

キーワード: 高電圧ウォッチドッグ, リンプホーム, リンプホームモード, フォルト耐性ウォッチドッグ, 障害耐性ウォッチドッグ, 故障耐性ウォッチドッグ, 高電圧ウォッチドッグタイマ, ウォッチドッグタイマ, 車載用ウォッチドッグタイマ, 車載用ウォッチドッグ, 自動車用ウォッチドッグ

Nov 08, 2010

アプリケーションノート 4270

高電圧ウォッチドッグタイマによる車載システムの安全性の向上

筆者: Robert Regensburger, Automotive Specialist, Automotive Product Definitions, Maxim Integrated Products, Germany

要約: 車載電子システムのほとんどには、必要なレベルの故障耐性と安全性を実現するための監視回路が必要です。ウォッチドッグタイマのMAX16997/MAX16998は、このような回路で監視デバイスとして使用するのに最適です。このタイマーはマイクロコントローラ(μC)の通常動作の間に作られるプログラム生成パルスを監視し、電気的な障害や μC の障害が発生した場合にバックアップ/冗長回路に切り替えます。これによってリンプホーム(よたよたしつつも家にたどりつく)機能が実現され、自動車はフェイルセーフ状態になって、困難な停止をすることなく走行することが可能です。

電子システムは、ますます多くの自動車の機械的な機能(エンジンのタイミングからブレーキやステアリングに至るまでのすべて)を引き継ぐようになりましたが、電子機器は故障する可能性があるため、システムの故障耐性を確保することに関心が高まりつつあります。(運転手や同乗者にとって)危険な状況を引き起こすおそれのある障害は1つでもあってはなりません。少なくとも、車が道路脇を「のろのろと進み」、最寄りのガソリンスタンドにたどり着けるようにしなければなりません。電気的な障害が発生しても車が確実に安全に走行を続けられるようにするため、監視回路を使用して、障害の間に動作を引き継ぐことのできるバックアップ回路に信号を転送します。

車両に純然たる機械式システムが搭載されていた日々を振り返ってみましょう。たとえば、初期のエンジンは、機械的に作られる信号に依存して燃料/空気の混合気体に着火していました。機械式の配給器は、適切なスパークプラグを選択し、ワイヤに沿って信号を送出していました。ブレーキシステムは、ペダルに加えられた力を、ブレーキシャフト、マスターブレーキシリンダ、および油圧パイプを通してブレーキキャリパに直接伝達していました。クラッチおよびスロットルのどちらのシステムも、単にペダルから接続された鋼線によって制御されていました。ステアリングは、金属のステアリングホイール、ステアリングシャフトとそのマウント、ステアリングギアボックス、およびステアリングロッドを通じて行われ、これによって必要なステアリング角がホイールに伝わる仕組みでした。エンジンの制御は、今日使用されている最新のデジタル電子制御ユニット(ECU)とは、まったく異なっていました。コンピュータ支援による、ブレーキ制御、クラッチ制御、スロットル制御、ステアリング制御などの機能はありませんでした。当然ですが、 μC のクラッシュや制御ユニットでの短絡などの不具合はなく、故障するおそれのあるのは、99の機械部品のみでした。ただし、社会が機械式システムに高い信頼を置いていたため、バックアップシステムや故障耐性に対する関心は低いものでした。何かが故障すると、危険な状態に陥る可能性があり、あるいは最良の場合でも運転手は故障現場で立ち往生し、レッカー車を手配して故障車両を最寄りのガソリンスタンドまで牽引しなければならませんでした。

より優れた快適性と利便性、効率性と環境浄化、性能の向上、および車両の安全性の向上を求める要求が高まることによって、自動車メーカーは、車両に電子機器を採用することになりました。ただし、初期のECUの多くは、システムに障害が発生した場合に単に動作を停止するだけでした。特に、ECUにおける電子動作は μC に依存するものでした。 μC はクラッシュすることがある上に、故障発生時に命にかかわる状況が生じるのを未然に防ぐ対策や、少なくとも修理場所まで到達可能な短距離の移動手段が用意されていなかったため、故障耐性に対する関心が急速に高まりました。このため、現在のECUの多くは「リンプホーム」モードを装備しています。

