システムの信頼性を高めるウォッチドッグの正しい選び方

さまざまなマイクロプロセッサ(μP)が低コストで利用できるようになったこともあり、以前は専用ハードウェアによって実現されていた回路機能がソフトウェアによって構成されるようになりました。ソフトウェアは、最も低コストでフレキシブルな解決方法であることが多いのですが、同時に、システムの信頼性を確保するために、設計段階で十分な注意を払う必要のある方法でもあります。この世に間違いのないプログラムなどというものは存在せず、十分なテストをしてもコード1,000行あたり1つくらいの間違いは残るものです。つまり、10,000行程度の典型的な制御ソフトウェアには、少なくとも10箇所ほどのバグがあると考えるべきなのです。

システムをクラッシュさせるようなエラーをデスクトップアプリケーションが発生させても、あまり大きな問題にはなりません。ユーザがシステムを再起動できるし、データの損失も最小限に抑えられるからです。しかし、工業用制御ソフトウェアでは、人間が操作することなく、コードエラーからシステムが復帰できる必要があります。この機能が特に重視される2つの分野は、サーバや電話システム、製造ラインなどの常時稼動が必要とされるシステムと、自動車や医療機器、工業用制御、ロボット、自動ドアなどのクラッシュによって人的被害が発生する危険があり、高信頼性が必要とされるシステムです。これほど厳しい条件が不要な分野でも、リセットスイッチを押したり電源を入れ直したりという操作をユーザがすることなく、システムがクラッシュから復帰できるのは望ましいことです。デバイスがエラーから自動的に復帰できれば、デバイス内部で問題が発生したこと自体をユーザが知ることがないため、デバイスが高品質であるという印象を与えることができます。このようにシステムの信頼性を高める簡単で有効な方法は、ウォッチドッグを使用することです。

ウォッチドッグとは

ウォッチドッグとは、ウォッチドッグタイムアウト期間内にクリアする必要があるカウンタのことです。クリアされない場合、ウォッチドッグは、システムを再起動するリセット信号を送出するか、ノンマスカブル割込(NMI)を発行してエラー回復ルーチンを実行させます。ウォッチドッグは、ほとんどがエッジトリガ型です。つまり、ウォッチドッグ入力(WDI)に立ち上がりエッジか立ち下がりエッジが入力されると、カウンタがクリアされます。WDIピンは、ソフトウェアでトグルされるプロセッサのI/Oピンに接続します(図1)。ウォッチドッグカウンタをクリアするコマンドは、メインプログラムループに組み込んでおきます(図2)。ウォッチドッグがクリアされないとリセットが発生し、プログラムの実行がアドレス0000(プログラムの最初)に戻ります。なお、メインループの実行時間は、計算が難しいのが普通です。システムへの入力にもよりますが、さまざまなサブルーチンが呼ばれるかも知れないからです。そのため、ウォッチドッグタイムアウトを、実測ループ時間の最大値あるいは最長の計算値よりも長くとるという方法がよくとられます。図3は、正常動作時のウォッチドッグとリセット信号の関係です(タイムアウト期間内にウォッチドッグがクリアされます)。図4のようにウォッチドッグカウンタがタイムアウトに達するとリセットが発生します。業界標準のウォッチドッグ回路のタイムアウトは、100msから2sの範囲です。もちろん、もっと広範囲(30msから分単位まで)をカバーできる調整可能なウォッチドッグやカスタムウォッチドッグもあります。使用するウォッチドッグに対してメインループの実行時間が長すぎる場合は、メインループの複数箇所にウォッチドッグトグルコマンドを実装するか、タイムアウトの長いデバイスに交換することになります。

