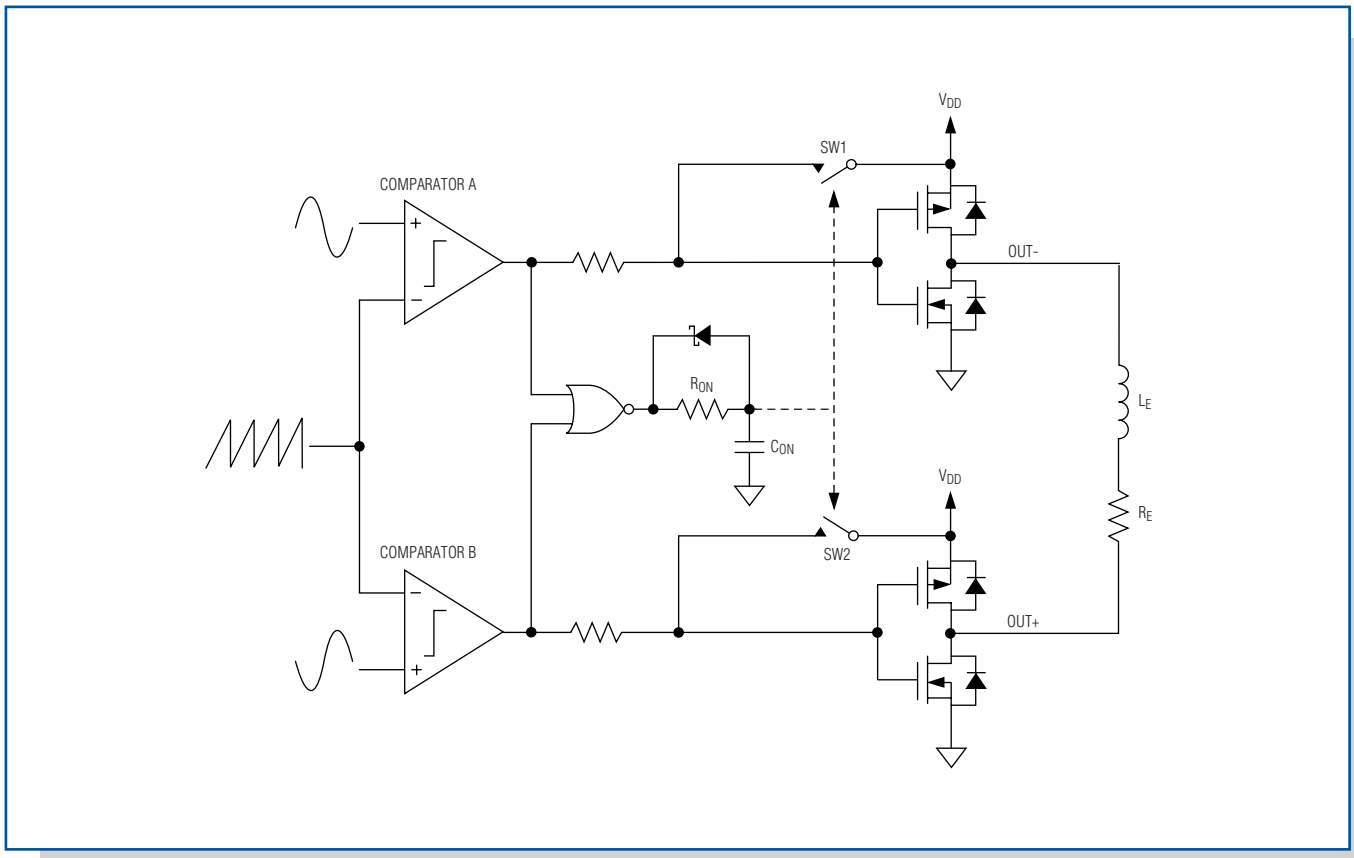
DALLAS SEMICONDUCTOR MAXIM

# Engineering Journal

Volume Fifty-Nine






*MAX9700のフィルタレスD級変調器トポロジを示す簡略化されたファンクションダイアグラム(8ページを参照)*

# News Brief

## マキシム、2007年度第1四半期の売上と利益を発表

Maxim Integrated Products, Inc. (NASDAQコード：MXIM)は、2006年9月23日までの第1四半期における総売上高が5億270万ドルであったと発表しました。これは、2006年度第4四半期に対して1.5%の減少ですが、前年同期に対して18.5%の増加となります。

2007年度第1四半期の純利益は1億750万ドル、希薄後1株当り利益(株式による報酬費用を含む)で0.33ドルとなりました。なお比較のために申し添えると、2006年度第4四半期は、純利益が1億2,430万ドル、希薄後1株当り利益が0.37ドルであり、前年同期は純利益が1億540万ドル、希薄後1株当り利益(株式ベースの補償費用を含む)が0.31ドルでした。

研究開発費は1億3,020万ドルで、総売上高の25.9%でした。これに対し、2006年度第4四半期は1億2,720万ドルで、24.9%でした。今期、研究開発費が増加した主な理由は、今後の製品開発をサポートするために行った人員増強およびその関連の出費によるものです。

販売一般管理費は4,010万ドルで、総売上高の8.0%でした。これに対し、2006年度第4四半期は3,790万ドルで、7.4%でした。今期、販売一般管理費が増加した主な理由は、当社ストックオプションプログラムの監査に300万ドルを要したことです。

第1四半期の総営業利益は1億5,080万ドルで、総売上高の30.0%でした。これに対し、第4四半期は1億7,330万ドルで、34.0%、2006年度第1四半期は1億4,580万ドルで、34.4%でした。

税率が2%続けて上昇していますが、これは、域外所得に対する課税控除がなくなり、そのかわり、国内生産に対する控除が7年間をかけて段階的に導入されること、また、研究開発に対する税額控除を米国政府が延長しなかったことによるものです。これは、純利益を330万ドル、希薄後1株当り利益を0.01ドル押し下げる結果となりました。

この第1四半期中、現金および現金等価物は5,140万ドル増えて14億ドルとなりました。これは、210万株の自社株(普通株)を6,080万ドルで買い戻し、5,000万ドルの配当を支払い、9,490万ドルの設備機器を購入した後の数字です。売掛金は、80万ドル減少して2億9,170万ドルとなり、たな卸資産は1,060万ドル増えて2億1,790万ドルとなりました。なお、この数字には、株式による報酬費用1,560万ドルが含まれています。

Giffordは、次のようにコメントしています。「当社取締役会は、2007年度第2四半期の現金配当を0.156ドル/株と決定しました。配当は、2006年11月21日現在の株主に対し、2006年12月5日に支払う予定です。」

2007年度第1四半期の業績に関する詳細なリリース(セーフハーバー条項を含む)は、japan.maxim-ic.com/NewsBriefをご覧ください。

MaximのロゴはMaxim Integrated Products, Inc.の登録商標です。Dallas SemiconductorのロゴはDallas Semiconductor Corp.の登録商標です。
© 2007 Maxim Integrated Products, Inc. All rights reserved.

# D級アンプ：基本動作と開発動向

*D級アンプは高効率であることから、ポータブルでコンパクトな高出力アプリケーションに最適です。従来のD級アンプは、パルス幅変調(PWM)出力波形からオーディオ信号を抽出するためにローパスフィルタを外付けする必要がありました。これに対し最近のD級アンプは最先端の変調方式を採用しており、多くのアプリケーションで外部フィルタリングが不要になるとともに、電磁干渉(EMI)も低減されています。外部フィルタが不要になるとボードスペースが削減できるだけでなく、多くのポータブル/コンパクトシステムのコストも大幅に削減することができます。*

## はじめに

オーディオシステムの設計に携わるエンジニアであれば、A級、B級、AB級といったリニアなオーディオアンプに対し、D級アンプは電力効率が優れていることをよく知っています。AB級などのリニアアンプの場合、相当の電力が、素子のバイアスと出力トランジスタをリニア動作させるために消費されてしまいます。これに対してD級アンプは、電流を負荷に流し込むスイッチとして機能するため、出力段で浪費される電力が最小限ですみます。D級アンプで発生する電力損失は、ほとんどが、出力トランジスタのオン抵抗、スイッチング損失および間接的な自己消費電流によるものです。アンプ内で消費される電力は、そのほとんどが熱で消費されます。D級アンプではヒートシンクが不要か、必要な場合でもかなり小さくてすむことから、コンパクトな高出力アプリケーションに最適です。

これまで、PWMによるD級アンプは、高い電力効率というメリットはあっても、外部フィルタの部品コスト、EMI/EMC準拠、リニアアンプに対して低いTHD+N性能などのデメリットによって注目されませんでした。しかし、今日のほとんどのD級アンプは、最新の変調方式とフィードバック技術によって、このような問題がかなり軽減されています。

## D級アンプの基礎

最新のD級アンプで使用される変調器方式にはさまざまな種類がありますが、最も基本的な方式は三角波(のこぎり波)オシレータを使ったパルス幅変調(PWM)です。PWMを使用したハーフブリッジD級アンプのブロックダイアグラムを**図1**に示します。この回路は、パルス幅変調器と2つの出力MOSFET、それに増幅されたオーディオ信号を復元する外付けのローパスフィルタ($L_F$と$C_F$)で構成されています。図に示すように、pチャネルとnチャネルのMOSFETは、出力ノードを$V_{DD}$とグランドへと交互に接続する電流ステアリングスイッチとして動作します。出力トランジスタは、出力を$V_{DD}$とグランドのどちらかへ切り替えるため、D級アンプの出力は高周波の方形波となります。大部分のD級アンプのスイッチング周波数($f_{SW}$)は、一般に、250kHzから1.5MHzまでです。出力方形波は、入力のオーディオ信号によってパルス幅変調されています。このPWMは、入力オーディオ信号と内部で発生する三角波(のこぎり波)を比較し生成されます。この変調方式は、一般に、三角波オシレータがサンプリングクロックとして使われる「ナチュラルサンプリング」とも呼ばれます。こうして現れる方形波のデューティサイクルは、入力信号レベルに比例します。入力信号がないとき、出力波形のデューティサイクルは50%に等しくなります。入力信号レベルによって、PWM出力波形は**図2**のように変化します。