リンプホームモード

リンプホームモードはECU内の冗長機能であり、物理的に分離された、主としてアナログのスタンバイ回路によってフェイルセーフモードに移行することができるようにするものです。このモードは、自動車の電子システムに障害が発生した場合に、自動車の性能を抑えて安全に道路脇を走行することができるようにします。

現代のエンジンのECUの多くは、ウォッチドッグタイマなどの監視デバイスを装備しており、ECUが正常に動作しているかどうかを定期的に確認します。電気的な障害や μC (ソフトウェアのクラッシュ)の障害などの異常が検出された場合、監視デバイスがリンプホーム回路を有効にします。たとえば、エンジンチェックランプが点灯し、ファンが直ちに作動して、シリンダの半数のみに燃料が供給されず、シリンダの半数のみを燃焼させることによって、エンジンが生成する熱ははるかに少なくなります。車両は控えめの速度で走行可能です。また、自宅あるいは最寄りのガソリンスタンドに到達するだけのパワーが得られることになります。

他の良い例として、現代の車両の「車体制御コンピュータ」が挙げられます。この機能は、車両に搭載されているウィンドウリフト、ヘッドライト/テールライト、方向指示器、およびフロントガラスのウォッシュ/ワイパ、およびコンピュータシフトのトランスミッションを備えた車内のシフト制御コンピュータなどの機能を制御します。監視回路は、このようなECUが正常に動作しているかどうかを監視し、電気的な障害や μC の障害が発生した場合には、スタンバイ回路を起動し、運転性能を抑えます(ロービーム、テール/ブレーキライト、またはバックとセカンドギアのみなど)。この機能によって、当然、最高速度は制限されますが、自動車は最低限の機能を維持し、安全に「リンプホーム」を実行して、修理工場まで走行することができるようになります。

これは良くないことでしょうか。いいえ、そうではありません。これに代わる方法といえば、最終的に車が破壊する危険を抱えたまま通常速度で走行するか、あるいは安全を得られないまま何もできずに停止することです。

冗長性

コンピュータ制御によるアプリケーションの将来は、いわゆる「バイワイヤ(電気信号で制御)」であり、パワートレインの内外にある機械制御システムのほとんどが電気機械システムに置き換えられることとなります。たとえば、ステアバイワイヤシステムでは、ステアリングホイールと車輪間のすべての機構が電気的接続(ワイヤ)でリンクされたECUに置き換えられます。運転手によるステアリングホイールの物理的な動きが検知されてデジタル電気信号に変換され、この信号が車輪を制御する高性能電気機械作動ユニットに送信されます。

ブレーキバイワイヤシステムは、ブレーキシャフト、マスターブレーキシリンダ、および2つのコンピュータを装備したブレーキブースタ、サーボモータまたは電気機械キャリパ、およびいくつかのワイヤなどの部品が置き換えられます。

これらのシステムは本来、前述のシステムに比べてより安全性が重要視されています。ブレーキングやステアリングのロスが、命を脅かす状況を直ちに招く可能性があるからです。したがって、安全性および故障耐性に求められるレベルがはるかに高くなります。

これらの新しいアプリケーションのためのバックアップ回路を設計するエンジニアは、完全な冗長電子制御と監視のユニットを構築し、これをメイン制御ユニットから物理的に十分に離して、電子システムを常に安全に利用することができるようにしています。監視ECUは、1次システムを常に監視し、障害が発生した場合には、2次の冗長システムに切り替えます。冗長システムの背景にある理論は、複数の制御ユニットが同時に故障する確率は、単一のECUで単一の不良が発生する確率に比べて極めて小さいということです。このようにして、冗長制御ユニットによって、安全性が重要視される車載アプリケーションに安全性とセキュリティが追加されます。

