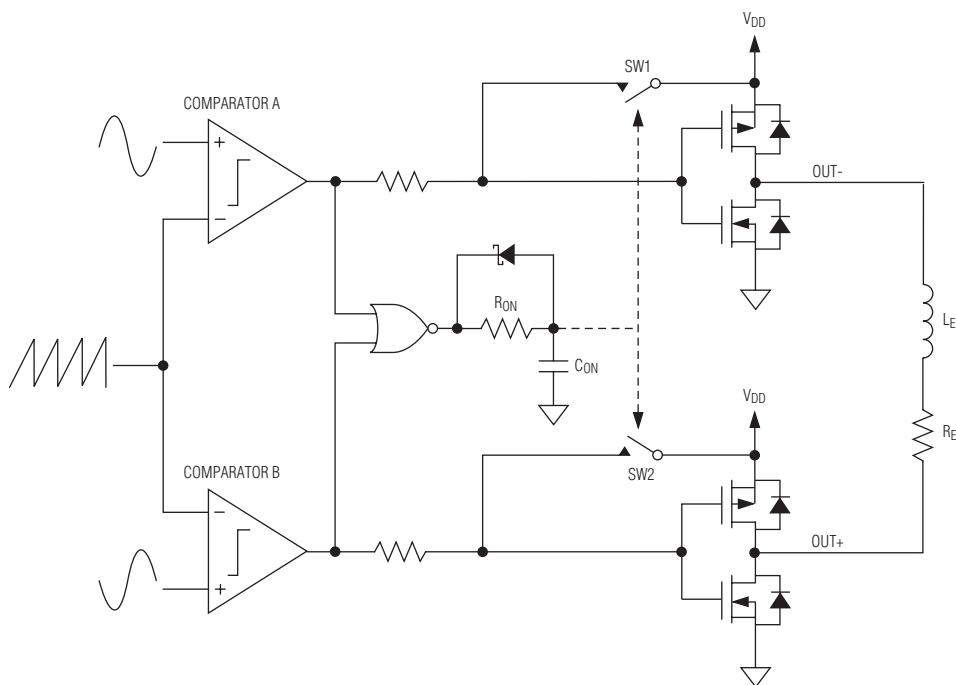


新闻简报		2
探讨文章	D类放大器：基本原理和近期发展	3
	嵌入式安全系统的发展趋势	10
	选择串行总线	14
设计实例	通过单个触点增加控制、存储器、安全和混合信号功能	18



该简化功能框图展示了MAX9700免滤波器D类调制器的拓扑。(见第8页)

新闻简报

Maxim公布2007财年第一季度的收入和收益

Maxim Integrated Products, Inc. (MXIM)公布，截至2006年9月23日的财务第一季度净收入达到502.7百万美元，比2006财年第四季度降低1.5%，比2006财年第一季度增长18.5%。

包括基于股票的补偿支出在内，2007财年第一季度的净盈利为107.5百万美元，或摊薄后每股收益0.33美元。相比2006财年第四季度，对应的净盈利为124.3百万美元，或摊薄后每股收益0.37美元；包括基于股票的补偿支出在内，去年同期的净盈利为105.4百万美元，或每股收益0.31美元。

第一季度的研发费用为130.2百万美元，或净收入的25.9%。相比2006财年第四季度，对应的研发费用为127.2百万美元，或净收入的24.9%。研发费用增长主要是由于新增的员工数量及其相关费用造成的，以支持未来产品的开发。

销售、日常行政开支为40.1百万美元，或净收入的8.0%。相比2006财年第四季度，对应的支出为37.9百万美元，或净收入的7.4%。销售、日常行政开支的增长主要是由于审计公司股票期权计划所支付的3.0百万美元。

第一季度的总运营利润为150.8百万美元，或净收入的30.0%，相比2006财年，第四季度为173.3百万美元，或净收入的34.0%；第一季度为145.8百万美元，或净收入的34.4%。

我们的税率增加了2个百分点，因为当地额外收入的课税减免政策正被当地生产减免政策所取代，新政策在若干年内分阶段实施，美国政府不再延续研发赋税优惠政策。这直接导致净收入降低3.3百万美元，或摊薄后每股收益降低0.01美元。

本季度，公司以60.8百万美元回购了约2.1百万股自己的普通股，支付了50.0百万美元的股息，并采购了94.9百万美元的固定设备，现金及约当现金增加了51.4百万美元，达到14亿美元。第一季度应收账款降低0.8百万美元，达到291.7百万美元。考虑了15.6百万美元基于股票的补偿后，本季度的库存增加10.6百万美元，达到217.9百万美元。

Gifford先生评论道：“公司董事会已宣布2007财年第二季度的现金股息为0.156美元每股。将于2006年12月5日向2006年11月21日登记的股东付讫。”

D类放大器： 基本工作原理和 近期发展

D类放大器的高效特性，使其成为便携式和大功率应用的理想选择。传统D类放大器需要一个外部低通滤波器，以从脉宽调制信号(PWM)输出波形中提取音频信号。然而，许多现代D类放大器采用先进的调制技术，可使各种应用免去外部滤波器并降低电磁干扰(EMI)。省掉外部滤波器不仅降低了电路板空间要求，同时大幅降低了很多便携式/紧凑型应用的成本。

引言

大多数音频系统设计工程师都非常清楚，D类放大器与线性音频放大器(如A类、B类和AB类)相比，在功效上有相当的优势。对于线性放大器(如AB类)来说，偏置元件和输出晶体管的线性工作方式会损耗大量功率。因为D类放大器的晶体管只是作为开关使用的，用来控制流过负载的电流方向，所以输出级的功耗极低。D类放大器的功耗主要来自输出晶体管导通阻抗、开关损耗和静态电流开销。放大器的功耗主要以热量的形式耗散。D类放大器对散热器的要求大为降低，甚至可省掉散热器，因此非常适用于紧凑型大功率应用。

过去，基于PWM方式的典型D类放大器需要外部滤波元件，会产生EMI/EMC兼容性问题，并且THD+N性能较差，因此与线性放大器相比，它的高效优势大为失色。然而，最新一代的D类放大器采用先进的调制和反馈技术，可很好地缓解上述问题。

D类放大器基础

现代D类放大器使用多种调制器拓扑结构，而最基本的拓扑组合了脉宽调制(PWM)以及三角波(或锯齿波)振荡器。图1给出一个基于PWM的半桥式D类放大器简化框图。它包括一个脉宽调制器，两个输出MOSFET，和一个用于恢复被放大的音频信号的外部低通滤波器(L_F 和 C_F)。如图所示，p沟道和n沟道MOSFET用作电流导向开关，将其输出节点交替连接至 V_{DD} 和地。由于输出晶体管使输出端在 V_{DD} 或地之间切换，所以D类放大器的最终输出是一个高频方波。大多数D类放大器的开关频率(f_{SW})通常在250kHz至1.5MHz之间。音频输入信号对输出方波进行脉宽调制。音频输入信号与内部振荡器产生的三角波(或锯齿波)进行比较，可得到PWM信号。这种调制方式通常被称作“自然采样”，其中三角波振荡器作为采样时钟。方波的占空比与输入信号电平成正比。没有输入信号时，输出波形的占空比为50%。图2显示了不同输入信号电平下所产生的PWM输出波形。

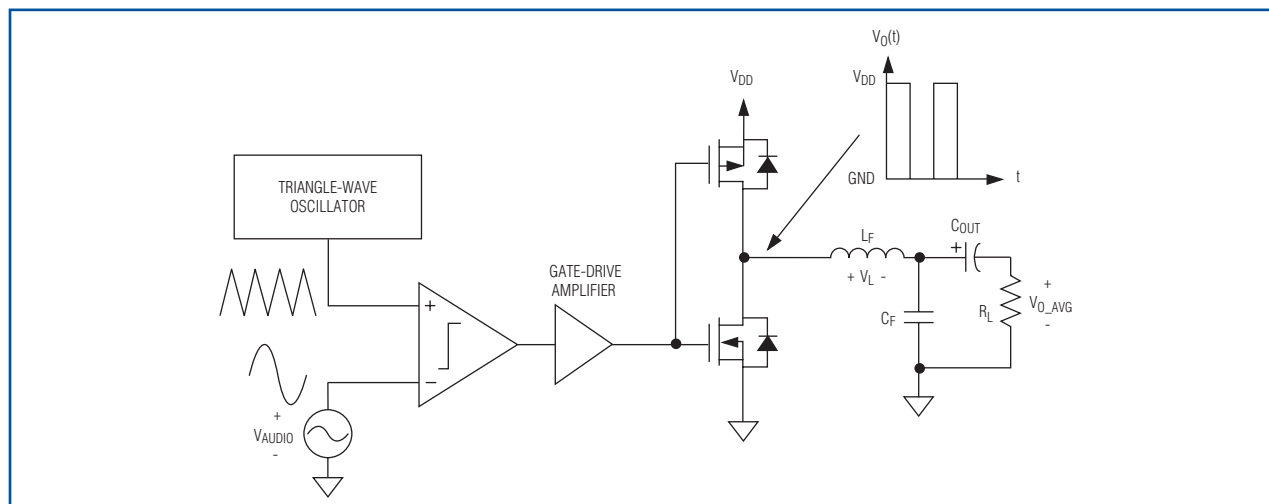


图1. 该简化功能框图展示了一个基本的半桥式D类放大器的结构。

为了从PWM波形中提取出放大后的音频信号，需将D类放大器的输出送入一个低通滤波器。图1中的LC低通滤波器作为无源积分器(假设滤波器的截止频率比输出级的开关频率至少低一个数量级)，它的输出等于方波的平均值。此外，低通滤波器可防止在阻性负载上耗散高频开关能量。假设滤波后的输出电压(V_{O_AVG})和电流(I_{AVG})在单个开关周期内保持恒定。这种假设较为准确，因为 f_{SW} 比音频输入信号的最高频率要高得多。因此，占空比与滤波后的输出电压之间的关系，可通过对电感电压和电流进行简单的时间域分析得到。