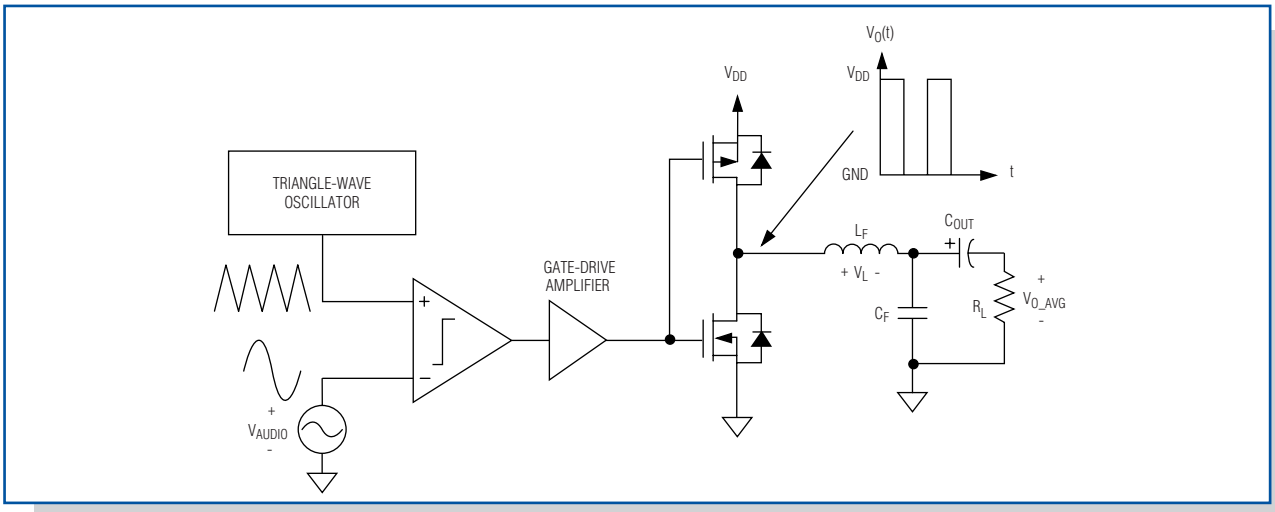



*図1. 基本的なハーフブリッジD級アンプの機能ブロックダイアグラム*

増幅されたオーディオ信号をこのPWM波形から取り出すため、D級アンプの出力をローパスフィルタに入力します。図1のLCローパスフィルタは、受動的な積分器として動作し(フィルタのカットオフ周波数が、出力段のスイッチング周波数に対して、少なくとも1桁低いと仮定します)、フィルタの出力では方形波の平均値に等しい値が得られます。また、ローパスフィルタであることで、高周波のスイッチングエネルギーが抵抗性負荷で消費されることも防ぎます。ここで、フィルタリング後の出力電圧($V_{O\_AVG}$)と電流($I_{AVG}$)が、1回のスイッチング期間において一定であると仮定します。$f_{SW}$が、オーディオ入力の最も高い周波数よりはるかに高いことから、これはかなり正確な仮定です。これにより、デューティサイクルとフィルタリング後の出力電圧との関係は、インダクタ電圧とインダクタ電流の単純な時間領域解析で導くことができます。

インダクタを流れる瞬間的な電流は、次式で表されます。

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

ここで$V_L(t)$は、図1に示す極性で表わしたインダクタの両端の瞬間的な電圧です。

負荷に流れる平均電流($I_{AVG}$)は、1回のスイッチング周期において一定であると仮定されているため、スイッチング周期($T_{SW}$)の始まりのインダクタ電流は、**図3**に示すように、スイッチング周期の最後のインダクタ電流と等しくならなければなりません。

これを数学的に表現すると、次式のようになります。

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

式2は、1回のスイッチング周期についてインダクタ電圧を積分すると0にならなければならないことを表わしています。式2を用いて図3に示す$V_L(t)$波形を考察すると、式2が成立するためには、面積($A_{ON}$と$A_{OFF}$)の絶対値が互いに等しくなければなりません。これにより、フィルタリング後の出力電圧をスイッチング波形のデューティ比によって表すことができます。

$$A_{ON} = |A_{OFF}| \qquad (式3)$$

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

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

式4と式5を式3に代入すると、次式が得られます。

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

これを$V_O$について解くと、次のようになります。

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

ここで、Dは出力スイッチング波形のデューティ比です。

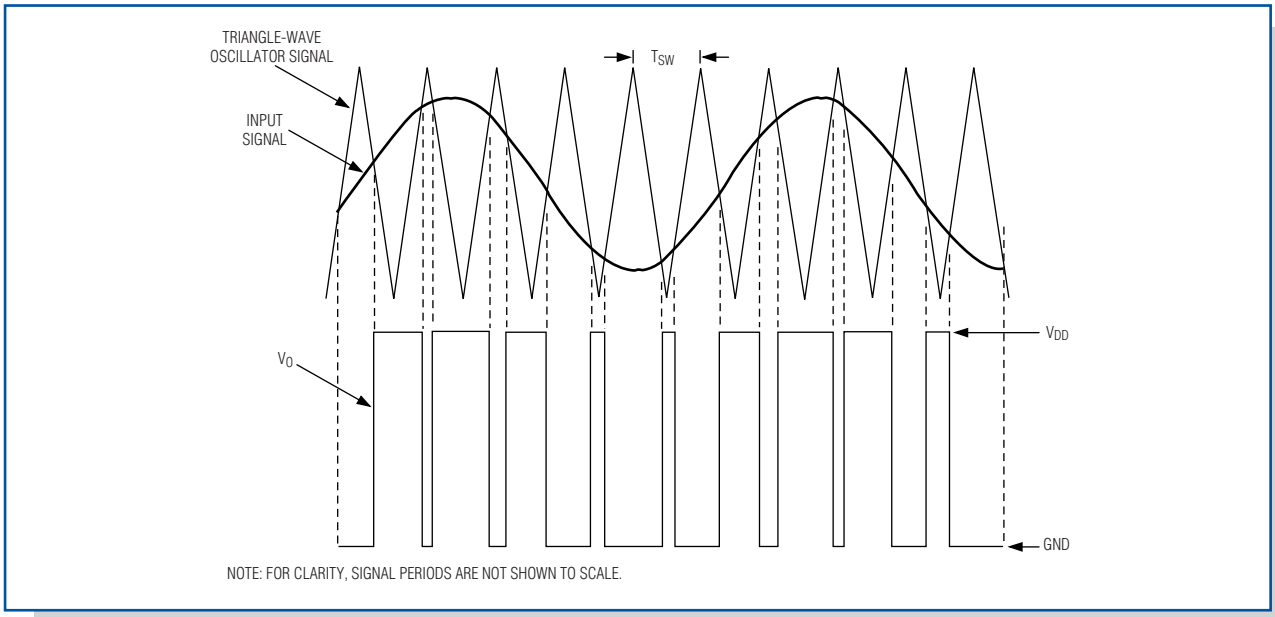



*図2. 出力信号のパルス幅は、入力信号の振幅に比例して変化します。*

## フィードバックによる性能改善

D級アンプの多くは、PWM出力をデバイス入力に戻す負帰還を利用します。閉ループを構成するとデバイスの直線性が向上するとともに、デバイスの電源除去比が高くなるというメリットがあります。これに対し、開ループアンプは、本質的に(あったとしても)最小限の電源除去比しか得られません。閉ループの方式では、出力波形を検出し、アンプの入力へフィードバックするために、電源電圧の変動が出力で検出され、制御ループによって補正されることになります。ただし、このような閉ループ設計のメリットは、フィードバックを利用するすべてのシステムと同じく、安定度の問題を犠牲にする可能性がついてきます。つまり、どのような動作条件でも十分な安定度が得られるように、制御ループを注意深く設計し、補償しなければならないのです。

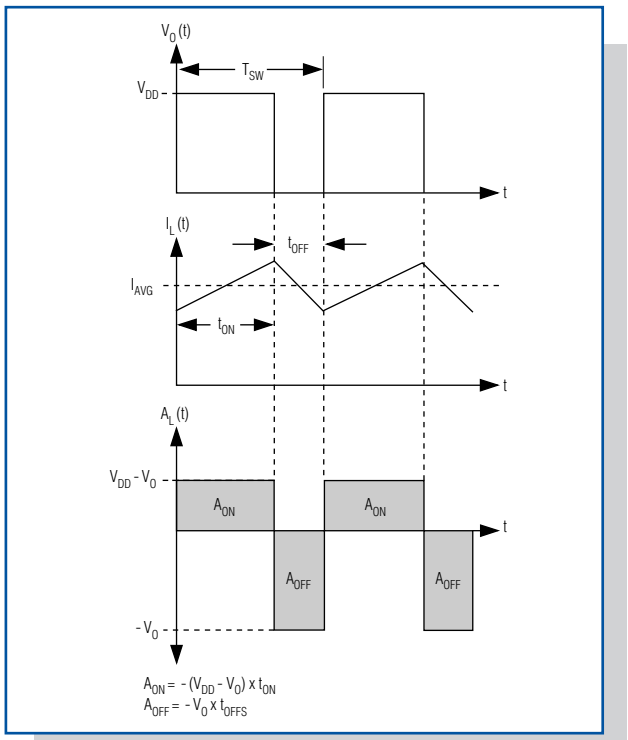



*図3. 基本的なハーフブリッジD級アンプにおけるフィルタのインダクタに流れる電流と電圧の波形*

通常のD級アンプでは、パルス幅変調器の非直線性と出力段、電源電圧変動による帯域内ノイズを大きく減らすことができるノイズシェーピング型のフィードバックループを使用し動作します。この方式は、シグマデルタ変調器で使われるノイズシェーピングとほぼ同じです。このノイズシェーピング機能を説明するため、**図4**に、1次のノイズシェーピングの簡略化したブロックダイアグラムを示します。フィードバック回路は、一般に、抵抗分圧器を使ったネットワークとしますが、簡単にするため、図4の例ではフィードバック比を1としています。理想的な積分器は利得が周波数に反比例するため、この積分器の伝達関数は1/sという簡単な形になります。また、PWMブロックはユニティゲインであり、かつ、制御ループに対する位相シフトがゼロであると仮定します。基本的な制御ブロックの解析から、出力を表す次式が得られます。

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

式8では、ノイズ項$E_n(s)$にハイパスフィルタ関数(ノイズ伝達関数)が掛けられており、入力項、$V_{IN}(s)$にはローパスフィルタ関数(信号伝達関数)が掛けられています。このノイズ伝達関数のハイパスフィルタ応答がD級アンプのノイズとなります。出力フィルタのカットオフ周波数を適切に選べば、このノイズの大半を帯域外に押し出すことができます(図4)。この例では1次のノイズシェーピング