高電圧ウォッチドッグの進歩

潜在的な安全性の問題を考えると、車載電子システムのほとんどは、必要なレベルの故障耐性と安全性を実現するための監視回路が必要です。ウォッチドッグタイマのMAX16997/MAX16998は、このような回路で監視デバイスとして使用するのに最適です。このタイマは、 μC の通常動作の間に生み出されるプログラム生成パルスを監視し、電気的な障害や μC の障害が発生した場合にバックアップ/冗長回路に切り替えるからです。

MAX16997/MAX16998は、タイムアウト機能とウィンドウ型ウォッチドッグ機能、オープンドレインの μC リセット出力(RESET)、ウォッチドッグのトリガ入力(WDI)、およびオープンドレインの冗長システムイネーブル出力(ENABLE)を装備しています。

MAX16998の場合、低電圧電源(μC 電源)、外部電圧監視入力(RESETIN)、およびGNDの間の外付け抵抗分圧器を使用することによってリセットスレッショルド電圧を設定することができます(図1に表示)。MAX16997は、イネーブル入力(EN)端でKL15(イグニッションスイッチ)のステータスを読み取ることが可能で、イグニッションがオンの場合、内蔵の監視タイマーを起動します(図2)。ここで、初回のウォッチドッグタイムアウト期間は8倍に延長され、 μC に十分な起動時間を与えます。

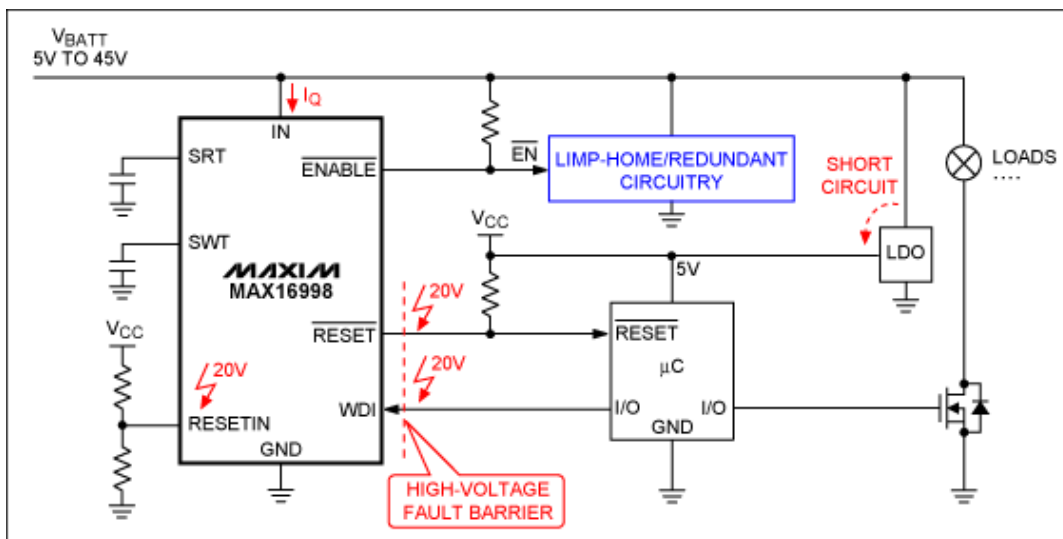


図1. 高電圧ウォッチドッグタイマのMAX16998は、ダウストリームの低電圧電源(LDO)とは独立して動作し、バッテリー電圧への短絡に対して堅牢なバリアを設け、故障状態時にデバイスが安全に冗長回路に切り替わるようにします。