流经电感的瞬时电流为：

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

其中， $V_L(t)$ 是图1中使用符号法则后的电感瞬时电压。由于流入负载的平均电流(I_{AVG})在单个开关周期内可以看作是恒定的，所以开关周期(T_{SW})开始时的电感电流必定与开关周期结束时的电感电流相同，如图3所示。

借助数学术语，可用以下等式表示：

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

等式2表明，电感电压在一个开关周期内的积分必定为0。利用等式2并观察图3给出的 $V_L(t)$ 波形，可以看出，各区域面积(A_{ON} 和 A_{OFF})的绝对值只有彼此相等，等式2才能成立。基于这一信息，我们可以利用开关波形占空比来表示滤波后的输出电压：

$$A_{ON} = |A_{OFF}| \quad (\text{等式3})$$

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

$$A_{OFF} = V_O \times t_{OFF} \quad (\text{等式5})$$

将等式4和5代入等式3，得到以下等式：

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

最后，得到 V_O 的表达式：

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

式中D是输出开关波形的占空比。

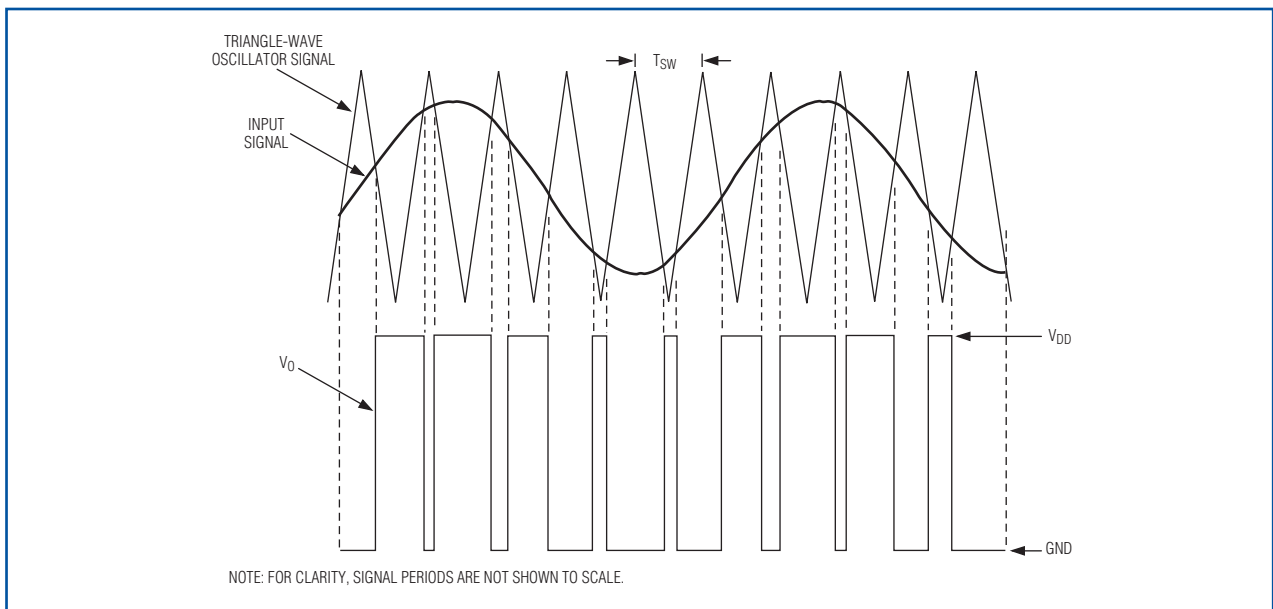


图2. 输出信号脉宽与输入信号幅值成正比。

利用反馈改善性能

许多D类放大器采用PWM输出至器件输入的负反馈环路。闭环方案不仅可以改善器件的线性，而且使器件具备电源抑制能力。开环放大器却正相反，它的电源抑制能力微乎其微(如果有的话)。在闭环拓扑中，因为会检测输出波形并将其反馈至放大器的输入端，

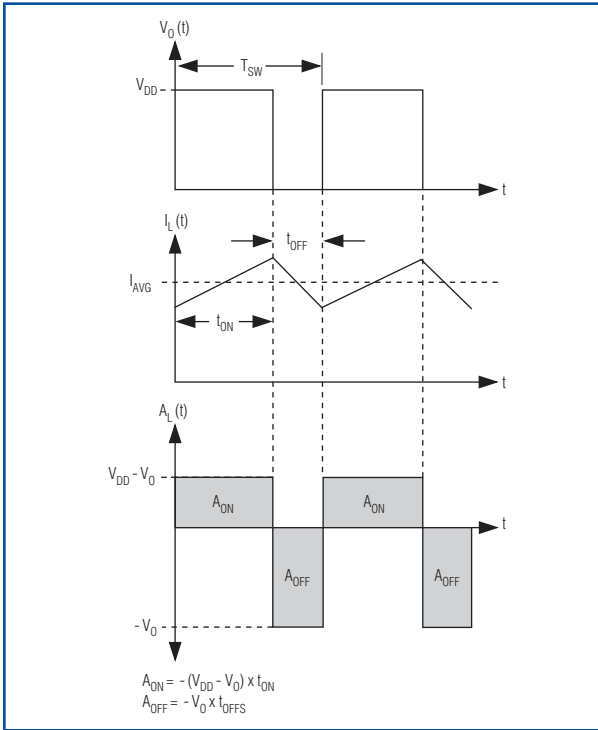


图3. 基本的半桥式D类放大器中，滤波器电感电流和电压波形。

所以能够在输出端检测到电源的偏离情况，并通过控制环路对输出进行校正。闭环设计的优势是以可能出现的稳定性问题为代价的，这也是所有反馈系统共同面临的问题。因此必须精心设计控制环路并进行补偿，确保在任何工作条件下都能保持稳定。

典型的D类放大器采用具有噪声整形功能的反馈环路，可极大地降低由脉宽调制器、输出级以及电源电压偏离的非线性所引入的带内噪声。这种拓扑与用在 Σ - Δ 调制器中的噪声整形类似。为阐明噪声整形功能，图4给出了一个1阶噪声整形器的简化框图。反馈网络通常包含一个电阻分压网络，但为简便起见，图4的反馈比例为1。由于理想积分器的增益与频率成反比，图中积分器的传递函数也被简化为 $1/s$ 。同时假定PWM模块具有单位增益，并且在控制环路中具有零相位偏移。使用基本的控制模块分析方法，可得到以下输出表达式：

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

由等式8可知，噪声项 $E_n(s)$ 与一个高通滤波器函数(噪声传递函数)相乘，而输入项 $V_{IN}(s)$ 与一个低通滤波器函数(信号传递函数)相乘。噪声传递函数的高通滤波器对D类放大器的噪声进行整形。如果输出滤波器的截止频率选取得当，大部分噪声会被推至带外(图4)。上述例子使用的是1阶噪声整形器，而多数现代D类