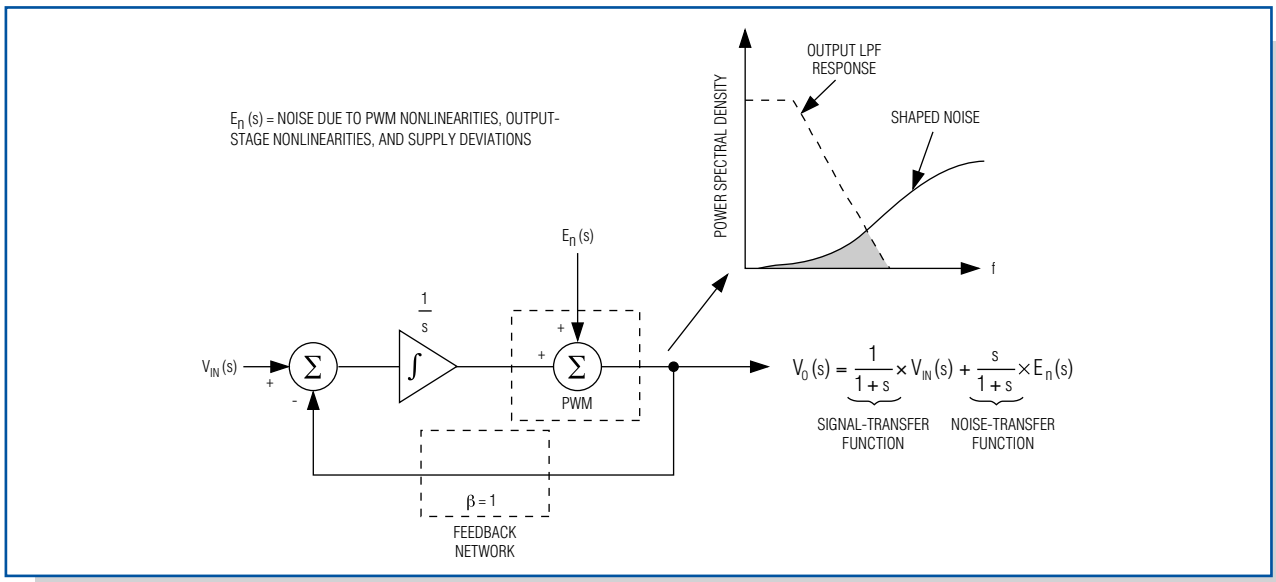



*図4. 1次のノイズシェーピングの制御ループをD級アンプに付加し、ノイズの大半を帯域外に押し出します。*

としましたが、最近のD級アンプは高次のノイズシェーピングを利用し、直線性と電源除去比のさらなる最適化を図っています。

## D級方式—ハーフブリッジ 対 フルブリッジ

D級アンプの中には、フルブリッジ出力段を持つものも数多く存在します。フルブリッジでは、ふたつのハーフブリッジ段を使って負荷を差動駆動します。このような負荷の接続方法は、一般に、ブリッジ接続負荷(BTL)と呼ばれます。**図5**に示すように、フルブリッジ構成は、負荷を導通経路を交互に切り替えるように動作します。これにより、負電源を用意したり、DC成分をブロックするコンデンサを用意することなく、負荷に正負両方向の電流を流すことができます。

**図6**は、従来のBTL接続PWM型D級アンプの出力波形です。図6からわかるように、互いに補完する形の出力波形となっており、負荷の両端にPWM信号が差動的に加わります。この場合も、ハーフブリッジ型方式と同じように出力へLCフィルタを外付けし、低周波のオーディオ信号を取り出すとともに高周波エネルギーが負荷で消費されないようにする必要があります。

フルブリッジD級アンプは、AB級のBTLアンプと同じメリットを持つ上、電力効率が高いという特長があります。BTLアンプの第一のメリットは、単一電源動作時に、DC成分をブロックするコンデンサが出力に必要ないという点です。ハーフブリッジアンプの場合は、出力が$V_{DD}$とグランドの間で変化し、アイドル時にはデューティサイクルが50%となるため、同様にはいきません。出力に$V_{DD}/2$というDCオフセットが現れるということです。フルブリッジアンプとすると、このオフセットが負荷の両側に発生するため、出力に流れるDC電流はゼロになります。第二のメリットは、負荷を差動駆動するため、電源電圧が同じなら、ハーフブリッジアンプに対して倍の出力信号スイングが得られる点です。これはつまり、同じ電源電圧で動作するハーフブリッジアンプに対し、理論上、4倍の最大出力が得られることを意味します。

しかし、フルブリッジのD級アンプとするためには、ハーフブリッジ方式に対して倍の数のMOSFETスイッチが必要になります。一般にスイッチ数が増えるほど伝導損失とスイッチング損失が大きくなることから、これをフルブリッジアンプのデメリットだと考える人もいます。しかし、これは、出力電流と電源電圧の両方が大きい高出力のパワーアンプ(10W以上)においてのみです。このためハーフブリッジアンプは、いくぶん高効率なために、高出力アプリケーションでよく採用されます。高出力のフルブリッジアンプは、一般に、8Ω負荷に対して、80%から88%という電力効率を示します。それに対し、MAX9742などのハーフブリッジアンプは、8Ω負荷でチャネル当り14W以上の出力を出した場合でも、90%以上の電力効率を実現することができます。

## 出力フィルタの省略—フィルタレス変調方式

従来のD級アンプが抱える大きな問題は、LCフィルタを外付けしなければならない点です。これは、ソリューションのコストを押し上げ、実装面積が必要になるだけでなく、フィルタ部品の非直線性によって歪みが発生する可能性も出てきます。幸いなことに、最近のD級アンプでは最新の「フィルタレス」変調方式によって、外部フィルタを省略できるか、少なくとも最小にできるようになりました。

**図7**は、MAX9700のフィルタレス変調器方式の簡略化したファンクションダイアグラムです。従来のPWM BTLアンプと異なる点は、ハーフブリッジごとに専用コンパレータが用意され、それぞれの出力を独立に制御できるようになっていることです。変調器は、差動オーディオ信号と高周波ののこぎり波によって駆動されます。両方のコンパレータの出力がともにローであるとき、D級アンプの出力は両方ともハイになります。同時に、NORゲートの出力がハイになりますが、$R_{ON}$と$C_{ON}$によるRC回路で遅延を行っています。NORゲートの遅延出力が定められたスレッショルドを越えると、スイッチ、SW1とSW2が閉じます。この結果、OUT+とOUT-がローになり、次のサンプリング周期が始まるまで、ローの状態が保たれます。この方式では、両方の出力が、$R_{ON}$と$C_{ON}$によって決まる最短時間($t_{ON(MIN)}$)の間、オンになります。**図8**に示すように、入力信号がゼロのときは、出力は、$t_{ON(MIN)}$に等しい、同相のパルス幅になります。入力のオーディオ信号が増加、あるいは減少すると、一方のコンパレータがもう一方よりも先に遷移します。この動作と最小オンタイム回路により、一方の出力のパルス幅を変化させると同時に、もう一方の出力のパルス幅を$t_{ON(MIN)}$に保ちます(図8)。言い換えると、それぞれの出力の平均値には、出力オーディオ信号を半波整流したものが含まれていることになります。それぞれの出力の平均値の差分をとれば、完全な出力オーディオ波形が得られます。

MAX9700の出力は、アイドル時、同相信号となるため、負荷には差動電圧が印加されず、外付けフィルタなしで自己消費電力を最小限に抑えることができます。マキシムのフィルタレスD級アンプは、出力からオーディオ信号を取り出すために、外付けLCフィルタに頼るのではなく、スピーカ負荷が持つインダクタンスと人の耳によってオーディオ信号を取り出す形となっています。スピーカの電気抵抗($R_E$)とインダクタンス($L_E$)により、次式のカットオフ周波数を持つ1次のローパスフィルタを構成します。