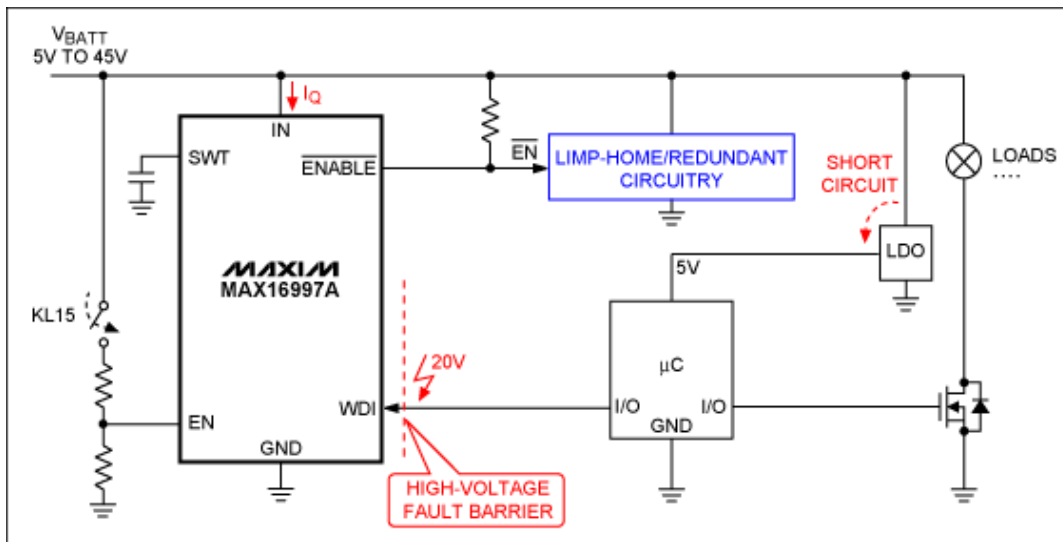


図2. MAX16998と同様、MAX16997は、故障状態時に安全に冗長回路に切り替わるようにします。MAX16997は、ウォッチドッグタイマのオン/オフを切り替えるアクティブハイネーブル入力(EN)も装備しています。

リセットの遅延(MAX16998のみ)とウォッチドッグのタイムアウトは、機能ごとに(SRTとSWT入力に対してそれぞれ)1つの外付けコンデンサを使用することによって、独立して設定可能です。オープンウォッチドッグウィンドウの割合は、工場出荷時に、調整済みウォッチドッグ時間の50%または75%に設定されています。

MAX16997/MAX16998は、18 μ A (typ)という超低動作電流であるため、常にオン状態の車載ECUにとって非常に価値のあるものとなります。さらにこれらのデバイスは、3mm x 3mmの8ピン μ MAX $\text{\textcircled{R}}$ パッケージで提供され、-40 $^{\circ}$ C~+125 $^{\circ}$ Cの自動車用温度範囲での動作が保証されています。

これらのICは、標準のウォッチドッグタイマデバイスとは異なり、12Vの自動車バッテリーのレールから直接電力を得ることが可能で、最大45Vの過渡電圧耐性を備えているため(INとENABLEピン上)、ダウストリーム低電圧電源(たとえば、5V)とは独立して動作します。したがって、ダウストリーム回路に電力が供給されない、またはGNDに短絡した場合でも、MAX16997/MAX16998は動作を続け、ENABLEピンをアサートすることによって冗長回路への切り替えが可能です。これらのウォッチドッグタイマの故障耐性をさらに高めることによって、RESET、WDI、EN、およびRESETINピンは、車のバッテリー電圧への短絡にも耐えられるよう、20Vの耐性を備えています(図1と2)。したがって、これらは、ダウストリームの高電圧の電氣的障害に対して堅牢なバリアを設け、バックアップ回路を「通常」の制御回路から物理的に分離し、このような故障が発生したときに安全にバックアップモードに切り替わるようにしています。