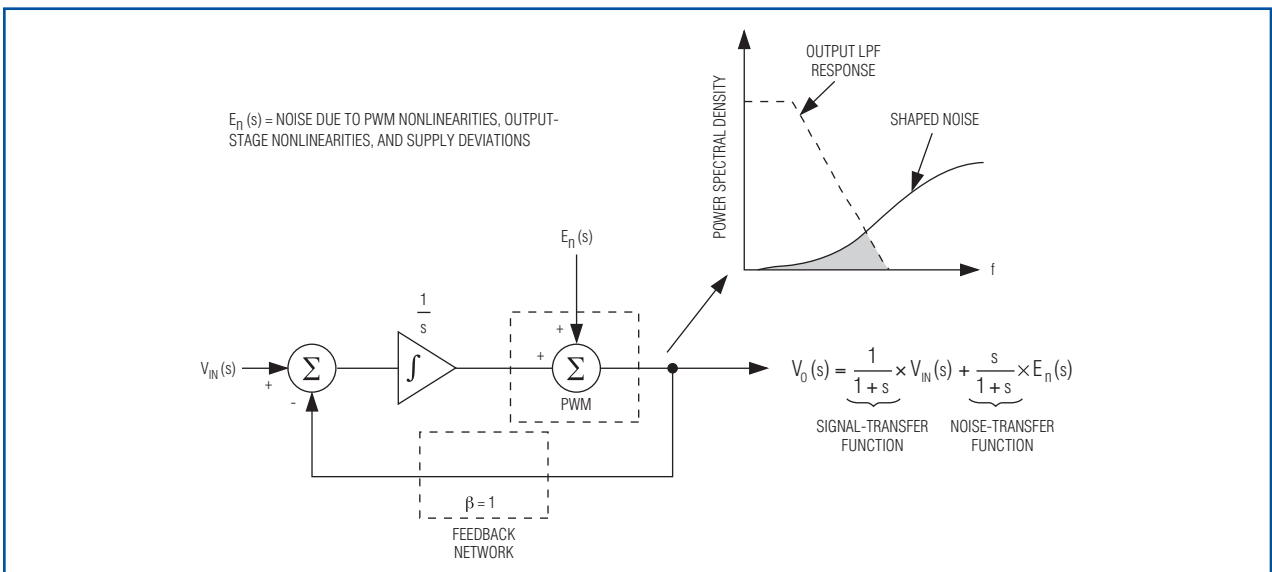


图4. D类放大器的控制环路包含1阶噪声整形电路，可将大部分噪声推至带外。

放大器采用高阶噪声整形拓扑，以便进一步优化线性度和电源抑制特性。

D类拓扑——半桥与全桥

很多D类放大器还会使用全桥输出级。全桥电路使用两个半桥输出级，并以差分方式驱动负载。这种负载连接方式通常称为桥接负载(BTL)。如图5所示，全桥结构是通过转换负载的导通路径来工作的。因此负载电流可以双向流动，无需负电源或隔直电容。

图6展示了传统的、基于PWM的BTL型D类放大器输出波形。在图6中，各输出波形彼此互补，从而在负载两端产生一个差分PWM信号。与半桥式拓扑类似，输出端需要一个外部LC滤波器，用于提取低频音频信号并防止在负载上耗散高频能量。

全桥式D类放大器除具有与AB类BTL放大器相同的优点外，还具有高效特性。BTL放大器的第一个优点是，采用单电源供电时输出端不需要隔直电容。半桥式放大器则不然，因为它的输出会在 V_{DD} 与地之间摆动，空闲时占空比为50%。这意味着它的输出具有约 $V_{DD}/2$ 的直流偏移。全桥式放大器中，这个偏移会出现在负载的两侧，输出端的直流电流为零。它们具有的第二个优点是，在相同的电源电压下，输出信号摆幅是半桥式放大器的2倍，因为负载是差分驱动的。在相同电源电压下，理论上它可提供的最大输出功率是半桥式放大器的4倍。

然而，全桥式D类放大器所需的MOSFET开关个数也是半桥式拓扑的2倍。一些人会认为这是它的缺点，因为更多的开关意味着会产生更多的传导和开关损耗。然而，这仅对于大功率输出的放大器(> 10W)是正确的，因为它们需要更高的输出电流和电源电压。因此，半桥式放大器往往凭借其在效率上的微弱优势而被大功率设备所采用。大多数大功率的全桥式放大器在驱动 8Ω 负载时，功效在80%到88%之间。然而，当每个通道向 8Ω 负载注入高于14W的功率时，类似MAX9742的半桥式放大器可获得90%以上的效率。

省去输出滤波器——免滤波器调制器

传统D类放大器的一个主要缺点就是它需要外部LC滤波器。这不仅增加了方案总成本和电路板空间，也可能因滤波元件的非线性而引入额外失真。幸好，很多现代D类放大器采用了先进的“免滤波器”调制方案，从而省掉或至少是最大限度降低了外部滤波器要求。

图7给出了MAX9700免滤波器调制器拓扑的简化功能框图。与传统的PWM型BTL放大器不同，每个半桥都有自己专用的比较器，从而可独立控制每个输出。调制器由差分音频信号和高频锯齿波驱动。当两个比较器输出均为低电平时，D类放大器的每个输出均为高。与此同时，或非门的输出变为高电平，但会因为 R_{ON} 和 C_{ON} 组成的RC电路而产生一定延时。一旦或非门延时输出超过特定门限，开关SW1和SW2随即闭合。这将使OUT+和OUT-变为低，并保持到下个采样周期的开始。这种设计使得两个输出同时开通一段最短时间($t_{ON(MIN)}$)，这个时间由 R_{ON} 和 C_{ON} 的值决定。如图8所示，输入为零时，两个输出同相并具有 $t_{ON(MIN)}$ 的脉冲宽度。随着音频输入信号的增加或减小，其中一个比较器会在另一个之前先翻转。这种工作特性外加最短时间导通电路的作用，将促使一个输出改变其脉冲宽度，另一个输出的脉冲宽度保持为 $t_{ON(MIN)}$ (图8)。这意味着每个输出的平均值都包含输出音频信号的半波整流结果。对两路输出的平均值进行差值运算，便可得到完整的输出音频波形。

由于MAX9700的输出端在空闲时为同相信号，所以负载两端没有差分电压，从而最大限度降低了静态功耗，并且无需外部滤波器。Maxim的免滤波器D类放大器从输出中提取音频信号时并不依靠外部LC滤波器，而是依靠扬声器负载固有的电感以及人耳的听觉特性来恢复音频信号。扬声器电阻(R_E)和电感(L_E)形成一个1阶低通滤波器，其截止频率为：