$$f_C = \frac{1}{2\pi \times \frac{L_E}{R_E}} \qquad (式9)$$

ほとんどのスピーカにおいて、この1次の減衰で十分にオーディオ信号を復元することができ、スピーカの電気抵抗で消費される高周波スイッチングエネルギーが過剰に

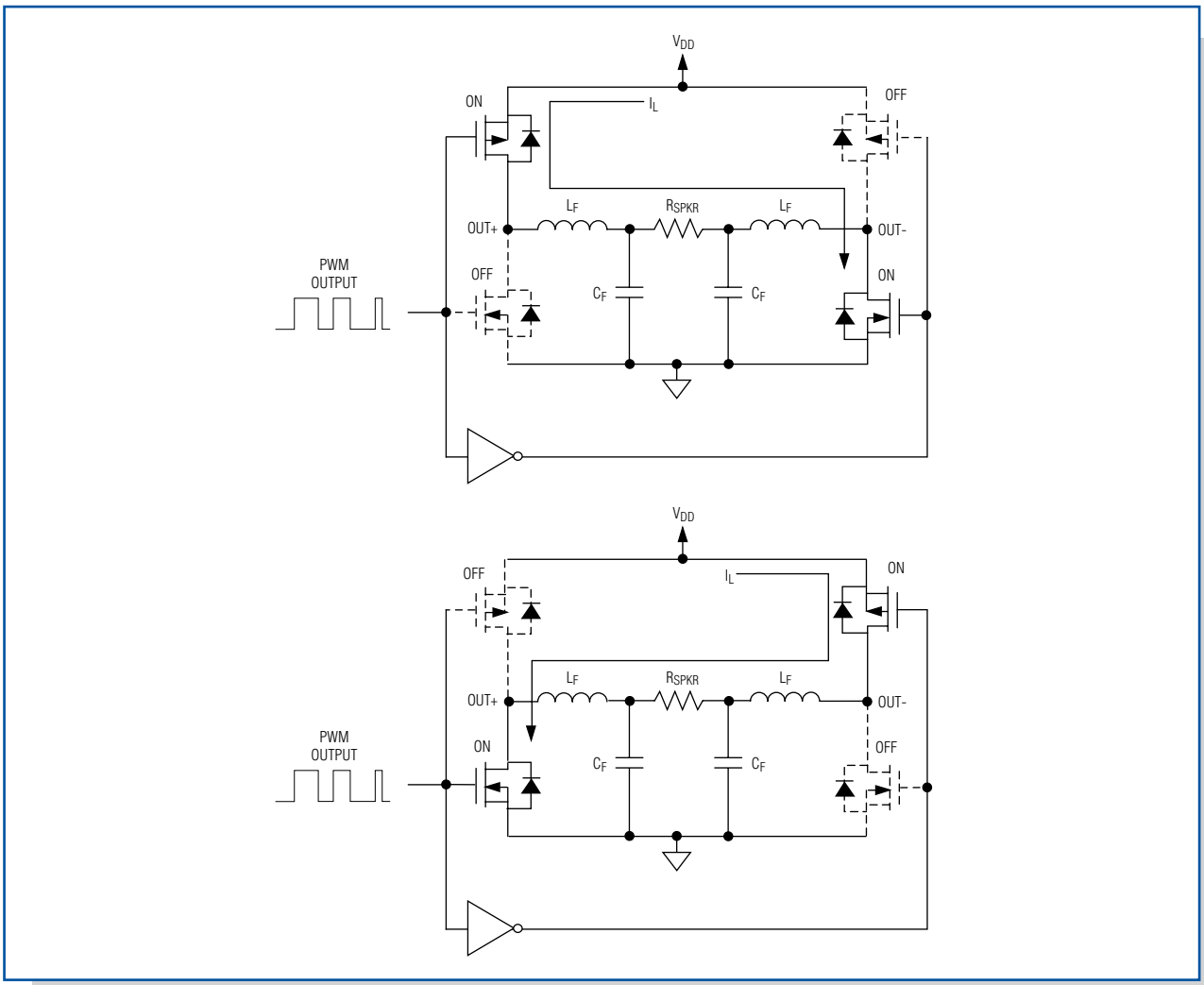



*図5. 従来のフルブリッジD級アンプの出力段では、2つのハーフブリッジ段を用い、負荷を差動駆動します。*

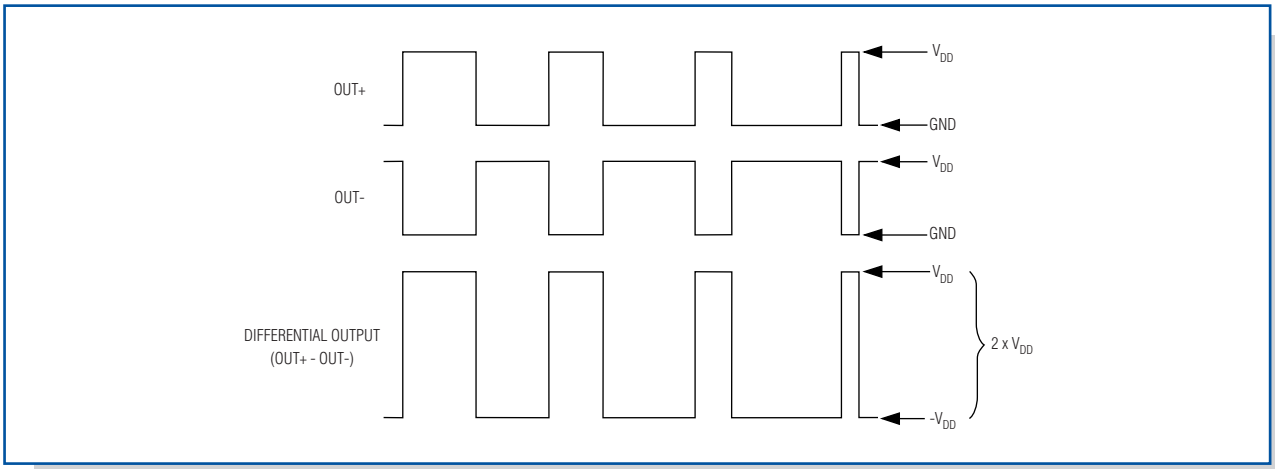



*図6. 従来のフルブリッジD級アンプの出力波形は互いに補完し、負荷の両端に差動のPWM信号が印加されます。*

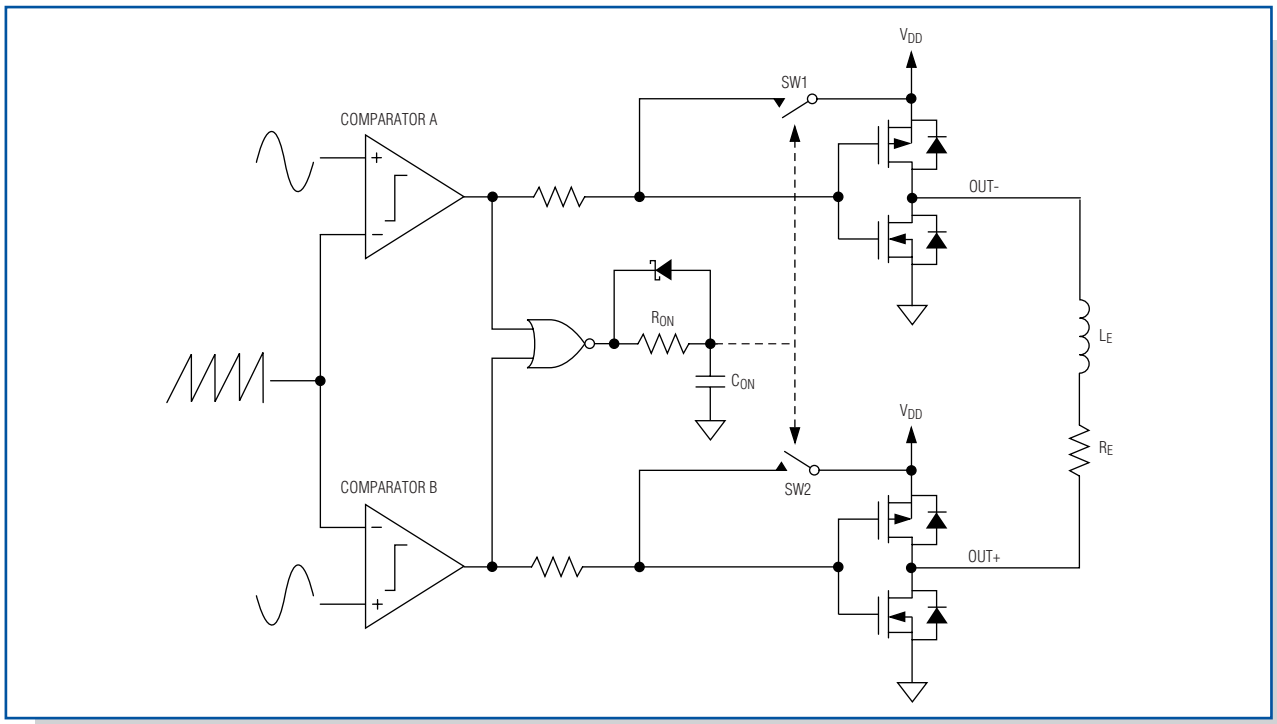



*図7. MAX9700のフィルタレスD級変調器方式の簡略化したファンクションダイアグラム*

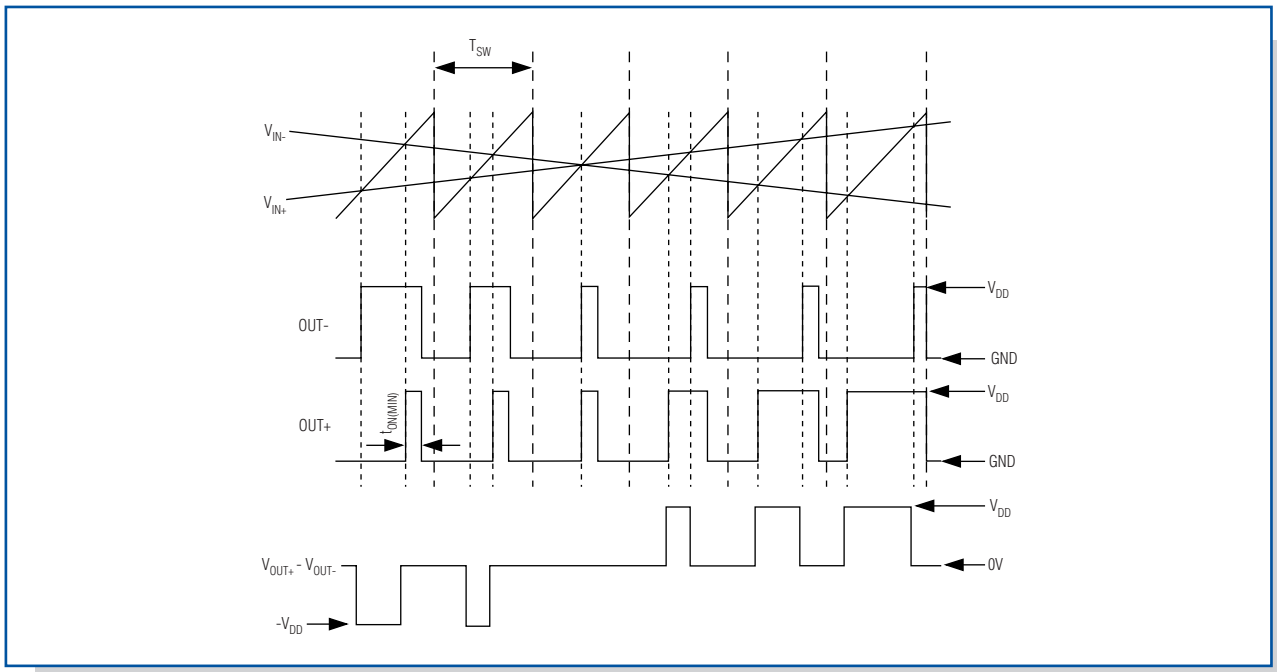



*図8. MAX9700のフィルタレス変調器方式の入力波形と出力波形*

なることも避けられます。減衰しきれなかったスイッチングエネルギーがスピーカを動かすことがあっても、その周波数は人間の可聴周波数外であり、聴感に影響を与えることはありません。フィルタレスのD級アンプを使用する場合、高い出力を得るためには、アンプのスイッチング周波数においてスピーカが誘導性負荷である必要があります。

## スペクトラム拡散変調方式により EMIを最小化

フィルタレス動作が抱える問題点は、スピーカケーブルからEMI放射が発生する可能性がある点です。D級アンプの出力波形は高速過渡エッジの高周波数の方形波であるため、出力スペクトラムには、スイッチング周波数とその整数倍の周波数のところに大きいスペクトルエネルギーがあります。デバイス近傍に外付け出力フィルタがないため、この高周波エネルギーがスピーカケーブルから放射される可能性があります。マキシムのフィルタレスD級アンプでは、スペクトラム拡散変調と呼ばれる特許技術*によってEMI問題の可能性を軽減しています。

スペクトラム拡散変調方式では、D級アンプのスイッチング周波数をディザリングまたはランダムに変化させます。スイッチング周波数は、通常、定格スイッチング周波数の最大±10%の範囲で変化させます。スイッチング波形は、サイクルごとにランダムに変化させても、デューティサイクルは影響されないため、スイッチング波形に含まれるオーディオ成分は変化しません。**図9a**と**図9b**は、スペクトラム拡散変調の効果を示すMAX9700の広帯域の出力スペクトラムです。通常は、スペクトルエネルギーがスイッチング周波数およびその高調波に集中するのですが、スペクトラム拡散変調では、出力信号のスペクトルエネルギーが効果的に拡散されます。つまり、出力スペクトラム中に含まれるエネルギーの総量に変化はありませんが、全体のエネルギーが、より広い帯域に分散されます。この結果、出力に生まれる高周波エネルギーのピークが低くなり、スピーカケーブルからEMIが放射される可能性も最小にします。スペクトラム拡散変調としたことによって、スペクトラムノイズの一部がオーディオ帯域に混入する可能性はありますが、混入したノイズは、フィードバックループのノイズシェーピング機能によって抑止されます。

マキシムのフィルタレスD級アンプの多くは、スイッチング周波数を外部クロック信号に同期させることができます。この機能を活用すれば、アンプのスイッチング周波数を影響を受けにくい周波数帯に設定することができます。

スペクトラム拡散変調は、フィルタレスD級アンプのEMI性能を大幅に高めますが、FCCやCEで規定された放射基準に適合できるスピーカケーブルの長さには一定の限界があります。スピーカケーブルが長すぎて放射試験に合格できない場合には、出力波形の高周波成分をさらに減衰させるため、外付け出力フィルタが必要になる場合もあります。スピーカケーブルがそれほど長くない一般的なアプリケーションでは、フェライトビーズ/コンデンサによるフィルタを出力に追加すれば十分です。EMI性能はレイアウトの影響も大きいため、FCCやCEのレギュレーションを満足するためには、PCBレイアウトのガイドラインにも厳密に従う必要があります。