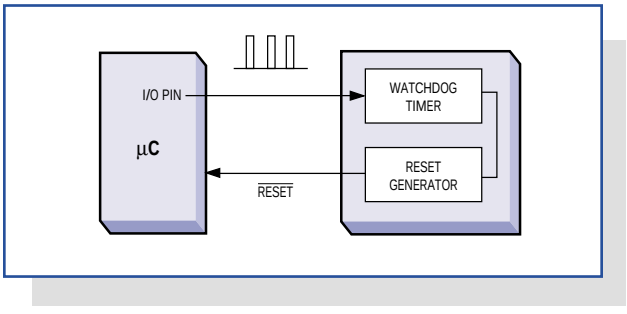

図1. リセットしない場合は、μPからWDIピンにパルスを送り、ウォッチドッグタイマをクリアします。

システムが無限ループに陥らないようにする方法として、メインループの最初で当該I/Oピンをハイにセットし、メインループ内の他のセクションでローにセットするという方法があります。こうすれば、メインループの初期に無限ループに入ってしまっても、WDIがハイ状態のままなのでウォッチドッグのタイムアウトが発生し、システムがリセットされます(図5)。図2のようにロー・ハイ・ローのパルスを使用しても、ウォッチドッグのクリアはできますが、システムがハングアップから抜け出せなくなります。モニタリングが必要な複数のタスクを処理するプログラムでは、もっと高度なスキームが必要になります。それぞれのタスクでフラグをセットし、全フラグがセットされていればウォッチドッグのトグル

を行うようにするのです。この場合、ウォッチドッグタイムアウト期間内に全タスクの処理が終わらなければなりません。図2も図5も、実際のプログラムと比較してあまりに簡単だと感じられるかもしれませんが、コンセプトはお分かりいただけるはずです。複雑なシステムでは、メモリリークやスタックオーバフローなどの問題もモニタリングする必要があります。今回はここまで踏み込んだ解説をしませんが、このような処理は、通常、適切な設計手順に従い、注意深くコードの検証を行い、特殊なソフトウェアツールを使えば行うことができます。

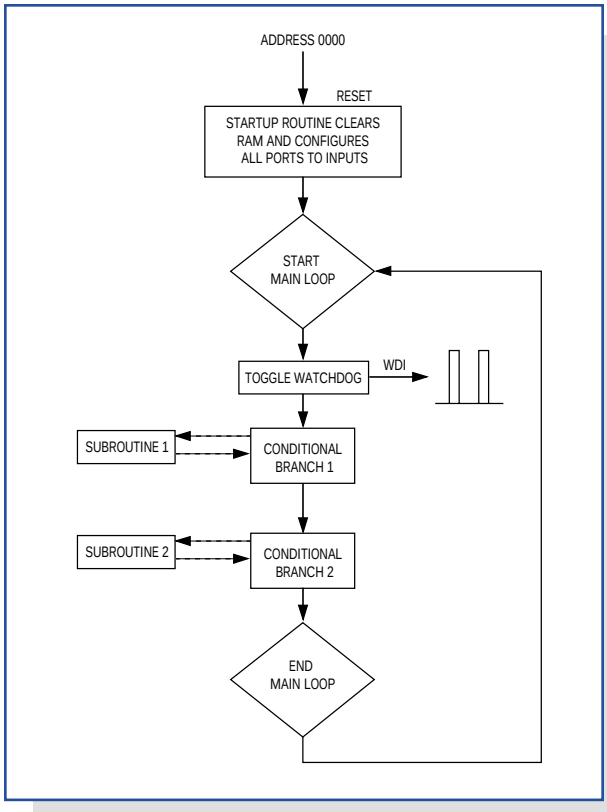

図2. メインループでWDI信号を生成する典型的なプログラムフロー例です。

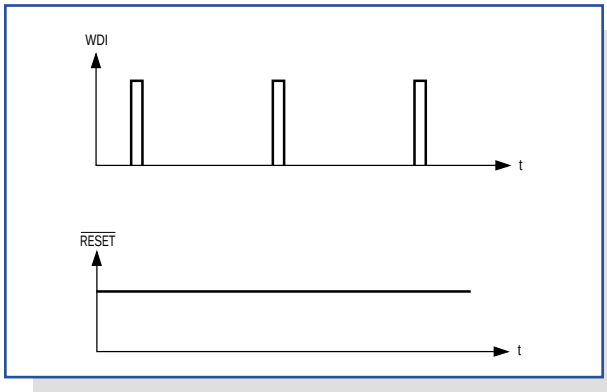

図3. ウォッチドッグタイムアウト期間中にWDIピンがトグルされればリセットは発生しません。

内蔵ウォッチドッグと外部ウォッチドッグ

多くのμPは、ソフトウェアによってディセーブルできるプログラマブルウォッチドッグを内蔵しています。このような内蔵ウォッチドッグはコードエラーの影響を受けるため、独立した外部ウォッチドッグほどの保護機能が得られません。安全性が重視されるアプリケーション