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

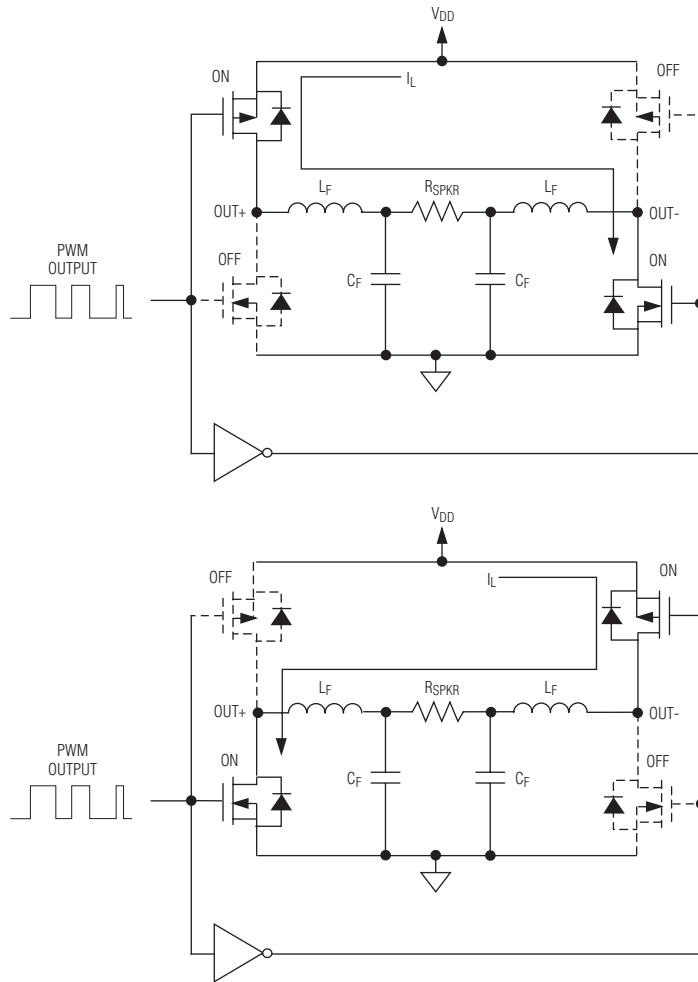


图5. 传统的全桥式D类输出级，使用两个半桥输出级对负载进行差分驱动。

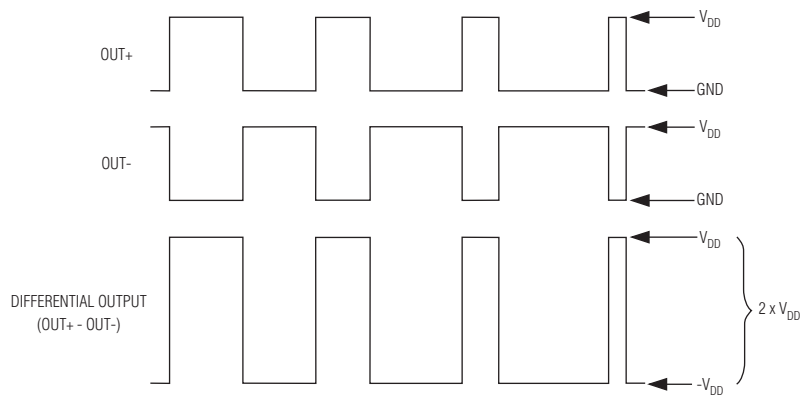


图6. 传统的全桥式D类输出波形彼此互补，在负载两端产生一个差分PWM信号。

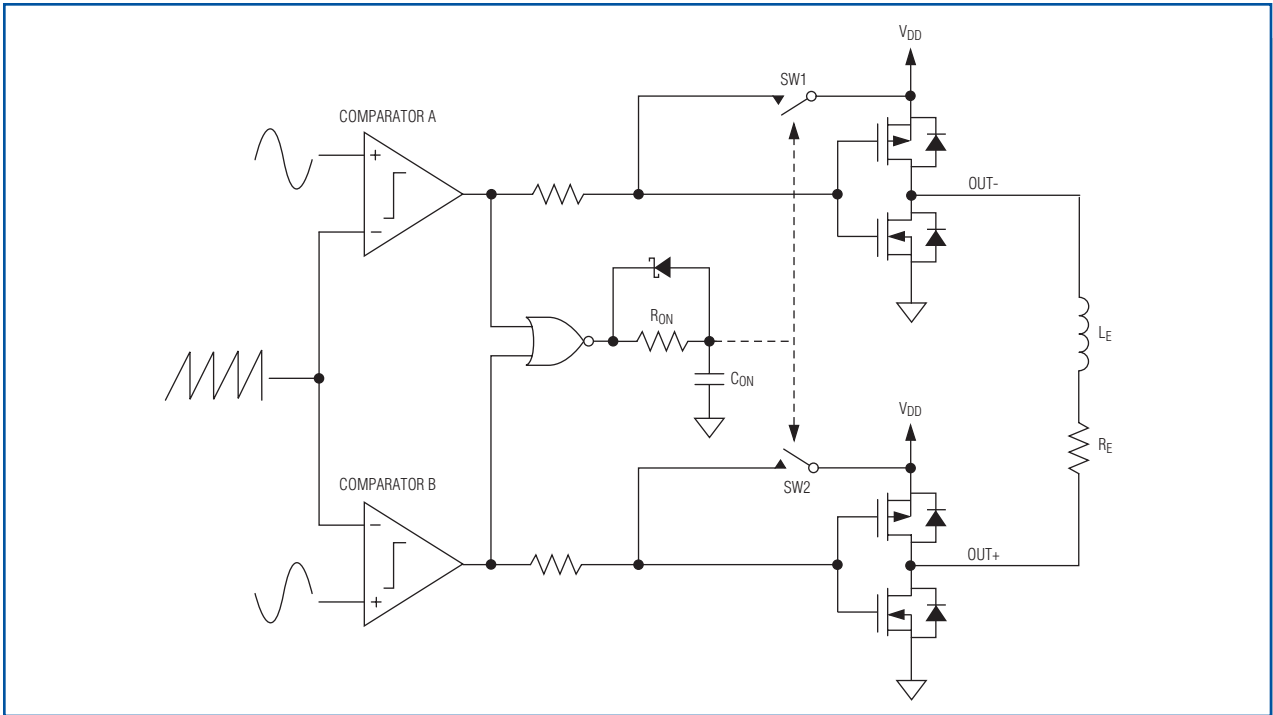


图7. 该简化功能框图展示了MAX9700免滤波器D类调制器的拓扑。

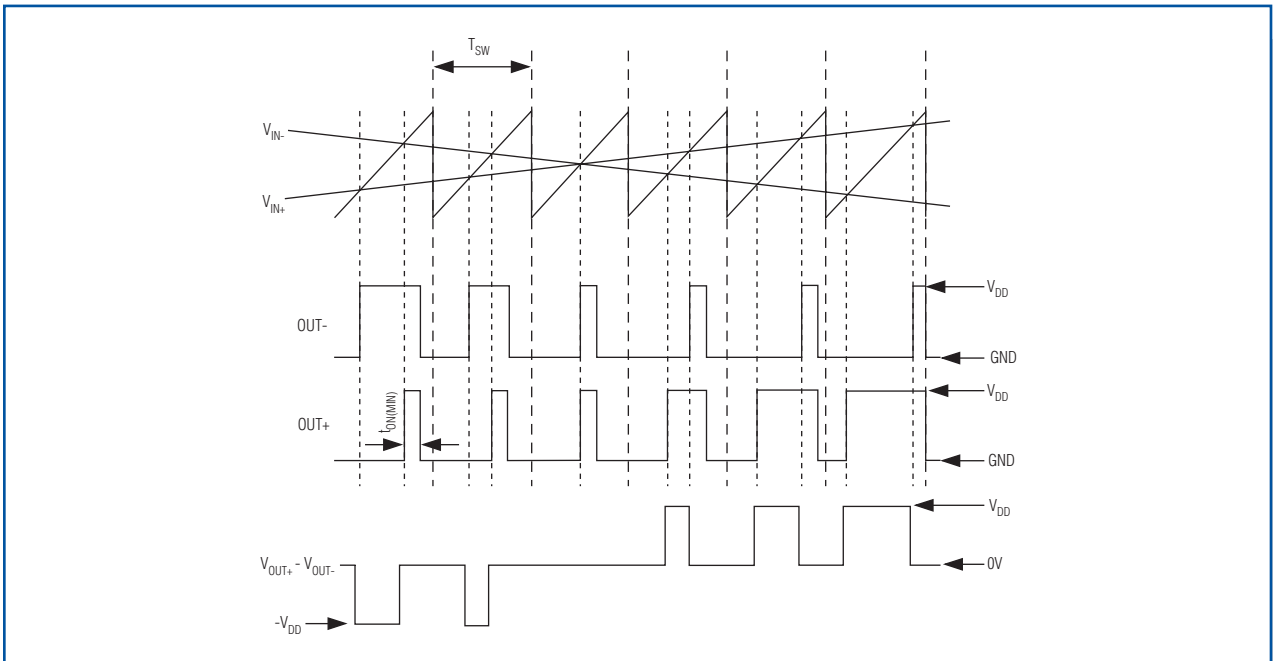


图8. MAX9700免滤波器调制器拓扑的输入和输出波形。

对大多数扬声器而言，这个1阶滚降足以恢复音频信号，并可防止在扬声器电阻上耗散过多高频开关能量。即使依然存在残余开关能量使扬声器组件产生运动，

这些频率也无法被人耳听到或影响听觉感受。使用免滤波器D类放大器时，为获得最大输出功率，扬声器负载应保证在放大器开关频率下仍为感性负载。

扩谱调制使EMI最小化

免滤波器工作方式的一个缺点就是可能通过扬声器电缆辐射EMI。由于D类放大器的输出波形为高频方波，并具有陡峭的过渡边沿，因此输出频谱会在开关频率及开关频率倍频处包含大量频谱能量。在紧靠器件的位置没有安装外部输出滤波器的话，这些高频能量就会通过扬声器电缆辐射出去。Maxim的免滤波器D类放大器采用享有专利的扩谱调制*方案，可帮助缓解可能的EMI问题。

通过抖动或随机化D类放大器的开关频率实现扩谱调制。实际开关频率相对于标称开关频率的变化范围可达到 $\pm 10\%$ 。尽管开关波形的各个周期会随机变化，但占空比不受影响，因此输出波形可以保留音频信息。图9a和图9b显示了MAX9700的宽带输出频谱，可以看到扩谱调制的效果。扩谱调制有效展宽了输出信号的频谱能量，而不是使频谱能量集中在开关频率及其各次谐波上。换句话说，输出频谱的总能量没有变，只是重新分布在更宽的频带内。这样就降低了输出端的高频能量峰，因而将扬声器电缆辐射EMI的机会降至最少。虽然一些频谱噪声可能由扩谱调制引入音频带宽内，这些噪声可以被反馈环路的噪声整形功能抑制掉。

Maxim的很多免滤波器D类放大器还允许开关频率同步至一个外部时钟信号。因此用户可以将放大器开关频率设置到相对不敏感的频率范围内。

尽管扩谱调制极大地改善了免滤波器D类放大器的EMI性能，为了满足FCC或CE辐射标准，实际上还是需要扬声器电缆长度加以限制。如果设备因扬声器电缆过长而没能通过辐射测试，则需要一个外部输出滤波器来衰减输出波形的高频分量。对于许多具有适度扬声器电缆长度的应用来说，在输出端安装磁珠/滤波电容即可满足要求。EMI性能对布局也十分敏感，为确保满足适用的FCC和CE标准，必须严格遵循PCB布局原则。