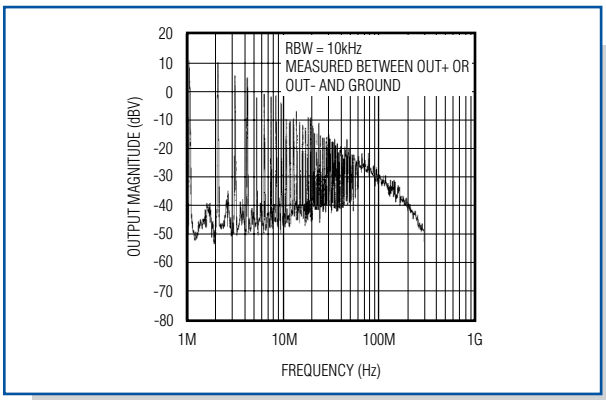



*図9a. 固定スイッチング周波数動作のMAX9700の広帯域出力スペクトラム*

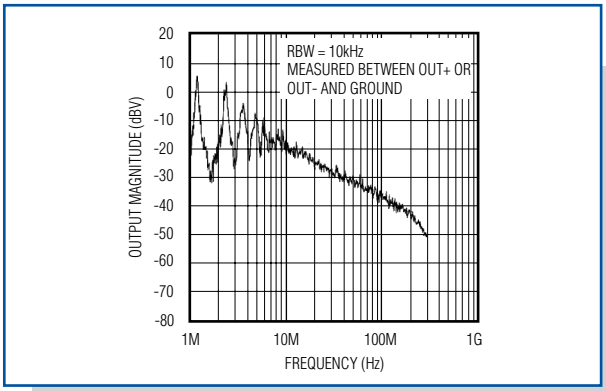



*図9b. スペクトラム拡散変調によりMAX9700のスペクトルエネルギーが広い帯域に拡散*

## まとめ

最近のD級変調技術の進歩で、今までリニアアンプの優勢だったアプリケーションでもD級アンプが使われるようになりました。現代のD級アンプは、高い電力効率に加えて、AB級アンプの特長(高い直線性と少ない実装面積)も、すべて、持つようになりました。現在、さまざまなアプリケーションに適したいろいろな種類のD級アンプが提供されています。バッテリ寿命、実装面積要求とEMI適合が重視される低電力のポータブルアプリケーション(携帯電話やノートパソコンなど)から、ヒートシンクの小型化と発熱量の削減が非常に重要となる高出力アプリケーション(車載オーディオシステムやフラットパネルディスプレイなど)まで、さまざまなアプリケーションがあります。D級アンプの基本の理解とその今日の技術的発展を理解すれば、アプリケーションに適したアンプを選び、それぞれが持つメリットとデメリットを正しく比較検討できるようになるでしょう。

*米国特許#6,847,257。

# 進化する組込みセキュリティ

*電子システムの設計では、あらゆる側面においてセキュリティの問題が急速に重要度を増しており、今後、メーカや回路設計者は、今まで存在しなかった課題に直面することになります。従来、電子機器のセキュリティが問題となるのは、ソフトウェア関連の技術であるか、あるいは、金融や軍用、入出場管理といった限られた市場を対象とした特殊なハードウェアくらいなものでした。しかし今後は、満足しなければならない規格や取得しなければならない認証、学ばなければならない技術的知識が次々と登場し、設計者を取りまく状況は大きく変化しようとしています。このような知識の大半は、長年、組込型電子システムの設計に携わってきた技術者にとって、なじみのないもののはずです。このような技術のトレンドを理解し、それが設計や製造のコストにどのような影響を与えるかを知ることは、今後、組込みシステムのメーカにとって重要なことになります。*

ソフトウェア/ファームウェアの完全性を確保することは非常に困難な課題であるため、複雑なセキュリティ実装において弱点とならず、セキュリティを確保するという負担はハードウェアが負わなければなりません(11ページの「アペンディックス1ー分類」を参照)。Trusted Computing Group™など、新しい規格策定の団体が組織されるとともに、DRM (デジタル著作権管理)が声高に叫ばれるようになったことから、消費者用、メディア用、工業用、医療用、自動車用、テレコミュニケーション用など、さまざまな機器においてセキュリティが急速にクローズアップされるようになりました。この問題は、もちろん、政府や国のセキュリティシステムのアップグレードにも、電子バンキングや電子商取引アプリケーションの普及にも関係があります。

しかし、どのようなセキュリティソリューションも、十分な効果を持つためには、物理的なタンパー防止策とそれを実現する方法を検討する必要があります。現在、もっともセキュリティが優れていると言われるマイクロプロセッサやFPGA、スマートカード、各種セキュリティ部品も、それぞれ、攻撃の方法が必ず存在します。このように脆弱性がなくならないということは、システムがダウンしている間も「稼動している」アクティブ回路の一部に、重要情報や知的財産を引きだそうとする、あるいは盗もうとする行為を検出する機能を持たせる必要があります。そのためには、デバイスの消費電力が非常に少ないことが必要です。また、重要な情報を保持する回路の周りにセキュリティフェンスを構築する各種センサとのインタフェースを持ったタンパー反応型のパッケージに収めておく必要もあります。

暗号化アルゴリズムの強さが、攻撃対象でなくなったことも認識しておく必要があります。鍵を盗む方法を考えたほうが、容易であり、より有益であるからです。そのため、物理的なハードウェア保護の要件が注目されるようになりました。

## 新しく登場するセキュリティ規格

最新のセキュリティ規格は、米国のNIST (National Institute of Standards and Technology)が定めたものと、英国のCESG (Communications-Electronics Security Group)が定めたものをベースとしています。両組織は、それぞれ、FIPS 140-1とITSECを策定しました。

新しい規格が次々と登場するとともに、必要とされるセキュリティのレベルが高まっていることから、これらの規格から優れている点を参考にして、ひとつの規格にまとめようという動きがあります。これが「Common Criteria」(共通基準)と呼ばれるものです(12ページの「アペンディックス2—一般的な認証/規格」を参照)。そのため、NISTもFIPSを140-2にアップデートするとともに、今後は、Common Criteriaに近づけていくとしています。

金融処理に対応した機器の普及に伴い、他の規格も考慮しなければならないことが増えています。その中でも特に重要なのが、MasterCardとVisaが策定したEMV (European MasterCard® Visa®)とPCI PED (デビットカード、PIN入力機器)です。今後は、注目を集めるDRMとの兼ね合いもあり、ユーザやシステムのアイデンティティを守りつつ、モバイルプラットフォームで金融関連のトランザクションを行うことの増加もあり、かつ、FIPS 201 PIV (Personal Identity Verification)のような政府構想が登場して来るであろうことから、これらの認証規格は次第に厳しくなっていくものと考えるべきでしょう。

これらの規格は、いずれも、最終製品のカテゴリーごとに認証取得に必要な物理的セキュリティ要件が定められています。このようなセキュリティでは、一般に、シリコン、つまりプロセッサのレベルからスタートして重要情報やアルゴリズムにアクセスすることができるプロセッサやメモリ、データパスを囲むパッケージングまで、複数のレイヤで対応することが求められます。最終製品が認証を取得するためには、認証ラボで詳細な試験を受けるとともに、さまざまな物理的セキュリティの脅威について、それぞれどのように対応しているのかを記したセキュリティターゲット文書を作成する必要があります。規格によっては(PCIなど)、新しい基準を満足するために、既存製品に対してどの部分のセキュリティが改善されたのかをメーカが示さなければならないものもあります。どのようにセキュリティを製品に組み込まなければならないかは曖昧模糊としており、そのような要件を今まで取り扱ったことのないメーカや設計チームにとってはいらいらすることが多いはずです。

どのレベルのセキュリティ認証を受けなければならないかという条件も、場合によって大きく異なります。しかし、それでも物理的タンパー保護に対する要求が厳しくなる一方であることは確かです。この背景には、高度な攻撃を仕掛けるために必要な高度な解析ツールと技術的ノウハウの普及があるからです。

## DS3600ファミリのセキュリティコントローラ

サイズとコスト、電力消費を抑えつつ、物理的セキュリティのニーズの高まりに対応することができるように、マキシム/ダラスセミコンダクタでは、物理的ハードウェア保護のニーズを考慮したセキュリティコントローラのシリーズを発表しました。それがDS3600製品ファミリで、組込みシステムを設計する際、現在および将来の認証要件として必要なセキュリティのレイヤを追加することができます。

このファミリには高度な温度モニタリング機能と漏れ電流の小さなコンパレータ、極低温攻撃に対する保護機能、経過時間を計る機能やタンパーを記録する機能など、暗号用サブシステムに必要とされる各種機能が内蔵されています(**図1**)。この豊富な機能の中核となるのが、トップレベルの暗号鍵とセキュリティ認証を守るユニークなメモリセル構造です。従来のメモリセルでは、過去に保存された情報の痕跡が残るデータインプリンティングと呼ばれる現象が起きますが、この痕跡は、さまざまな攻撃方法で抽出することができます。DS3600の内蔵メモリはインプリンティングが起きないタイプであり、よく攻撃されるこの特性をなくしたはじめてのデバイスです。また、メモリアレイ全体をハードウェアコマンドひとつで瞬間的に消去することもできます。このような機能を持つこのセキュリティコントローラなら、消費電力を大幅に削減することができるとともに、暗号鍵が記録されたメモリをホストプロセッサの介入で保護する必要性がなくなります。

このファミリのコントローラにはさまざまな機能が統合されており、同等の機能をディスクリートで実現するためには、40個以上の部品が必要になります。このようにDS3600ファミリは、サイズとコストを削減するとともに、必要電力も従来に比べてごくわずかであり、かつ、セキュアなマイクロプロセッサなどの高価な部品も不要にしてくれます。このため、セキュアではないプロセッサを用いたアーキテクチャを使ってきた組込みシステムのメーカが認証を取得し、ソフトウェアに関する過去の知的財産を利用することが可能になります。なお、このファミリは認証要件を満足するように設計されているため、製品認証に必要な文書の作成においても大きな助けとなります。

## アペンディックス1—分類

必要なセキュリティレベルを求めるためにIBM®が10年以上も前に定めた分類が、現在も、受ける可能性のある攻撃を分類する際に使われています。

### クラスI (賢いアウトサイダー)

- 知能レベルは高いことが多い。
- システムについては、十分な知識を持っていない。
- 比較的高度な機器を利用することができる場合がある。
- システムに弱い部分を発生させるのではなく、既存の弱点を攻撃してくることが多い。