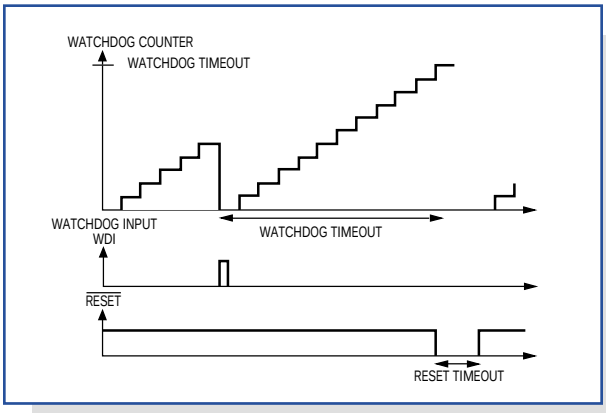

図4. ウォッチドッグカウンタがタイムアウト値に達するとリセットが発生します。

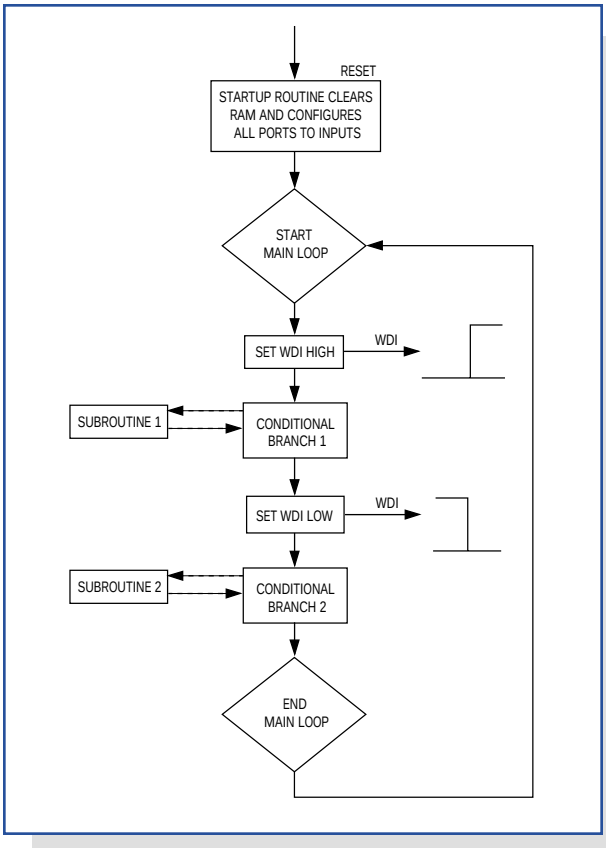

図5. ウォッチドッグトグルコマンドを2つに分けるという改良を施したプログラムフロー例です。それぞれのトグルコマンドは、WDIピンに立ち上がりエッジあるいは立ち下がりエッジを出力します。このようにすれば、無限ループに陥ることを防止できます。

(自動ドアや医療機器、ロボットなど)では、内蔵ウォッチドッグは使えません。規制当局により、独立した外部ウォッチドッグの採用が義務づけられているのです。つまり、重大なシステム障害のリスクを低減するためには、外部ウォッチドッグを使った方がいいのです。

ウォッチドッグとリセットを組み合わせたシンプルな製品

ウォッチドッグタイムアウトが発生すると普通はシステムがリセットされるため、ウォッチドッグは、プロセッサへの電源電圧の監視も行うμPのリセットと統合されるのが普通です。このとき、μPのリセットは、ウォッチドッグあるいは電圧低下により行われます。図6に示すMAX823～MAX825ファミリは、これら2つの機能を組み合わせた製品で、標準リセット電圧に加えて、公称ウォッチドッグタイムアウト1つとリセットタイムアウト1つを持ち、消費電流は6μAと低く抑えられています。パッケージは超小型のSC70です。

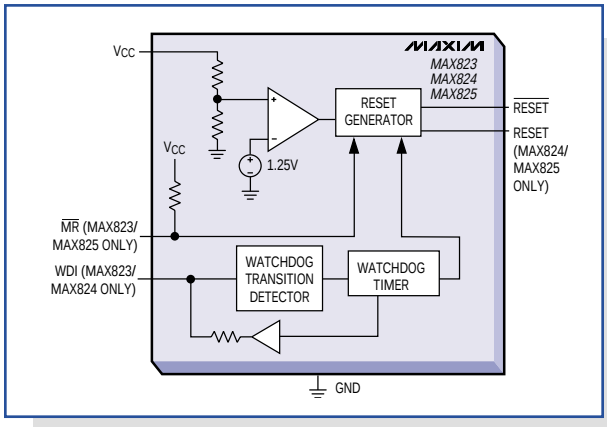

図6. MAX823～MAX825ファミリでは、ウォッチドッグとリセットというよく使われる機能が統合されています。

出荷時プリセット型ウォッチドッグファミリ

MAX6316～MAX6322ファミリは、26種類のリセット電圧、4つの公称ウォッチドッグタイムアウト期間、4つの公称リセットタイムアウト期間、4種類の出力形式の組み合わせが自由に選べる出荷時プリセット型の製品です(表1参照)。