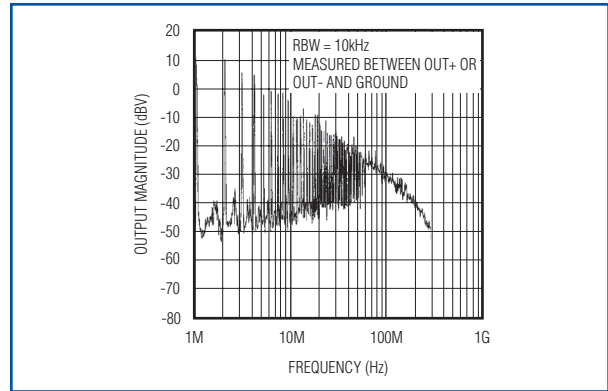


图9a. 固定开关频率下MAX9700的宽带输出频谱。

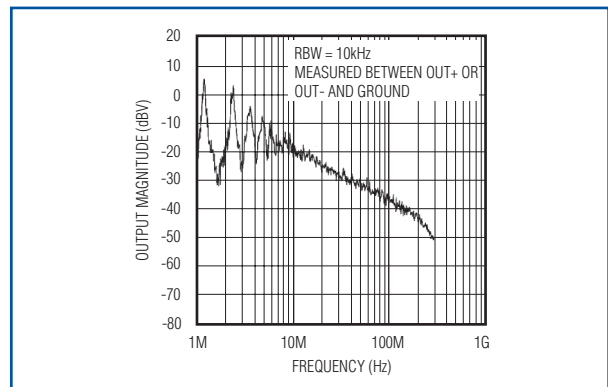


图9b. 扩谱调制将MAX9700的频谱能量分布在更宽的频带内。

结论

D类调制器技术的最新发展，允许D类放大器在线性放大器一度占主导地位的应用领域盛行起来。现代D类放大器除具有AB类放大器的所有优点(即良好的线性和最小的电路板空间)外，更具有高效优势。当前，有多种D类放大器可供选用，以满足各类应用需求。这当中包括低功耗便携式设备(如蜂窝电话和笔记本电脑)以及大功率设备(如车载音响系统或平板显示器)，对于前者来说，电池寿命、电路板空间和EMI兼容性往往至关重要；而后者则要求最大限度降低散热需求和发热量。对D类放大器及其最新的技术发展有一个基本理解，将有助于设计者为具体应用选择合适的放大器，并正确权衡某些功能特性的优势和劣势。

*美国专利号：#6,847,257。

嵌入式安全系统的发展趋势

随着安全性需求不断渗透到电子系统设计的各个环节，制造商和电路设计人员面临着前所未有的挑战。过去，只有少量的电子设备用户才会考虑安全性问题，而且主要集中在金融行业、军用产品、门禁控制市场等，大多采用相关的软件技术或专用硬件实现。而这种状况在最近几年发生了巨大变化，工程师需要面对层出不穷的安全标准、需要获得相关的产品认证，即便是很有经验的嵌入式系统设计人员，也要不断学习掌握这项新技术。了解这一技术趋势以及相关的设计、制造成本对于嵌入式系统制造商非常关键。

由于通过软件/固件设计很难保证全面的系统安全性，这就需要借助硬件保证系统的安全性，降低设计的复杂度(见第11页附录1—等级分类)。新推出的标准体系，例如：Trusted Computing Group™及各种数字版权管理(DRM)，涉及到消费类电子、多媒体、工业、医疗、汽车、电信等各个领域。当然，这一问题还涉及到政府、国家安全系统升级和不断发展的电子银行、电子商务系统。

为了获得更有效的安全体系，系统必须具备防物理篡改功能。即便是最老道的安全微处理器、FPGA、智能卡或其它安全设施，都会存在一些易受攻击的薄弱环节。这就需要系统有一个适当的有源保护电路，该电路即使在系统关断的情况下也能处于有效工作状态，监测可能发生的窃取敏感信息或知识产权的操作。为了完成这项任务，器件必须具备极低的功耗，并将防篡改响应电路与适合不同传感器的接口电路相结合，为敏感数据提供一道有效的防护网。

应该注意到，加密算法已不再是防范攻击的重点。攻击者会通过各种途径窃取密钥。因此，设计人员已经不在加密算法上投入过多精力，而是将注意力转向硬件保护方案的设计。

新的安全标准

新推出的安全标准大多参考了美国国家标准局(NIST)和英国通信电子安全组(CESG)制定的安全规范。这两个组织提供的标准分别是FIPS 140-1和ITSEC。

随着对安全水平要求的提高，以及众多新标准不断涌现，负责制定标准的跨国组织正采纳一个新的、统一的标准，称为“公共标准”，它组合了这些标准的优点(见第12页附录2—通用认证/标准)。例如，NIST最近将其FIPS规范更新为140-2版，并且很快会统一到公共标准。

此外，随着金融领域对安全设备需求量的增多，其它标准也开始变得活跃起来。公认的有MasterCard和Visa制定的EMV(欧洲MasterCard® Visa®)和PCI PED(支付卡行业，PIN输入设备)。这些标准与DRM相融合，能够使移动平台具备处理金融交易的能力，并可保护用户及系统的身份。政府也制定了新的法案，如FIPS 201身份验证(PIV)等。由此可见，安全认证标准的要求会越来越严格。

上述标准都论述了对物理安全性的要求，以满足不同终端产品范畴的规范。通常，这些安全性要求被划分到多个层次，从处理器开始到最终封装，包括处理器、涉及敏感数据或算法的存储器及数据通道。终端产品要取得认证，必须通过认证机构的全面测试，并提供一份安全文档，说明产品如何防范各种物理威胁。要通过某些标准认证(例如PCI)，制造商必须说明新产品在安全方面比现有产品有哪些改进，以满足新升级的标准。许多情况下，制造商和设计部门之前并没有面临类似要求，因此不清楚需要在产品中实现怎样的安全性。

不同应用对安全等级的要求千差万别，但是，对物理篡改保护功能的要求越来越严格。随着一些用于窃取数据的高端分析工具和专业技术的出现，越来越多的应用要求具有物理篡改保护功能。

DS3600系列安全控制器

为了帮助设计人员以小尺寸、低成本、低功耗满足严格的物理保护功能的需求，Maxim/Dallas Semiconductor推出了新一代安全控制器产品，用于保护硬件设备。DS3600系列产品能够为嵌入式系统提供可靠的安全保证，满足现有标准和新标准的要求。

这些器件具备精心设计的温度监视(利用具有超低漏电流的比较器)、低温攻击保护、计时和篡改记录功能，以及密码子系统(图1)需要的众多其它功能。这些功能的核心是独特的存储单元结构，可进一步保护顶层密钥和认证信息。传统的存储单元都存在数据印迹现象，即存储单元会残留先前保存的信息。可以通过多种攻击手段提取这些残留信息。DS3600内部的无印迹存储器是第一款具备该功能的器件，可有效防范这种常见的攻击方式。此外，使用一条硬件命令可迅速擦除整个存储器阵列。这种组合多种功能的安全控制器可极大地降低功耗，并且密钥存储器保护无需主处理器介入。

大多数情况下，该系列控制器的高集成度可替换40个以上的分离元器件。DS3600系列不仅具有小尺寸、低

成本和低功耗的特点，还可省掉其它价格昂贵的器件，如安全微处理器。因此，嵌入式系统制造商不必采用安全处理器架构即可通过认证，并实现对软件资产知识产权的保护。由于这些产品专为满足认证要求而设计，当设计人员必须提供必要文档以取得产品认证时，它们可提供最有力的帮助。

附录1—等级分类

为确定系统需要的安全等级，10多年前IBM®给出了一种等级分类方法，用来说明潜在的攻击等级，并且沿用至今。

等级I (聪明的外行)