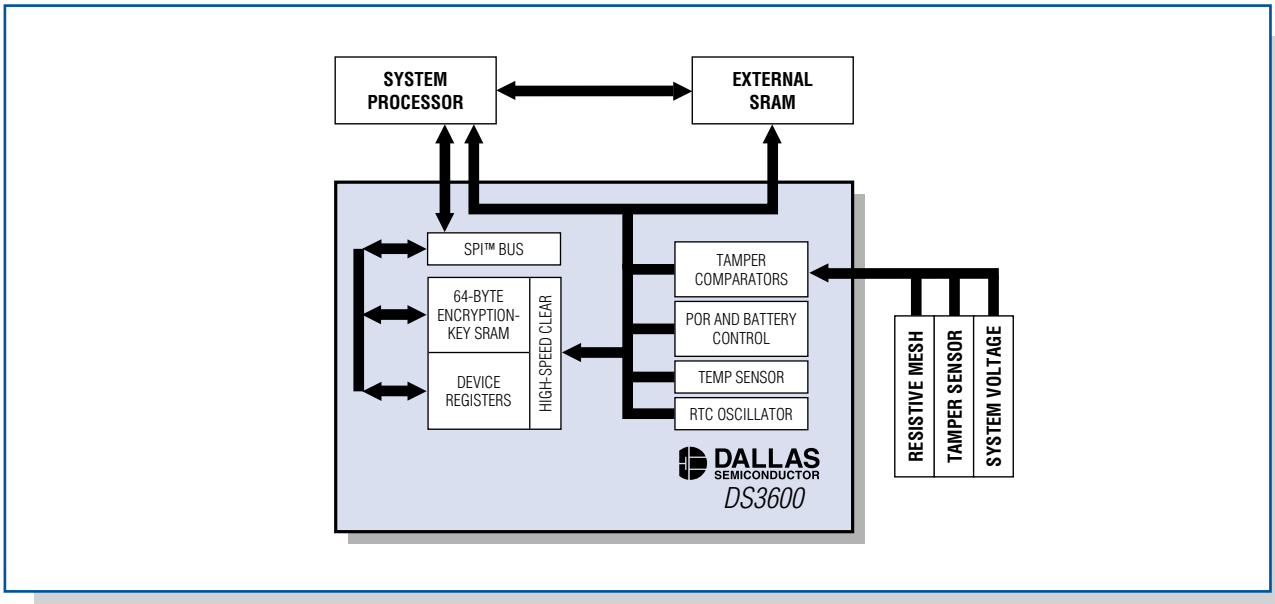



*図1. 耐タンパー性を持つDS3600コントローラは、ハイインピーダンスのコンパレータを持ち、低消費電力でシステムのモニタリングを継続し、高いレベルのCommon Criteria要件を満足することができます。*

**クラス II (豊富な知識を持つインサイダー)**

- 技術的な専門教育を受け、豊富な経験を持つ。
- システムについても一定の知識を持ち、システムのほとんどにアクセスすることができる可能性がある。
- 高度な分析機器やツールを利用可能な場合が多い。

**クラス III (資金力のある組織)**

- ほとんど無尽蔵の資金を持つ。
- スペシャリストのチームを編成することができる。
- 最先端の解析ツールを入手あるいは利用することができる。
- 詳細な解析や高度な攻撃の組立てを行うことができる。
- クラスIIの豊富な知識を持つインサイダーを攻撃チームの一員とすることが多い。

認証を受けようとするシステム設計者は、少なくとも、以下のよくある攻撃シナリオに関連する脅威について記述することができる必要があります。

**物理的攻撃**

- パッケージの侵害
  - 切断、エッチング、イオンあるいはレーザを使った穿孔
  - リバースエンジニアリング(複数のサンプルデバイスを必要とする)
    - 回路図の作成
    - ROMコードの抽出
    - 鍵となる回路素子(メモリ)の物理的位置を特定
  - メモリへのアクセス確保
    - FIBワークステーションによる回路変更
    - 電離放射線の照射による特定トランジスタの状態変更
    - マイクロプロービング
    - メモリセル酸化物の高度な分光分析

**非侵襲型攻撃**

- 電離放射線や高温/極低温
- 電圧変動やクロック障害の誘発
- 電力差分解析

## アペンディックス2—一般的な認証/規格

### NIST FIPS 140-2レベル1～4

- CESG ITSEC E1～E6
- Common Criteria EAL1～EAL7
- EMV 4.1レベル1～2 (基本的にバンキング/POSで使用)
- ZKA (基本的にバンキング/POSで使用)
- PCI PED (基本的にバンキング/POSのPIN入力で使用)

**業界は「Common Criteria」への統一に向かって動いている**

- さまざまな保護プロファイルとセキュリティターゲット、スキームが存在しうる。
  - UK EN45011:1998
  - ISO 15408
  - Trusted Computer Groupも、保護プロファイルを追加
  - IBM Trusted Mobile Platformセキュリティ

以下は、関連するセキュリティレベルの説明とともにこれら規格団体についてまとめたものです。

### NIST FIPS 140-2

**FIPS 140-2**には、4レベルのセキュリティ保証が定められています。最低レベルから最高レベルに向かい、各レベルは下のレベルに上乗せする形となっています。

**レベル1**とは、データ通信用暗号標準(DES)、トリプルDES (3DES)、次世代暗号化規格(AES)など、NIST標準暗号アルゴリズムを製品が適切に実装していることを示す。

**レベル2**とは、製品にはタンパーが明らかとなるコーティングが施されており、デバイスを破損するとすぐにわかるようになっていることを示す。

**レベル3**とは、回路部品に対する物理的攻撃をモジュールが検出した場合、暗号モジュールが保存している鍵を削除するようになっていることを示す。レベル3の製品は、認証アクセスを必要とする。

**レベル4**は、過冷却など、物理的なアクセス制御を妨害しようとする攻撃に対する保護を必要とする。

セキュリティ製品の多くは、FIPS 140-2レベル2あるいはレベル3の認証を受けています。いずれも、モジュールが制御環境下におかれている限り、十分な認証です。

### Common Criteria

Common Criteriaでは、EAL (評価保証レベル：evaluation assurance level)というスケールを用います。セキュリティターゲット文書と保護プロファイル文書に規定された機能要件を製品が満足しているかどうかを評価するものです。文書はベンダーが作成し、Common Criteriaの評価担当者が評価を行います。EALレベルにはEAL1からEAL7までありますが、ほとんどの製品は、Common Criteria EAL4以下の認証となっています。

**EAL1** 製品は基本的な要件を満たしている。

**EAL7** 製品は、非常にセキュアな環境で必要とされる要件を満たしている。

EAL5、EAL6、およびEAL7の認証は非常に厳しく、機能試験だけでなく、開発プロセスや理論的な枠組みの評価も行われます。

なお、EALのレーティングは、セキュリティターゲットの文書化と保護プロファイルの文書化をまず評価しないと、意味がありません。

*Embedded Systems Europeの2006年10月号にも、同様のアーティクルが掲載されています。*

IBMはIBM Corp.の登録商標です。
MasterCardはMasterCard Worldwideの登録商標です。
SPIはMotorola, Inc.の商標です。
Trusted Computing GroupはThe TCGの商標です。
VisaはVisaの登録商標です。

# シリアルバスの選択

*最先端のエレクトロニクス製品の中心にはマイクロコントローラ(μC)があり、周辺機器デバイスと通信を行っています。昔のμCでは、周辺機器がメモリにマッピングされ、データとアドレスバスに接続されていました。この場合、各コンポーネントの位置は、アドレスラインからデコードしたチップセレクト信号により、限られたアドレス範囲における一意の位置として決定されます。このようなインタフェースとすると、最小限必要なピン数は、電源とグランド以外に、8 (データ) + 1 (R/$\overline{W}$) + 1($\overline{CS}$) + n (アドレスライン数) [n = log2(内部レジスタ数あるいはメモリバイト数)]となります。16バイトのデバイスでは、8 + 1 + 1 + 4 = 14ピンが通信用として必要になります。アクセスが速いというメリットはありますが、ピン数が多いとパッケージサイズと全体的なコストが上昇するというデメリットもあります。コストとパッケージサイズを縮小したいなら、シリアルインタフェースの採用が真っ先に浮かぶでしょう。*

シリアルバスを選ぶのは簡単なことではありません。データレートとビットシーケンス(最初に来るのが最上位ビットか最下位ビットか)、電圧だけでなく、以下の点も考慮する必要があります。

- 周辺機器の選択方法(ハードウェアがチップセレクト入力経由で選ぶのか、ソフトウェアプロトコルで選ぶのか)
- 周辺機器とμCとの同期方法(ハードウェアクロックラインを使うのか、データストリームにクロック情報を組み込むのか)
- データ伝送はシングルラインとするのか(「ハイ」と「ロー」をスイッチングする)、2線の差動接続とするのか(2線が同時、逆向きに電圧を変化させる)
- 通信ラインの両端ともインピーダンスマッチングを取り、終端処理されている状態か(差動信号でよく使われる形式)、あるいは、両端とも終端処理されていないか、一端のみ終端処理されている状態か(シングルエンドバスでよく使われる形式)

**表1**は、組合せとよく使われるバスシステムの関係です。組合せとしては16種類が考えられますが、製品が販売されているパターンは4種類のみとなっています。

このようなパラメータ以外に、アプリケーション側の要件として、電力の供給や絶縁、ノイズ耐性、μC (マスタ)と周辺機器(スレーブ)間の最大距離、ケーブルの構造(リニア、スター、ワイヤ逆接の影響を受けない)などの条件が加わる場合があります。ビルオートメーションや工業用制御、ユーティリティメータの読取りなどは、このような条件をすべて勘案して、それぞれに適した規格が策定されています。[1、2]

## 回路基板からバックプレーンまでのアプリケーションの要件

周辺機器機能を実現するシリアルバスは、システム全体にとって負担となるものであってはなりません。特に、以下の点に注意が必要です。

- ルーティングが容易な接続であること(信号数が少ない方が良い)。
- ソフトウェアで実装しやすいプロトコルであること(あるいは、使用するμC/μPがネイティブでサポートしているプロトコルとする)。
- デバイス機能を適切に選択できること。
- 拡張が容易なバスであること。

必要な信号数が最も少ないのは、シングルエンド、セルフクロッキングのシステムでアドレッシングをソフトウェアプロトコルで行う場合です。このような条件を満たすのは、表1に示す1-Wire®とLINバス、SensorPath™です。ただし、このような形式では、他にも検討しなければならない点があります(**表2**参照)。

### 表1. シリアルバスシステムの概要

<table>
<tr><td></td><td colspan="4">アドレッシング(選択)</td><td></td></tr>
<tr><td>同期方法</td><td colspan="2">プロトコル</td><td colspan="2">チップセレクトライン</td><td>インピーダンス</td></tr>
<tr><td rowspan="3">セルフクロッキング</td><td>1-Wire、LINバス、SensorPath</td><td></td><td></td><td></td><td>マッチングなし</td></tr>
<tr><td></td><td>RS-485、LVDS、CAN、USB 2.0、FireWire®</td><td></td><td></td><td rowspan="2">マッチングあり</td></tr>
<tr><td rowspan="2">クロックライン</td><td></td><td></td><td></td><td></td></tr>
<tr><td>I²C、SMBus™</td><td></td><td></td><td>SPI™、MICROWIRE™</td><td>マッチングなし</td></tr>
<tr><td></td><td>シングルエンド</td><td>差動</td><td>シングルエンド</td><td></td></tr>
<tr><td></td><td colspan="3">伝送モード</td><td></td></tr>
</table>