容量可変ウォッチドッグ

ウォッチドッグタイムアウトをフレキシブルに調整したい場合は、調整が可能な回路を使用します。MAX6746～MAX6753ファミリでは、リセット電圧は出荷時プリセットあるいは抵抗分割でプログラマブルとなり、ウォッチドッグタイムアウト期間とリセットタイムアウト期間は外付けコンデンサによる設定が行えます。図7は回路例です。

- リセット電圧は、分圧抵抗R1/R2によって決まります。
- リセットタイムアウト期間は、リセットタイムアウト設定用コンデンサ(C_{SRT})によって決まります。
- ウォッチドッグタイムアウト期間は、ウォッチドッグタイムアウト設定用コンデンサ(C_{SWT})によって決まります。

図8は、ウォッチドッグタイムアウト期間とC_{SWT}(100pF～100nF)の関係を示すグラフです。このようにウォッチドッグタイムアウトを広い範囲で自由に設定できるため、アプリケーションに適したソリューションの構築が可能になります。MAX6301～MAX6304ファミリは、機能的にはMAX6746～MAX6753ファミリと同じですが、パッケージがSOPとDIPになります。

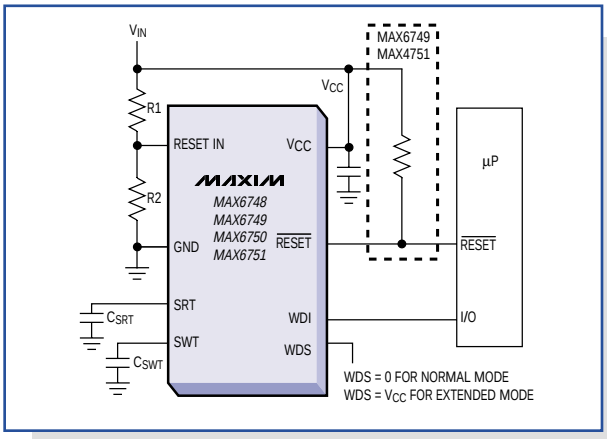

図7. MAX6346～MAX6353容量可変ウォッチドッグファミリの回路例です。

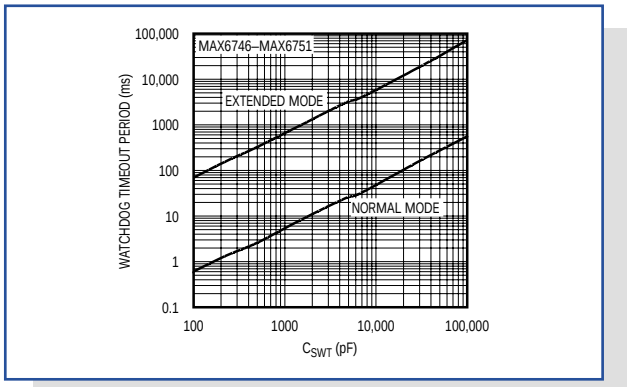

図8. ウォッチドッグタイムアウト期間を広い範囲で調節可能です。

長いスタートアップ/タイムアウトに対応できるピン選択式ウォッチドッグ

スタートアップルーチンに時間がかかる場合は(図2参照)、スタートアップルーチン用の長いタイムアウト期間と通常動作用の短いタイムアウト期間を持つウォッチドッグを採用すべきです。MAX6369～MAX6374ファ

ミリは、ピン選択により、スタートアップ遅延は200ms～60sの範囲で、ウォッチドッグタイムアウト期間は30ms～60sの範囲で設定することができます。スタートアップルーチンが特に長い場合にも対応できるように、第1エッジによるウォッチドッグ起動機能を持ったデバイスもあります。このようなデバイスでは、スタートアップにはウォッチドッグがディセーブルされており、µPの当該I/Oピンからの第1エッジを受け取るとウォッチドッグを起動します。