- 通常很聪明
- 系统知识匮乏
- 可能使用过适度复杂的设备
- 通常会攻击系统的薄弱环节，而不会构建一个新系统

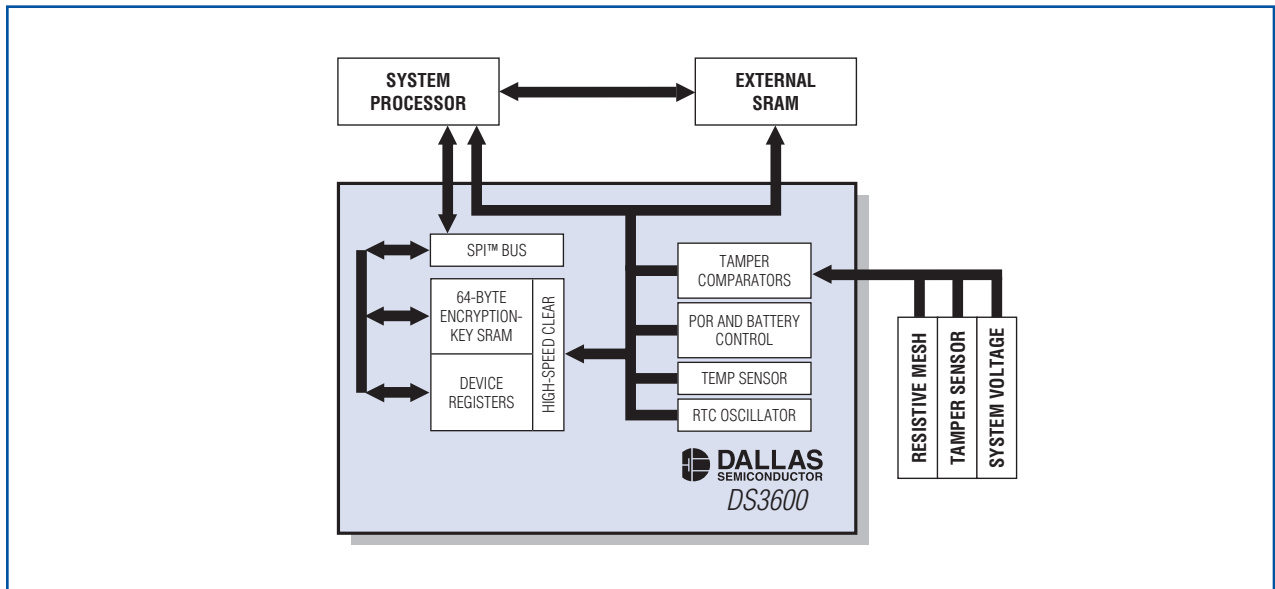


图1. DS3600防篡改控制器具有超高性能的比较器，可连续监控低功耗系统，符合最高级别的公共标准要求。

等级II (知识渊博的内行)

- 具备扎实的专业技术教育背景和工作经验
- 具备一些系统知识，可能接触过系统的大部分模块
- 经常使用高端工具和分析仪器

等级III (资金雄厚的机构)

- 拥有大量资金
- 能够组建专家队伍
- 能够获取或使用大部分高端分析工具
- 能够深入分析并设计复杂的攻击行为
- 可能招募等级II中知识丰富的行家，以扩充其攻击队伍

系统设计者寻求通过认证时，至少应该能够抵御以下常用攻击手段带来的威胁。

物理攻击

- 侵入封装
 - 切割、蚀刻以及离子或激光钻孔
- 反向工程(需要若干器件样品)
 - 生成电路原理图
 - 提取ROM码
 - 识别关键电路单元(即存储器)的物理位置
- 探测存储器
 - 通过FIB工作站更改电路
 - 通过致电离辐射改变某些特定晶体管的状态
 - 微探针测试
 - 对存储单元氧化物进行先进的光谱分析

非侵入式攻击

- 致电离辐射和热/冷侵袭
- 引入电压波动和时钟扰动
- 差分能量分析

附录2——通用认证/标准

NIST FIPS 140-2, 第1级至第4级

- CESG ITSEC E1至E6

- 公共标准EAL1至EAL7
- EMV 4.1 第1级和第2级 (主要用于银行/POS)
- ZKA (主要用于银行/POS)
- PCI PED (主要用于银行/POS PIN输入)

业界正统一到“公共标准”

- 存在不同的保护要求、安全目标和方案
 - UK EN45011:1998
 - ISO 15408
 - 可信计算联盟提出额外的保护要求
 - IBM可信移动平台安全要求

这些标准体系归纳如下，并简短说明了相应的安全级别。

NIST FIPS 140-2

FIPS 140-2定义了4个安全保证等级，从最低级到最高级，每一级构建于前一级基础之上。

第1级：要求产品正确实现NIST标准加密算法，包括数据加密标准(DES)、3DES和高级加密标准(AES)。

第2级：产品具有防篡改保护屏障，确保器件的任何毁坏都是可知的。

第3级：适用于密码模块，当模块侦测到物理攻击电路元件时，应清除密钥。符合第3级标准的产品要求访问必须通过授权。

第4级：当篡改者试图阻挠物理访问控制功能时(如通过冷却方式)，提供相应保护。

大多数安全产品采用FIPS 140-2第2级或第3级认证规范，只要模块安装在受控的环境内，两者都可提供足够的安全性能。

公共标准

公共标准采用评估保证级别(EAL)分级标准。该标准要求产品满足安全目标和保护要求文档给出的功能需求。这些文档由供货商提供，并由公共标准评估机构评估。EAL的级别分为EAL1至EAL7，大多数产品采用EAL4或更低级别的公共标准认证。

EAL1：产品满足基本的安全要求。

EAL7: 产品满足极为安全的要求。

EAL5、6和7的认证要求极为严格，需要评估产品的开发过程和理论框架，并且需要进行功能测试。

首先需要评估安全目标和保护要求文档，这样EAL评估才有意义。

类似文章发表在2006年10月出版的*Embedded Systems Europe*上。

IBM是IBM Corp.的注册商标。

MasterCard是MasterCard Worldwide的注册商标。

SPI是Motorola, Inc.的商标。

Trusted Computing Group是The TCG的商标。

Visa是Visa的注册商标。

选择串行总线

微控制器(μC)是当今各种先进电子产品的核心,它需要与一个或多个外设器件通信。以前,μC的外设是以存储器映射方式与数据和地址总线连接的。对地址线译码以获得片选信号,从而在有限的地址范围内为每个外设分配唯一的地址。这种接口类型所需的最少引脚数(除电源和地之外)为: $8(\text{数据}) + 1(R/\overline{W}) + 1(\overline{CS}) + n$ 条地址线 [$n = \log_2(\text{内部寄存器或存储器字节的数目})$]。例如,与一个16字节外设通信时,需要的引脚数为: $8 + 1 + 1 + 4 = 14$ 。这种接口的访问速度快,但较多的引脚数也同时带来了封装尺寸增大和总成本提高的问题。要降低成本和缩小封装尺寸,串行接口显然是理想的替代方案。

选择串行总线并非易事。除需要考虑数据速率、数据位传输顺序(先传最高位或最低位)和电压外,设计者还应该考虑以下几点:

- 通过何种方式选择某个外设(通过硬件片选输入或软件协议)。
- 外设如何与μC保持同步(借助一条硬件时钟线,或借助内嵌于数据流中的时钟信息)。
- 数据是在单根线上传输(在“高”和“低”之间转换),还是在一对差分线上传输(两根线按相反的方向同时转换其电压)。

- 通信线路的两端均使用匹配电阻实现阻抗匹配(通常用于差分信号传输),还是不匹配或仅在一端匹配(通常用于单端总线)。

表1以矩阵的形式展示了各种通用总线系统之间的差异。16种可能组合中只有4种通用类型为大家所熟知。

除这些特性外,具体应用还会提出更多要求,如供电方式、隔离、噪声抑制、μC(主机)与外设(从机)间的最大传输距离、以及电缆连接方式(总线型、星型、可承受线路反接等)。提出类似要求的应用包括楼宇自动化、工业控制和抄表等,并且都已制定了相应的标准。^{1,2}

电路板到背板的应用需求

提供外设功能的串行总线系统不应该给应用系统增加任何沉重的负荷。尤其需要注意以下几点:

- 互连布线一定要简单(信号线越少越好)。
- 必须能够轻松地通过软件实现协议(或所选的μC/μP本身提供这种接口)。
- 需要提供功能广泛的器件。
- 总线系统必须易于扩展。

单端、自同步系统使用软件协议完成寻址,因此需要的信号线最少。从表1可以看出,1-Wire®、LIN总线和SensorPath™能够满足这些条件。在这类总线系统中,还需要考虑其它因素(见表2)。

表1. 串行总线系统概括

		寻址(片选)		
同步方式	协议		片选线	阻抗
自同步	1-Wire, LIN bus, SensorPath			不匹配
	RS-485, LVDS, CAN, USB 2.0, FireWire®			匹配
时钟线				
	i ² C, SMBus™		SPI™, MICROWIRE™	不匹配
		单端	差分	单端
传输方式				

表2. 1-Wire、LIN总线和SensorPath总线系统的性能差异

	1-Wire ³	LIN总线 ⁴	SensorPath ⁵
网络物理尺寸	电路板或背板, 可扩展至~300m	~40m	电路板
网络驱动器 (硬件)	基于RS-232、I ² C、USB和通用μP 端口引脚的驱动器 ^{6,7}	基于μP端口引脚的驱动 器	Super-I/O芯片, μP端 口引脚
网络驱动器 (软件)	免费提供基于各种工作平台(包括 μC在内的)软件 ⁸	免费提供基于Freescale™ μC的软件	不提供
电源	借助数据线供电(通常情况), 本地 V _{CC} (某些器件)	借助数据线供电	本地V _{CC}
数据速率	高达~15kbps (标准模式)或~125kbps (高速模式) ⁹	最高~20kbps	与传输的数据信息有 关, 最高~20kbps
网络节点查找 功能	通过网络功能命令“search ROM” 完成	不具备, 基于消息的寻 址方式	不支持
器件功能选择 范围	器件功能丰富, 包括序列号、仪表 测量和安全存储器等	功能局限于汽车应用	功能局限于温度传感器 和电压ADC

