wide pulse) to transmit a logic 0 or releases the line (short pulse) to allow the bus to return to the logic 1 state. To read data, the master again initiates a time slot by driving the line with a narrow low pulse. A slave can then either return

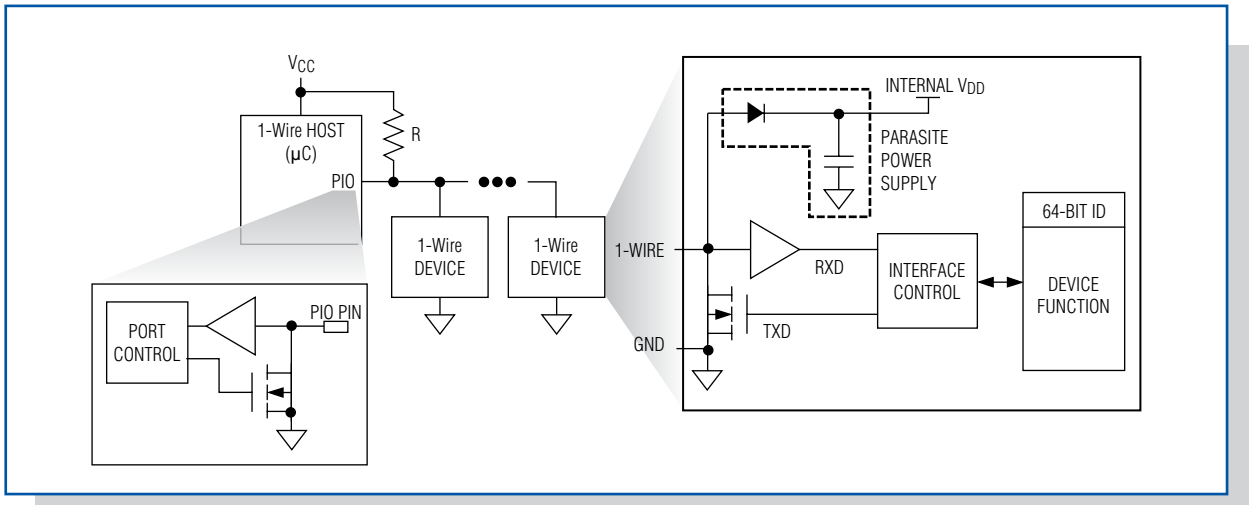


Figure 1. In a 1-Wire master/slave configuration, all devices share a common data line.

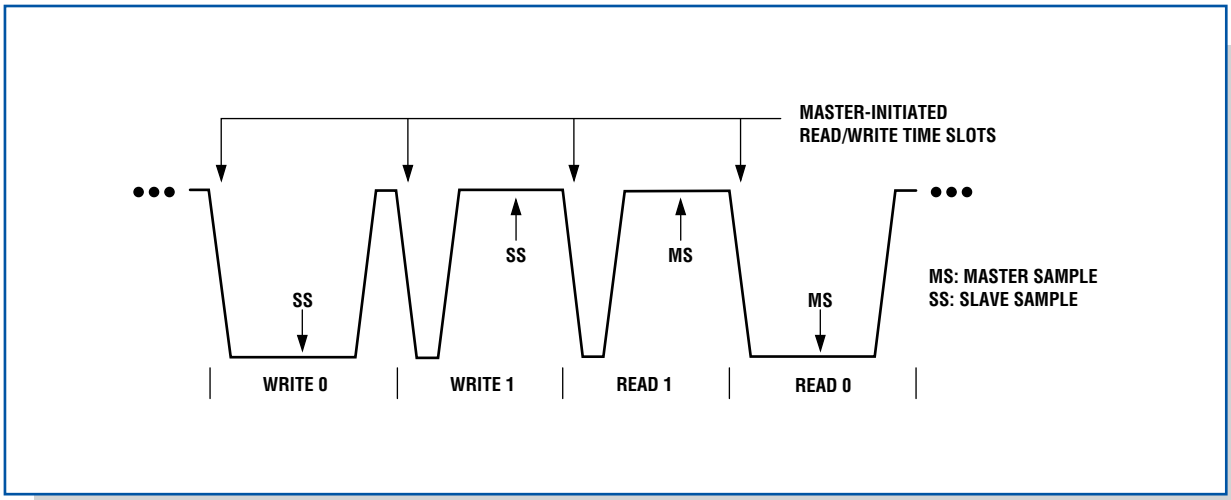


Figure 2. This waveform example shows master-initiated write/read of data bits with slave and master sampling points.

a logic 0 by turning on its open-drain output and holding the line low to extend the pulse, or a logic 1 by leaving its open-drain output off to allow the line to recover. Most 1-Wire devices support two data rates: Standard speed of about 15kbps, and Overdrive speed of about 111kbps. The protocol is self-clocking and tolerates long inter-bit delays, which ensures smooth operation in interrupted software environments.

Device Selection

The first action in a 1-Wire communication is selecting a slave device for subsequent communications. In a single slave-device environment, the selection sequence is minimal. In a multidevice environment, however, slave selection is done either by selecting all slaves or a specific slave targeted by its 64-bit ID. A binary search algorithm (described as ROM-level commands in 1-Wire data sheets) enables the bus master to "learn" and subsequently select the respective 64-bit ID of any slave device on the line. Once a specific slave is selected, the master issues device-specific commands and sends data to it, or reads data from it. Meanwhile, all the other slave devices ignore communications until the next Reset pulse is issued.

Summary

Layered on these 1-Wire fundamentals are a variety of memory, digital, analog, and mixed-signal functions. This variety results in a product portfolio optimized for applications where the single-contact 1-Wire interface can solve an interconnect-constrained problem and/or add value with unique product-line features. The 1-Wire products are available in standard IC packaging and the Company's rugged, stainless steel iButton package. Products, packaging, and extensive software support are detailed at www.maxim-ic.com/1-Wire.