複数電圧に対応したウォッチドッグ

デュアル電源を使うシステムでは、MAX6358～MAX6360ファミリを使えば、2種類の標準電圧の監視が可能です。この製品には、通常のタイムアウトだけでなく、長時間のスタートアップにも対応したウォッチドッグが搭載されています。3種類の電圧が混在する場合や、アクティブハイやアクティブローによるリセット機能が必要な場合には、MAX6721～MAX6729ファミリが最適です。この製品には、通常のタイムアウトと長時間のスタートアップに対応したデュアルモードウォッチドッグが搭載されています。2種類の標準電圧の監視(MAX6721/MAX6722)、あるいは2種類の標準電圧に加えてもう1つの電源電圧(監視電圧は可変)の監視(MAX6723/MAX6724)が行えます。また、マニュアルリセット入力、パワーフェイルコンパレータ、デュアルリセット出力、RESET出力と$\overline{\text{RESET}}$出力も備えています。

超高信頼性のウィンドウ型ウォッチドッグ

超高信頼性が必要な場合には、MAX6323/MAX6324ウィンドウ型ウォッチドッグが最適です。これは、ウォッチドッグをクリアするためには設定されたウィンドウ時間内でパルスが発生しなければならないデバイスです。有効パルスが発生する期間は、例えば、最終パルスからわずか1.5ms後、あるいは最終パルスから10ms後までがあり得ます(レンジについては表1を参照のこと)。MAX6323/MAX6324なら、ループ内にウォッチドッグクリアコマンドを持たせれば、高速パルストレインが発生して、その無限ループからシステムを回復させることが可能です。通常のウォッチドッグでは、このようなパルスが発生するとクリアされ、リセットが発生することはありません。しかし、ウィンドウ型ウォッチドッグでは、ウォッチドッグパルス間に一定以上の遅延時間がなければならないので、このような事態を避けることができます。ウィンドウ型ウォッチドッグデバイスが適しているアプリケーションとしては、アンチロックブレーキシステムなどの自動車用回路や、高い安全性が求められる工業用アプリケーションや医療用アプリケーション、常時駆動が非常に重要なアプリケーションなどが考えられます。

結論

ソフトウェアプログラムには必ずコードエラーが存在するため、システムのロックアップを避ける工夫が必要です。データがノイズやEMIの影響を受け、システムの動作がおかしくなることもあります。このようなシステムの信頼性を高めるシンプルで安価な方法が、ウォッチドッグです。外部ウォッチドッグを使えば、ウォッチドッグタイムアウト期間内にWDIがトグルされなければµPをリセットするため、システムのハングアップを防止することができます。さまざまな種類のウォッチドッグが提供されているので、使用目的に合ったデバイスが必ず見つかるはずです。

表1. アプリケーション別ウォッチドッグ機能分類

アプリケーション	ファミリ	電圧監視	ウォッチドッグタイムアウト(min)	リセットタイムアウト(min)	特記事項
Simple plus reset	MAX823/ MAX824	Factory-preset 2.5V, 3.0V, 3.3V, or 5V	1.12s	140ms	SOT23 or SC70 packages
Customized	MAX6316–MAX6322	Factory-preset in 100mV steps 2.5V to 5V	4.3ms, 71ms, 1.12s, 17.9s	1ms, 20ms, 140ms, 1.12s	Push-pull, open-drain, or bidirectional output
Capacitor-adjustable	MAX6746–MAX6753	Factory-preset, or adjustable by voltage divider 1.575V to 5V	700ms to 70s in two ranges by 100pF to 100nF capacitor	Preset, or 0.5ms to 5s by capacitor	SOT23-8, min/max windowed option
	MAX6301–MAX6304				SO or DIP packages
Long startup, pin-selectable	MAX6369–MAX6374	Dual factory-preset 1.8V, 2.5V, 3.0V, 3.3V, or 5.0V	30ms to 60s; 200ms to 60s first-edge activation	Watchdog only	Dual mode, pin-programmable startup delay
Multisupply	MAX6369–MAX6360	Dual fixed 1.8V, 2.5V, 3.0V, 3.3V, 5V; or dual fixed plus one adjustable	1.6s normal	100ms	Manual reset, power-fail comparator, dual reset, RESET plus $\overline{\text{RESET}}$ outputs
	MAX6721–MAX6767		25.6s startup		
Windowed	MAX6323/ MAX6324 Dual Mode	Factory-preset 2.5V, 3V, 3.3V, or 5V	1.5ms to 719ms (min); 10ms to 1.3s (max) window	100ms	Eight factory-trimmed options; timeout reset pulses accepted only within the defined window