物理网络尺寸

只有SensorPath局限于电路板尺寸的应用。一定条件下, 使用恰当的硬件和软件网络驱动器, 可以极大地扩展1-Wire总线网络的距离。

网络驱动器

对于基于协议的网络, 设计者需要软件驱动程序来产生通信波形(链路层), 识别并寻址网络(网络层)的单个从器件/节点, 并发送/接收数据(传输层)。软件驱动程序与特定操作系统和通信端口有关。可提供基于各类端口的1-Wire硬件驱动芯片(主机)以及适配器, 端口类型包括COM、LPT、USB和I²C。在未作匹配的大型网络中, 电缆末端、连接器和分支的反射会限制网络的传输性能。

电源

必须为网络中的每个从器件供电, 以实现正常工作。最具成本效益的方法是通过数据线远程供电。该方法

也称为“寄生供电”, 这使得读取系统诊断信息(比如在掉电模式下)成为可能。具体范例请参考应用笔记178中的图3和相关内容: *利用1-Wire产品标识印刷电路板*。¹⁰当然由于必须为供电留出时间, 寄生供电也降低了可用的数据速率。

数据速率

通常来说, 数据速率越高, 网络传输距离越短, 反之亦然。1-Wire系统具有电源传输功能, 因此最大数据传输速率取决于网络的从器件数目以及电缆总长度(电容)。

网络节点查找功能

该特性允许主机识别网络中从器件的数目、类型和地址。这一点对于节点数动态(变化)的网络来说必不可少。请参考*Dallas工程期刊(第2期)*¹¹中第22页的示例。

器件功能选择范围

如果不能提供应用所需要的功能，即使再出色的总线也毫无用处。与LIN总线和SensorPath相比，1-Wire系统目前可以提供最丰富的功能。

I²C/SMBus与1-Wire总线

如果实际应用可以提供时钟线，则总线选择范围可扩展到I²C¹²和SMBus¹³接口。根据SMBus的规范，它可以看作是100kbps I²C总线规范增加了超时特性后的派生总线类型。在某个节点与总线主机失去同步的情况下，超时特性可避免总线发生闭锁，而I²C系统则需要经过一次上电复位过程，才能从这种故障状态恢复至正常工作状态。在1-Wire系统中，复位/在线检测周期可将通信接口复位至确定的启动条件下。除了时钟线外，I²C/SMBus还为总线上传输的每个字节提供一个应答位。这使得有效数据速率降低了12%。通信过程开始于一个启动条件，并跟随从器件地址和一个数据方向位(读/写)，最后结束于一个停止条件。对于1-Wire系统，首先需要满足网络层的要求(即选择某个特定器件，执行search ROM命令或者广播)；接下来发送与特定器件相关的命令代码，该代码同时会影响数据的传输方向(读/写)。

原有I²C和SMBus总线系统的一个突出问题是其有限的7位地址空间。由于可提供超过127种不同器件类型，我们无法根据从器件地址推断器件功能。此外，许多I²C器件还允许用户随意设置1个或多个地址位，以在总线上挂接多个相同器件。这一特性进一步减少了可用的地址空间。解决地址冲突问题的标准做法是将总线系统划分成若干段，某一时刻可在软件控制下激活某个网络段。这种划分网络的方法需要增加更多硬件，也使应用固件更为复杂。I²C系统不具备网络节点查找或枚举功能，因此很难处理节点数动态变化的系统。这一问题可借助SMBus Specification Version 2.0¹³中的地址分辨率协议得以解决。但是，支持该特性的SMBus器件极为稀少。

SPI和MICROWIRE接口

SPI¹⁴和MICROWIRE¹⁵ (SPI的子集)均需要为每个从器件提供一条额外的片选线。由于具有片选信号，SPI协议只定义了针对存储器地址和状态寄存器的读/写命令。它不提供应答功能。通常，SPI器件的数据输入和数据输出采用不同的引脚。鉴于数据输出在除了

读操作外的任何情况下均为三态(禁止)，因此可将两个数据引脚接到一起以构成单根双向数据线。当其它总线系统无法提供所需的功能或需要较高的数据传输速率时，可选用SPI总线，它可以支持2Mbps或更高的速率。SPI和MICROWIRE的缺点在于其寻址某个特定器件的CS信号由译码器产生。但是，其好处在于不会产生地址冲突。和I²C总线一样，不提供节点查找功能。主机无法根据从器件的逻辑地址来确定器件功能，因此很难管理节点动态变化的网络。

RS-485、LVDS、CAN、USB 2.0和FireWire

我们对这些标准进行讨论，以举例说明差分传输的特点。这类总线系统中传输速率最快的两种是FireWire¹⁶和USB 2.0¹⁷，它们采用点对点电气连接。使用先进的节点或集线器，可以构成树状拓扑的虚拟总线，数据包从源端发送至端点(USB)，或采用对等传输(FireWire)，突发数据速率高达480Mbps (USB 2.0)或1600Mbps (FireWire)。尺寸有限的数据包以及接收/缓冲/重发通信机制增加了传输时间，反过来降低了有效的数据吞吐能力。USB的拓扑和协议允许最多连接126个节点，FireWire允许最多63个节点，使用无源电缆时节点间的最大传输距离为4.5m。专为包括PC外设、多媒体、工业控制和航空(仅FireWire)应用而设计，USB和FireWire器件可以带电插入系统(热插拔)。该特性允许网络节点数动态变化。

LVDS¹⁸、RS-485¹⁹和CAN²⁰可实现挂接主机和从机的总线型结构，甚至可以连接多个主机。这些标准中低压差分信号(LVDS)是速率最快的，如果总线长度不超过10m，可工作在100Mbps速率下。可用的数据速率及吞吐可以更快或更慢，具体取决于网络尺寸。LVDS电气标准专为背板应用而设计，支持热插拔功能，但不包含任何协议。

RS-485也仅定义了电气参数。RS-485定义了负载和每条总线的最大负载数目(32)，而不是以节点的形式给出。一个电气节点的负载可以小于1。12m网络距离下的典型数据速率可高达35Mbps，1200m距离下数据速率可达100kbps，这些特性足以满足数据采集和控制应用。RS-485设备的协议通常基于原来设计用于RS-232的部分协议。

与此不同，控制器局域网(CAN)为分布式实时控制定义了通信协议，安全性非常高，专门面向汽车应用和

工业自动化领域。数据速率从40m距离下的1Mbps到1000m距离下的50kbps。寻址方式是基于消息的，协议本身对节点数没有任何限制。CAN节点支持热插拔，网络节点数可以动态变化。

结语

在简单、低成本总线系统中，与LIN总线和SensorPath相比，1-Wire系统的从器件可提供最广泛的功能和网络驱动器。I²C和SMBus除了需要数据线和参考地之外，还需要时钟线和V_{CC}电源，当然可供选择的器件功能也非常多。SPI和MICROWIRE需要额外的片选线，但可以提供更高的数据速率。

除支持寄生供电和网络节点查找功能外，1-Wire接口和协议还支持热插拔，这一特性通常仅在使用差分信号的高速系统以及SMBus 2.0兼容产品中才提供。iButton[®]产品是使用极为广泛的热插拔1-Wire器件，热插拔是这类器件的正常工作方式。事实已经证明，1-Wire器件在下列应用中极为有效：全球识别号²¹、电路板/配件标识与认证¹⁰、温度检测和执行装置等。另外一种非常成功的1-Wire产品是具有安全存储器和质询-响应机制的器件，它能以最低的成本实现双向认证和软件代码保护。^{22, 23}

类似文章出现在2006年9月出版的*Electronic Products*上。

参考资料

1. Interbus Club. www.interbusclub.com/ (工业自动化)
2. The valid M-Bus standard. www.m-bus.com/ (抄表)
3. "Overview of 1-Wire Technology and Its Use." www.maxim-ic.com.cn/AN1796 (1-Wire介绍)
4. LIN Local Interconnect Network. www.lin-subbus.org/ (LIN规范)
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. "性能优异的1-Wire网络驱动器。" www.maxim-ic.com.cn/AN244 (硬件驱动器)
7. "1-Wire网络可靠设计指南。" www.maxim-ic.com.cn/AN148 (1-Wire网络)
8. "1-Wire软件资源指南。" www.maxim-ic.com.cn/AN155 (软件驱动器)