## 表2. 1-Wire、LINバス、SensorPathの詳細比較

| | 1-Wire[3] | LINバス[4] | SensorPath[5] |
|---|---|---|---|
| 物理的なネットワークサイズ | ボードやバックプレーンは最大300mまで拡張可能 | 最大40m | ボード |
| ネットワークドライバ(ハードウェア) | RS-232、I²C、USB、汎用μPポートピン[6]、[7]用のドライバがある | μPポートピン用のドライバがある | Super-I/Oチップ、μPポートピン |
| ネットワークドライバ(ソフトウェア) | μC用を含め、さまざまなプラットフォームで無償ドライバが存在する[8] | Freescale™ μC用の無償ドライバが存在する | なし |
| 電源 | データライン経由(一般的なケース)、ローカル$V_{CC}$ (一部デバイス) | データライン経由 | ローカル$V_{CC}$ |
| データレート | 最大15kbps (標準)あるいは最大125kbps (オーバードライブ)[9] | 最大20kbps | データによる最大20kbps |
| ネットワークインベントリ | 「サーチROM」ネットワーク機能による | なし。メッセージベースのアドレッシングを行う | サポートなし |
| 利用できるデバイス機能 | シリアル番号、計測、セキュアメモリなど、さまざまなデバイス機能が利用可能 | 自動車アプリケーションで必要とされる機能に限られる | 温度センサと電圧ADCのみ |

### 物理的なネットワークサイズ

アプリケーションがボードサイズに限られるのはSensorPathだけです。1-Wireバスは、適切なハードウェアとソフトウェアネットワークドライバを採用し、条件がよければ、かなりの長距離にも対応することができます。

### ネットワークドライバ

プロトコルを使用するネットワークでは、通信波形を生成する(リンク層)、ネットワークにおけるスレーブ/ノードを個別に特定し、アドレスする(ネットワーク層)、デバイスとデータの送信/受信を行う(トランスポート層)ソフトウェアドライバが必要です。ソフトウェアドライバは、オペレーティングシステムと通信ポートに適したものが必要となります。1-Wireの場合は、ハードウェアドライバチップ(マスタ)とCOM、LPT、USB、I²Cといったポート用のアダプタがあります。終端処理がされていない大規模ネットワークでは、ケーブル端やコネクタ、スタブからの反射によって性能が低下する場合があります。

### 電源

ネットワークに接続されたデバイスは、電源を与えてやらないと動作することができません。費用対効果が最も高い方法は、データラインを通じて電源を供給する方法です。「寄生電源」と呼ばれるこの方法では、(パワーダウンモードなどでも)システム診断情報を読むことができます。実例は、図3およびアプリケーションノート178:「1-Wire製品によるプリント回路基板の識別」[10]をご覧ください。なお、寄生電源とすると、電力供給用の時間をとる必要があり、最大データレートが下がります。

### データレート

一般に、データレートを高めるためには、ネットワークサイズを小さくする必要があり、逆も同様です。1-Wireシステムでは、電源供給をする関係から、ネットワークに接続されているスレーブデバイスの数とケーブルの総延長(静電容量)によって最大データレートが変化します。

### ネットワークインベントリ

この機能は、ネットワークに接続されたスレーブデバイスの数と種類、アドレスをマスタが確認するものです。構成がダイナクックに変化するネットワークでは、この機能が必要になります。実例は、「ダラス・エンジニアリングジャーナル」(vol. 2)[11]の22ページをご覧ください。

### 利用できるデバイス機能

アプリケーションが必要とする機能が利用できなければ、インタフェースがベストであっても意味がありません。LINバスやSensorPathに比べると、1-Wireは、利用できるデバイス機能が豊富に存在します。

### I²C/SMBus 対 1-Wire

クロックラインがサポート可能なアプリケーションでは、I²C[12]とSMBus[13]もデバイスとして選ぶことができます。初期のSMBusは、100kbpsのI²Cバス仕様にタイムアウト機能を追加したと言ってよい仕様となっていました。このタイムアウト機能があると、バスドライバとの同期をノードが失っても、バスが作動不能とならずにすみます。I²Cシステムでは、このような状況から回復するためには、パワーオンリセットを行う必要があります。1-Wireシステムでは、リセット/プレゼンスーディテクトサイクルで通信インタフェースをリセットし、スタート状態とします。I²C/SMBusは、クロックラインを持つ以外に、バスでやりとりされるバイトごとに確認応答ビットの発生があります。このため、データレートが実質12%低下します。トランザクションは、まず、スタート状態から始まり、デバイスアドレスとデータ方向ビット(読み出しか書き込みか)と続いて、ストップ状態で終わります。1-Wireシステムでは、まず、ネットワーク層の要件が満足される必要があります(つまり、特定デバイスの選択、サーチROM、またはブロードキャスト)。その後、デバイス固有のコマンドコードで通信が始まります。なお、コマンドコードによっても、データ方向(読出しか書込みか)が影響を受けます。

オリジナルとなったI²CにもSMBusにも、アドレス空間が7ビットに制限されているという大きな問題があります。これに対してデバイスの種類は127を超えているため、スレーブアドレスからデバイス機能を得ることはできません。さらに、I²Cデバイスの多くは、1本のバスに同種類のデバイスを複数、接続できるように、ユーザがアドレスビットの一部を任意に設定することができるようになっています。この特長で、利用できるアドレス空間はさらに狭くなります。このため、一般には、バスを複数のセグメントに分割し、ソフトウェアによってアクティブなセグメントを切り替えることによって、アドレスの衝突を回避します。このセグメンテーションには、必要なハードウェアが増えるという問題と、アプリケーションファームウェアが複雑になるという問題があります。また、I²Cにはデバイスを列挙するインベントリ機能がなく、動的に変化するシステムの取り扱いが難しいという問題もあります。この問題は、*SMBus Specification Version 2.0*[13]で導入されたAddress Resolution Protocolによって解決済みですが、この機能をサポートしたSMBusデバイスはまだほとんど出回っていません。

### SPIとMICROWIRE

SPI[14]とそのサブセットであるMICROWIRE[15]は、デバイスごとに1本ずつ、チップセレクトラインを必要とします。このチップセレクト信号があるため、SPIプロトコルでは、メモリアドレスやステータスレジスタの読出しや書込みのコマンドだけが定義されています。確認応答機能もありません。SPIデバイスは、普通、データ入力とデータ出力に異なるピンが割り当てられています。読出し以外ではデータ出力がトライステートとなるため(ディセーブルがある)、2本のデータピンを接続して1本の双方向データラインとすることができます。SPIが選ばれるのは、他のバスシステムでは利用できない機能を使いたい場合か、2Mbps以上に達する比較的高いSPIのデータレートを利用したい場合です。SPIとMICROWIREの欠点は、各チップにアドレスする際に$\overline{CS}$信号を生成するデコーダが必要なことです。しかし、アドレスの衝突はおきません。I²Cと同じでインベントリ機能はありません。マスタが論理アドレスからデバイス機能を削除することはできないため、動的に変化するネットワークの管理は困難です。

### RS-485、LVDS、CAN、USB 2.0、およびFireWire

これらの規格は、差動信号の例として取りあげます。このうち、もっともスピードが速い2つの規格、FireWire[16]とUSB 2.0[17]は、電気的にはポイントトゥポイント接続となります。ハブと呼ばれる高度なノードによってツリー型トポロジの仮想バスを実装することで、ソースからエンドポイント(USB)へ、あるいはピアトゥピア(FireWire)に、480Mbps (USB 2.0)あるいは1600Mbps (FireWire)という最大バーストデータレートでデータパケットを転送することができます。パケットサイズが限られていること、また、受信/バッファリング/再送信という通信コンセプトであることから待ち時間が発生し、実際に実現できるデータスループットは低くなることがあります。トポロジとプロトコルから許容される限界としては、ノード数がUSBは126、FireWireは63で、ノード間距離は、パッシブケーブルを使った場合で最大4.5mとなります。PC周辺機器やマルチメディア機器、工業用制御、航空機(FireWireのみ)などのアプリケーション用として設計された規格であり、USBデバイスやFireWireデバイスは、システム(ホットスワップ)の電源を落とさなくても接続できるようになっています。このため、ネットワークの構成を動的に変化させることができます。

LVDS[18]、RS-485[19]、CAN[20]は、マスタとスレーブを持つ、あるいは複数のマスタを持つ真にリニアなバス構造とすることができます。この中で最速の規格、LVDS (低電圧作動信号)は、バス延長が10m以内のとき、100Mbpsで動作することができます。実際に実現できるデータレートとスループットは、ネットワークのサイズによって上下します。LVDSはバックプレーンアプリケーション用の電気的規格として策定されており、ホットスワッピングに対応するとともに、プロトコルが規定されていません。

RS-485も、電気的なパラメータだけが規定されています。RS-485では、ノードではなく負荷とバスあたりの最大負荷数(32)が規定されています。ひとつの電気的ノードが持つ負荷は1未満です。データレートは、通常、ネットワークサイズが12mで35Mbps以下、1200mで100kbps以下で、データ収集や制御のアプリケーションに適した値となっています。RS-485機器では、もともとRS-232用に設計されたコンポーネントをベースとしたプロトコルがよく用いられます。

これに対し、CAN (コントローラエリアネットワーク)は、自動車アプリケーションや工業用オートメーションを対象として、非常に高いレベルのセキュリティが実現できる分散型リアルタイム制御のシリアル通信プロトコルが定義されています。データレートはネットワークサイズにより、40mで1Mbpsから1000mで50kbpsという範囲になります。アドレッシングはメッセージベースであり、プロトコルの仕様によるノード数の制限はありません。CANノードはホットスワップが可能で、ネットワーク構成を動的に変化させることができます。

## まとめ

シンプルな低コストのバスシステムの中では、LINバスやSensorPathよりも1-Wireのほうがデバイス機能の選択肢が広く、ネットワークドライバも豊富にあります。I²CとSMBusはデータとグランドリファレンス以外にクロックラインと$V_{CC}$電力が必要になりますが、デバイス機能という面では選択肢が非常に豊富です。SPIとMICROWIREはチップセレクトラインが追加で必要になりますが、データレートが非常に高いという特長を持ちます。

1-Wireのインタフェースとプロトコルは寄生電源とネットワークインベントリの機能を持ち、ホットスワッピングをサポートしていますが、このような特長を持つのは、この他、差動信号を使用する高速システムかSMBus 2.0対応製品しかありません。ホットスワップ対応の1-Wireデバイスとして最も広く知られているiButton®では、ホットスワッピングが通常の使用方法となっています。1-Wireデバイスは、グローバル識別[21]や回路基板/アクセサリ識別、認証[10]、温度検出、アクチュエーションといった機能において高い効率を発揮することが実証されています。この他、成功例としては、セキュアメモリとチャレンジアンドレスポンス機能を持ち、双方向認証によって最小限のコストで知的財産を守ることができる1-Wireデバイスがあります。[22、23]