MAX16997/MAX16998のタイミング

起動時、RESETINピンの電圧(V_{RESETIN})が、パワーオンリセットのスレッシュホールド(V_{PON})を超えた後、RESETは、パワーオンリセット時間(t_{RESET})の間、ローのまま、その後ハイになります。これと同時に、ウォッチドッグタイマは、カウント(t_{WP})を開始します。ウォッチドッグのオープンウィンドウの期間(t_{OW})内にWDIピン上にトリガ信号がない場合、RESETは再びローにアサートされて μ Cがリセットされます。不良の3つのウォッチドッグトリガが連続すると、クローズウィンドウ段階(t_{CW})において、またはウォッチドッグ期間(t_{WP})が経過した後に信号がトリガされた場合、ENABLEはローにアサートされ、これによってシステムは冗長回路に切り替わります。良好な3つのウォッチドッグトリガが連続すると、WDIトリガ信号は、再び、オープンウォッチドッグのウィンドウ段階(t_{WDI})の範囲となり、ENABLEがデアサートされてシステムは元の通常回路に切り替わります(図3)。

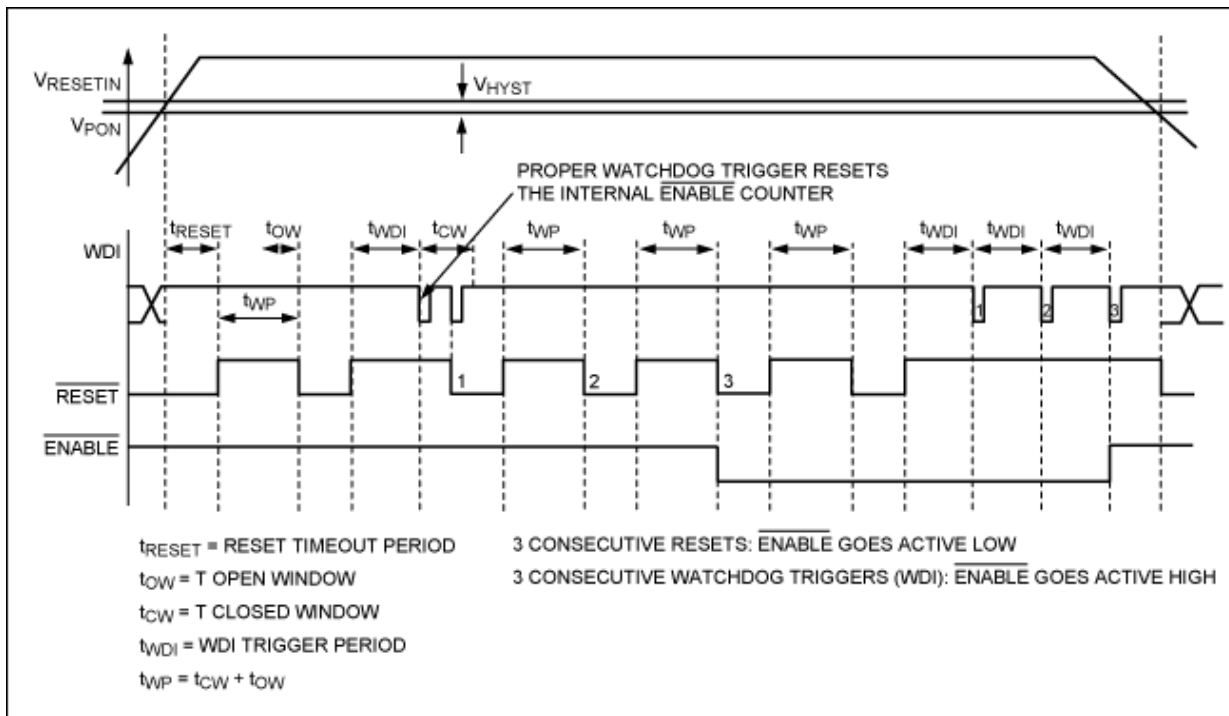


図3. MAX16998のタイミング図(ウィンドウ型ウォッチドッグを備えたバージョン)