9. "确定多从机1-Wire网络的恢复时间。" www.maxim-ic.com.cn/AN3829 (恢复时间)
10. "利用1-Wire产品标识印刷电路板。" www.maxim-ic.com.cn/AN178 (电路板识别)
11. "Dallas工程期刊," 第二期。 pdfserv.maxim-ic.com/cn/ej/DallasEJ2.pdf (动态网络)
12. "The I²C-Bus Specification, Version 2.1, January 2000." www.nxp.com/acrobat_download/literature/9398/39340011.pdf (I²C)
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规范)
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规范A部分)
- 20b. CAN in Automation (CiA). "CAN Specification 2.0, Part B." www.can-cia.org/downloads/ciaspecifications/?269 (CAN规范B部分)
21. "利用1-Wire器件建立全球标识符。" www.maxim-ic.com.cn/AN186 (全球标识符)
22. "保护您的研发成果—双向认证及软件功能保护。" www.maxim-ic.com.cn/AN3675 (双向认证)
23. "利用单总线接口的SHA-1安全存储器实现Xilinx® FPGA的身份识别及防拷贝机制。" www.maxim-ic.com.cn/AN3826 (FPGA保护)

1-Wire和iButton是Dallas Semiconductor Corp.的注册商标。
FireWire是Apple Computer, Inc.的注册商标。
Freescale是Freescale Semiconductor, Inc.的商标。
SensorPath和MICROWIRE是National Semiconductor Corp.的商标。
SMBus是Intel Corp.的商标。
SPI是Motorola, Inc.的商标。
Xilinx是Xilinx, Inc.的注册商标。

设计实例

通过单个触点增加控制、存储器、安全和混合信号功能

概述

Dallas Semiconductor的1-Wire总线采用非常简单的信令协议，通过一条公共数据线实现主机/主控制器与一个或多个从机之间的半双工、双向通信(图1)。从器件的供电和数据通信都是借助这条1-Wire线完成的。供电通过以下方式实现：在数据传输过程中，总线状态为高时为从机的内部电容充电，总线状态为低时利用电容存储的电荷为器件供电。典型的1-Wire主机包括一个开漏极I/O端口，并通过电阻上拉至3V至5V电源。Dallas Semiconductor还提供更加完善的主机，这种主机带有线驱动器。采用这种智能通信技术，可随时方便、高效地增加存储器、认证和混合信号功能。

64位序列号

所有1-Wire系统都有一个重要的基本特性：每个从机都有一个唯一、不能更改(ROM)的64位、工厂激光刻制序列号(ID)，这个序列号永远不会与另一个器件重复。除了为终端产品提供唯一的电

子ID外，64位ID码还允许主机从挂接在同一条总线上的许多从机设备中选择一个。64位ID码的一部分是8位家族码，用于识别器件类型及支持的功能。

数据位通信

总线主机启动和控制所有1-Wire通信。如图2所示，1-Wire通信波形与脉宽调制类似，因为在数据位传输期间(或时隙)是通过宽脉冲(逻辑0)和窄脉冲(逻辑1)发送数据的。当总线主机发出一个预定宽度的“复位”脉冲时，启动通信过程，并通过该脉冲同步整个总线系统。所有从机都会以一个逻辑低“应答”脉冲来响应复位脉冲。写数据时，主机首先拉低1-Wire总线以启动一个时隙，然后保持总线为低(宽脉冲)来发送逻辑0，或释放总线(窄脉冲)使总线返回逻辑1状态。读数据时，主机以窄脉冲方式拉低总线，重新启动一个时隙。然后从机可以通过导通开漏极输出并保持线路为低来延长该脉冲，从而返回逻辑0；或保持开漏极的

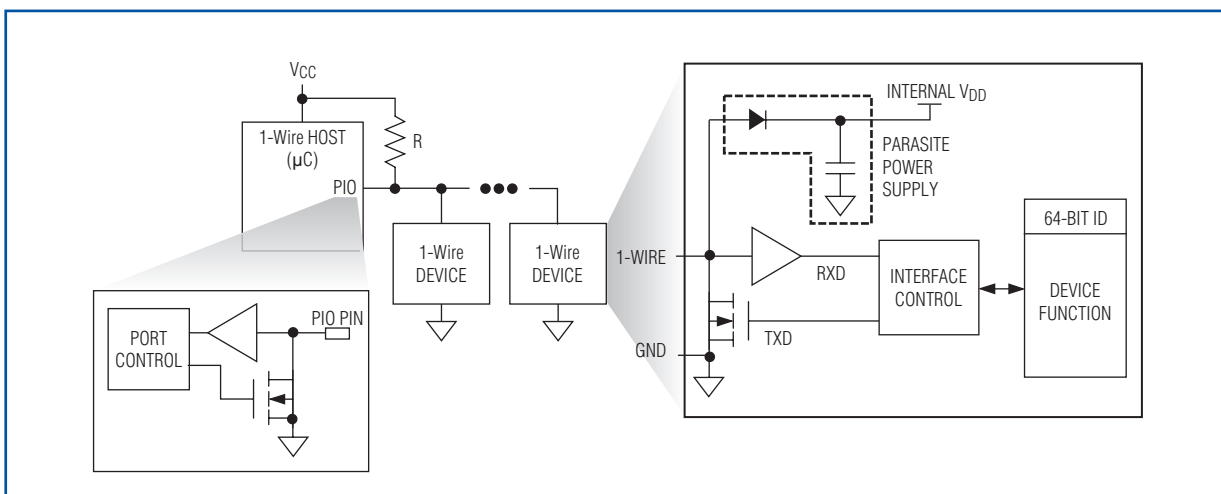


图1. 在1-Wire主机/从机配置中，所有设备共享一条公共数据线。

设计实例

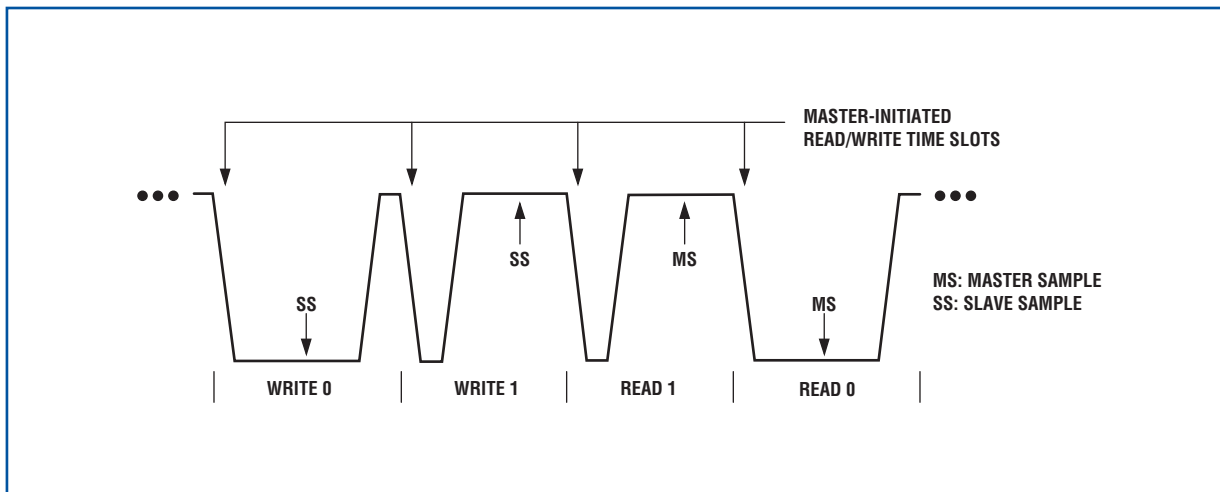


图2. 该波形示例展示了由主机启动的写/读数据位、以及从机和主机的采样点。

关闭状态以允许总线恢复，从而返回逻辑1。大多数1-Wire器件都支持两种数据速率：15kbps标准速率和111kbps高速速率。该协议为自同步，并可接受数据位之间的较长延迟，从而确保了中断软件环境下的正常工作。

器件选择

1-Wire通信的第一步操作是选择从机以进行后续通信。在只有一个从机的系统中，从机选择过程极为简单。而在多从机系统中，要么选择所有从机，要么通过64位ID码选择特定的从机。二元搜索算法(在1-Wire数据资料中称为ROM命令)允许主机“学习”并随后获取总线上所有从器件的相应64位ID。选择了特定的从机后，主机发出与该器件相

关的命令，并向从机发送数据，或读取从机数据。与此同时，其它所有从机均忽略该通信过程，直到主机发出下一个复位脉冲。

结语

可以在1-Wire系统中添加存储器，数字、模拟和混合信号功能。这一系列功能丰富的各种器件通过1-Wire单线接口实现系统性能的优化，完全可以解决空间局促的互联限制，并/或通过独特的器件性能实现增值功能。1-Wire产品提供标准IC封装，以及Maxim专有的坚固、不锈钢iButton封装。请访问www.maxim-ic.com.cn/1-Wire，了解产品、封装和软件支持的详细信息。