*Electronic Productsの2006年9月号にも、同様のアーティクルが掲載されています。*

### 参照


1. Interbus Club. www.interbusclub.com/ (工業オートメーション) (英文のみ)
2. The valid M-Bus standard. www.m-bus.com/ (メータ読取り) (英文のみ)
3. “Overview of 1-Wire Technology and Its Use.” japan.maxim-ic.com/AN1796 (1-Wireの基本) (英文のみ)
4. LIN Local Interconnect Network. www.lin-subbus.org/ (LIN規格) (英文のみ)
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) (英文のみ)
6. 「高度1-Wireネットワークドライバ」 japan.maxim-ic.com/AN244 (ハードウェアドライバ)
7. 「高信頼性1-Wireネットワークのガイドライン」 japan.maxim-ic.com/AN148 (1-Wireネットワーク)
8. 「1-Wireソフトウェアリソースガイド」 japan.maxim-ic.com/AN155 (ソフトウェアドライバ)
9. 「複数スレーブを備える1-Wireネットワークの回復時間の算出」 japan.maxim-ic.com/AN3829 (回復時間)
10. 「1-Wire製品によるプリント回路基板の識別」 japan.maxim-ic.com/AN178 (ボード識別)
11. 「ダラス・エンジニアリングジャーナル」 vol. 2. pdfserv.maxim-ic.com/jp/ej/DallasEJ2.pdf (ダイナミックネットワーク)
12. “The I²C-Bus Specification, Version 2.1, January 2000.” www.nxp.com/acrobat_download/literature/9398/39340011.pdf (I²C) (英文のみ)
13. “USB specification” www.smbus.org/specs/ (SMBus) (英文のみ)
14. “M68HC11E Family.” www.freescale.com/files/microcontrollers/doc/data_sheet/M68HC11E.pdf (SPI) (英文のみ)
15. “MICROWIRE™ Serial Interface.” www.national.com/an/AN/AN-452.pdf (MICROWIRE) (英文のみ)
16. The Air Power Australia Website. “Firewire.” www.ausairpower.net/OSR-0201.html (FireWire) (英文のみ)
17. “USB 2.0 Specification.” www.usb.org/developers/docs (USB規格) (英文のみ)
18. National Semiconductor. “LVDS Owner’s Manual: Low-Voltage Differential Signaling.” www.national.com/appinfo/lvds/files/ownersmanual.pdf (LVDS) (英文のみ)
19. Lammert Bies’ Website. “RS485 serial information.” www.lammertbies.nl/comm/info/RS-485.html (RS-485) (英文のみ)

20a. Robert Bosch GmbH. “CAN Specification, Version 2.0.” www.semiconductors.bosch.de/pdf/can2spec.pdf (CAN規格 パートA) (英文のみ)

20b. CAN in Automation (CiA). “CAN Specification 2.0, Part B.” www.can-cia.org/downloads/ciaspecifications/?269 (CAN規格 パートB) (英文のみ)

21. 「1-Wireデバイスによるグローバル識別番号の作成」 japan.maxim-ic.com/AN186 (グローバル識別番号)
22. 「研究開発の投資の保護—双方向の認証とセキュアなソフトによる機能の設定」 japan.maxim-ic.com/AN3675 (双方向認証)
23. 「1-Wire SHA-1セキュアメモリによるXilinx® FPGAのIFFコピー防止」 japan.maxim-ic.com/AN3826 (FPGA保護)



1-WireとiButtonは、Dallas Semiconductor Corp.の登録商標です。
FireWireはApple Computer, Inc.の登録商標です。
FreescaleはFreescale Semiconductor, Inc.の商標です。
SensorPathとMICROWIREは、National Semiconductor Corp.の商標です。
SMBusはIntel Corp.の商標です。
SPIはMotorola, Inc.の商標です。
XilinxはXilinx, Inc.の登録商標です。

# ひとつの接点で制御とメモリ、セキュリティ、ミックスドシグナル機能を追加

## 概要

ダラスセミコンダクタの1-Wireバスは、ホスト/マスタコントローラと、ひとつあるいは複数のデータラインを共有するスレーブとの間で双方向半二重通信を実現するシンプルな信号伝達スキームです(**図1**)。スレーブデバイスは、電力もデータ通信も、この1-Wireラインだけで受け取ることができます。電力供給については、ラインがハイ状態となっている間に電荷を内蔵コンデンサで捕らえ、ラインがロー状態となってデータ通信を行っている間、この電荷でデバイスを動作させる仕組みとなっています。1-Wireのマスタは、通常、オープンドレインのI/Oポートピンと、3V～5V電源に接続したプルアップ抵抗で構成されます。専用ラインドライバソリューションなど、もっと高度な構成のマスタもダラスセミコンダクタより入手可能です。この巧みな通信スキームを活用すると、いつでも簡単かつ効率的にメモリや認証機能、ミックスドシグナル機能などを追加することができます。

## 64ビットのシリアル番号

1-Wireシステムには、基礎的でとても重要な特長があります。スレーブデバイスは、それぞれ、固有で変えることができない(ROM)、64ビットのシリアル番号(ID)が工場出荷時に設定されています。この番号が他のデバイスと重複することはありません。64ビットのこのID値は、最終製品に一意の電子的IDを与えるとともに、1本のバスラインにつながれた複数のスレーブデバイスから目的のデバイスをマスタデバイスが選ぶ際にも利用されます。なお、64ビットIDの一部は、デバイスの種類とサポートされている機能を示す8ビットのファミリコードとなっています。

## データビットレベルの通信

1-Wireの通信は、すべて、バスマスタが開始し、制御します。**図2**に示すように、1-Wireの通信波形はパルス幅変調と似ています。これは、タイムスロットと呼ばれるデータビット時間の間、パルス幅をワイド(ロジック0)かナロー(ロジック1)とすることでデータが送られるからです。通信シーケンスは、バスマスタが一定の長さの「Reset」パルスを出し、バス全体の同期を取る形でスタートします。このResetパルスに対し、各スレーブは、ロジックローの「Presence」パルスで応答します。データを書きこむ場合、マスタは、まず、1-Wireラインをローにしてタイムスロットを開始した後、ラインをローのまま保持して(ワイドパルス)ロジック0を送信するか、ラインをリリースして(ショートパルス)バスをロジック1ステートに戻します。データを読む場合にも、まず、マスタがラインをナローローパルスで駆動してタイムスロットを開始します。スレーブは、オープンドレイン出力をオンにしてからラインをローにホールドしてパルスを引きのばし、ロジック

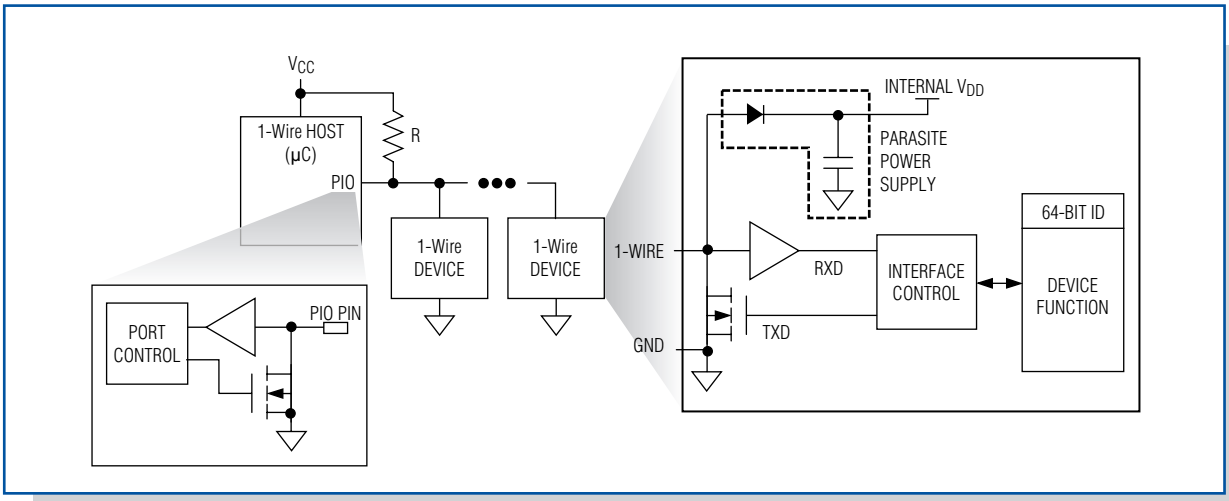



*図1. 1-Wireのマスタ/スレーブ構成では、すべてのデバイスが1本のデータラインを共有します。*

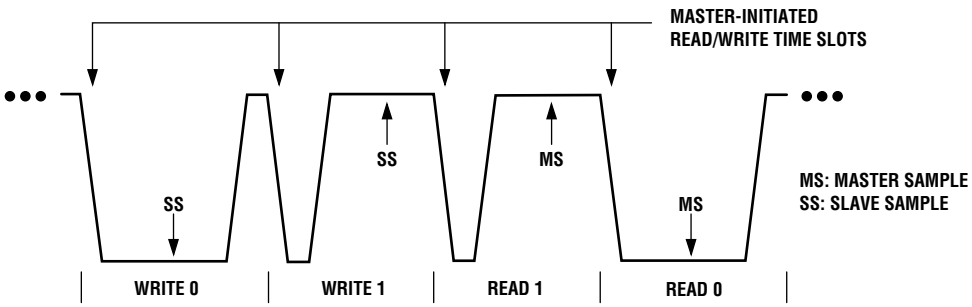



*図2. マスタが開始したデータビットの読み書きを示す波形です。スレーブとマスタのサンプリングポイントも表示されています。*

0を返すか、オープンドレイン出力をオフのままとしてラインを元に戻し、ロジック1を返します。なお、1-Wireデバイスのほとんどは、約15kbpsの標準速度と約111kbpsのオーバードライブ速度というふたつのデータレートをサポートしています。このプロトコルはセルフクロッキングであり、ビット間遅延が長くても問題が起きないため、割り込みが発生するソフトウェア環境でもスムースな運用が行うことができます。

## デバイスの選択

1-Wire通信で最初に行うことは、その後の通信相手となるスレーブデバイスを選択することです。スレーブデバイスがひとつだけの環境では、選択シーケンスは最小限ですみます。しかし、複数のスレーブデバイスがある環境では、すべてのスレーブを選択するか、64ビットIDで特定のスレーブを指定して選択するかになります。バイナリサーチのアルゴリズム(ROMレベルのコマンドとして1-Wireのデータシートに記載されています)はバスマスタが「学習」することを可能にし、ライン上にあるいずれのスレーブデバイスについても、それぞれ適切な64ビットIDを選ぶことができるようになります。いったん特定のスレーブが選択されると、マスタはそのデバイスだけに有効なコマンドを発行し、データを送るか、あるいは、そのスレーブからデータを読み出します。その間、他のスレーブデバイスは、Resetパルスが発行されるまで、通信を無視します。

## まとめ

1-Wireの基本構成に組み込まれるのは、各種のメモリ、ディジタル、アナログ、およびミックスドシグナル機能です。この多様性によって製品のラインナップは、単一接続の1-Wireインタフェースが配線の問題を解決し、ユニークな特長を持つ製品ラインに付加価値をつけることができるアプリケーションに最適となります。1-Wire製品は標準的なICパッケージングと堅牢なステンレスのiButtonパッケージがあります。製品、パッケージング、多彩なソフトウェアサポートについては、詳細をjapan.maxim-ic.com/1-Wireで紹介しています。