タイムアウトウォッチドッグ対ウィンドウ型ウォッチドッグ

MAX16997/MAX16998Aは、標準的なタイムアウトウォッチドッグの機能を装備していますが、MAX16998B/Dは、時間-ウィンドウ型のウォッチドッグ機能を備えています(図4)。必要なセキュリティレベルに応じて、いずれかのタイプのデバイスを選択することができます。タイムアウトウォッチドッグの改良版では、ウォッチドッグの期間内にタイマーのクリア信号が生成されるようにし、生成されない場合は、システムがリセットされます。したがって、これらのウォッチドッグは、遅すぎるコード実行や低速のデジタルクロック(たとえば水晶発振器によって生成されたクロック)などのソフトウェア障害を検知することができます。一方、時間-ウィンドウ型のウォッチドッグ機能は、正しいタイムウィンドウ内でタイマーのクリア信号が生成されるようにします。したがって、このウォッチドッグは、遅すぎるコード実行や高速動作の発振器などのその他のエラーを検知し、より高度なセキュリティを実現します。

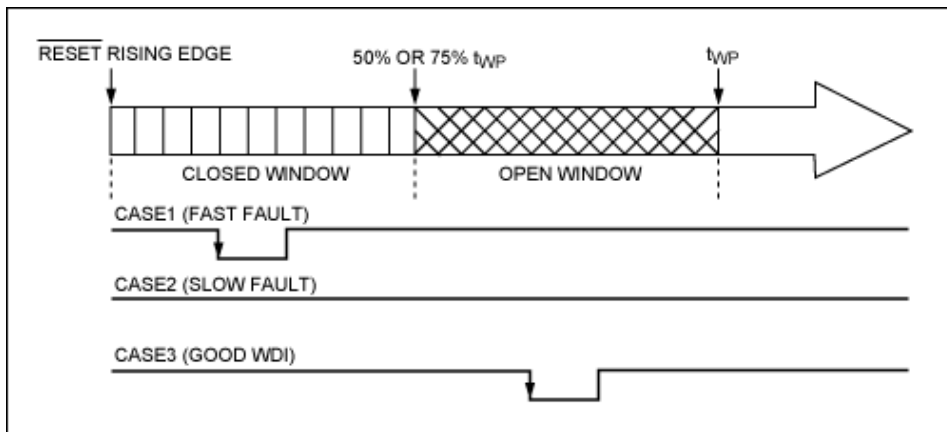


図4. MAX16998ウォッチドッグ期間のタイミング(ウィンドウ型ウォッチドッグを備えたバージョン)

図4のケース3は、正しいタイムウィンドウ内に生成される良好なWDIトリガを示しています。ケース1は、ウォッチドッグによる信号のトリガが早すぎる不良WDIトリガを示しています。これによって、遅すぎるコード実行や高速動作の発振器などのエラーを示しています。ケース2もウォッチドッグが信号をトリガするのが遅すぎる、コード実行が遅すぎる、または発振器の動作が遅い、などの不良WDIトリガを示しています。

結論

故障耐性と安全性は、車載エレクトロニクスにおいてますます重要な課題になりつつあります。効率と快適性を向上すると同時にリスクを低減するには、ハードウェア、ソフトウェア、センサー、エフェクタ、およびオペレータのすべてのシステム部品を効果的に管理することが必要となります。MAX16997/MAX16998などのウォッチドッグタイマは、この目標の達成における明らかなマイルストーンになります。

μMAXはMaxim Integrated Products, Inc.の登録商標です。

関連製品

MAX16997	可変タイムアウト遅延付き、高電圧ウォッチドッグタイマ	-- 無料 サンプル
MAX16998	可変タイムアウト遅延付き、高電圧ウォッチドッグタイマ	-- 無料 サンプル

自動アップデート

お客様が関心のある分野でアプリケーションノートが新規に掲載された際に自動通知Eメールの受信を希望する場合は、[EE-Mail™](#)にご登録ください。

アプリケーションノート4270: <http://japan.maxim-ic.com/an4270>

その他の情報

テクニカルサポート: <http://japan.maxim-ic.com/support>

サンプル請求: <http://japan.maxim-ic.com/samples>

その他の質問およびコメント: <http://japan.maxim-ic.com/contact>

AN4270, AN 4270, APP4270, Appnote4270, Appnote 4270

Copyright © by Maxim Integrated Products

法的小知らせ: <http://japan.maxim-ic.com/legal>