Keywords: limp home, fault tolerance, high voltage, watchdog timer, ECU, automotive safety, redundant system

APPLICATION NOTE 4210

High-Voltage Watchdog Timers Enhance Automotive System Safety

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

Jan 05, 2012

Abstract: As electronic systems take over many of the mechanical functions in a car—ranging from engine timing to steering and braking—there is a growing concern about fault tolerance. There should not be a single point of failure that would prevent a car from at least "limping" off the road or making it to the nearest service station. Redundant systems, watchdog timers, and other control circuits are used to reroute signals and perform other functions that ensure that a vehicle can safely make it off the road when a failure occurs.

Introduction

Modern high-end cars can have up to 80 electronic control units (ECUs). These vary from the most sophisticated circuits that control the engine, braking, and airbag deployment, to simpler ones that control the seat and side-mirror adjustments. But as with all electronics, things sometimes go wrong. All computers can crash. All software can have bugs. This is where a "limp-home mode" comes into play.

Limp-Home Mode

"Limp home" is a vehicle-operating mode that allows a fail-safe mode to be entered and permits the vehicle to be driven home slowly. Limp-home mode is implemented so that a faulty car can get its passengers home safely, while limiting damage to the car's engine and other components. Limp home encompasses both the engine-management system and the ancillary safety equipment, such as lights and windshield wipers, which are usually controlled by the body control unit (BCU).

A modern engine-management system has a self-test capability that periodically examines the signals from the engine sensors. For example, if the coolant level sensor reads below a critical level, the engine control module switches the engine to emergency mode. The fan is turned on immediately and only half of the cylinders get fuel. With only 50% of the cylinders firing, the engine generates much less heat because it operates at low power. The engine can move the vehicle at moderate speeds of up to about 50mph (approximately 80kph) and has just enough power to get the car home or to the nearest garage. While the engine-management system must ensure that the engine can run in a reduced mode, the BCU must ensure that other basic vehicle functions are maintained.

As the number of electronics in a car increases and systems become increasingly complex, it gets harder and harder to make a car fail-safe. The usual aim is to ensure that there can be no single point of failure that renders the vehicle immobile. The problem is exacerbated by the use of highly complex software, which is very difficult to test exhaustively.

Redundancy

Limp home is an alternative to the introduction of redundancy into a system. In a redundant system if the primary control system fails, there is another to take its place. Alternatively, a polling technique is used where more than two processors or logic circuits are polled and the majority decision determines whether or not an action is taken. The rationale is that the probability of two or more systems failing simultaneously is far less than the probability of a single system failing. The disadvantage of a true redundant system is its higher cost and complexity. In certain "by-wire" applications, redundancy is essential. However, in some systems it is sufficient if limited functionality can be maintained, even in the case of a processor failure.

One way to implement a fail-safe system is to use a hardware watchdog circuit that must be "serviced" periodically by the microcontroller to avoid a system reset. The use of a watchdog is a simple and low-cost technique that ensures the required limited functionality in the case of a fault and is not dependent on software.

Watchdog Advances

Given the aforementioned considerations, the MAX16997/MAX16998 are ideal to enhance system safety in automotive applications. These high-voltage watchdog timers are designed to provide extreme reliability and security in safety-critical microprocessor-controlled applications. In the event of a µC failure, the watchdog is activated and the device can safely switch to redundant circuitry (**Figures 1** and **2**).

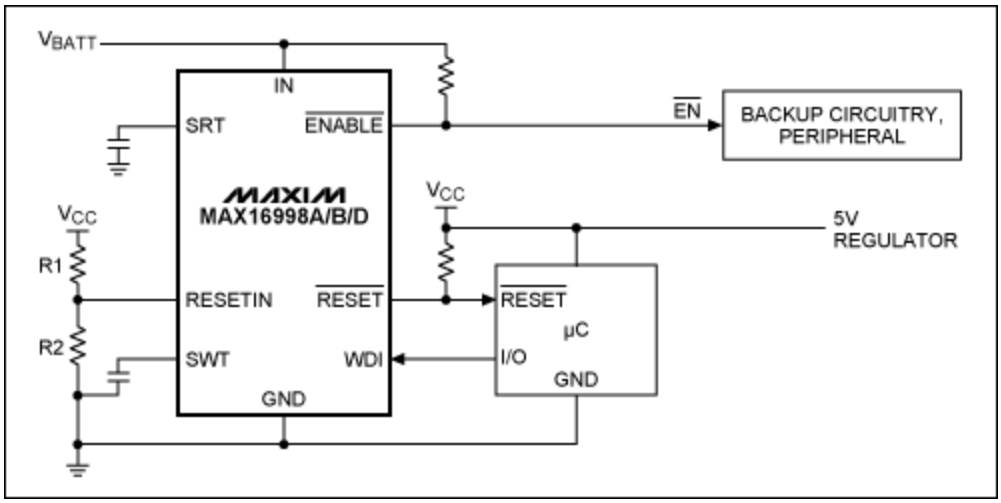

Figure 1. The MAX16998 switch over to backup circuitry.

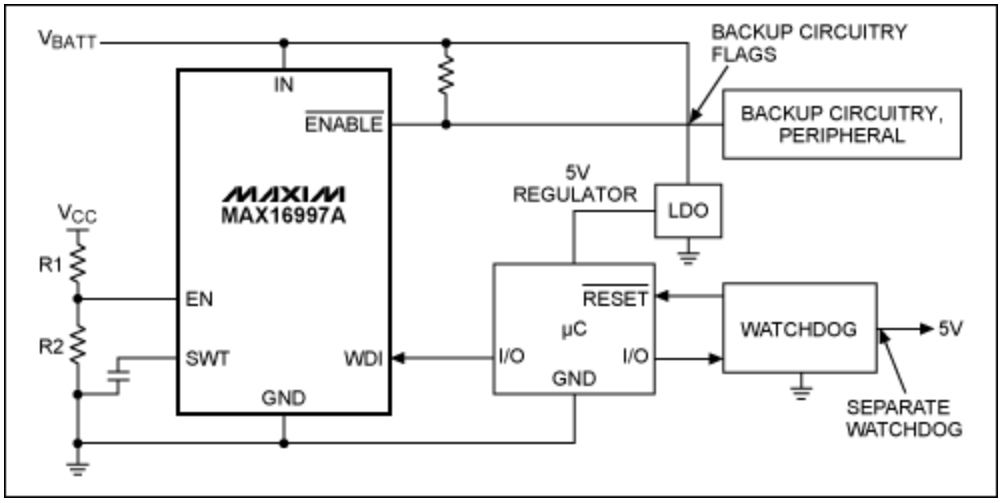

Figure 2. The MAX16997A typical application diagram.

The MAX16997/MAX16998 feature timeout or windowed watchdog functions, external voltage monitoring for power up/down reset, µC reset function, enable inputs and a high-voltage-tolerant system enable output. As these ICs can be directly powered from the 12V car battery and are transient voltage tolerant up to 45V, they operate independently of a low-voltage supply, unlike standard low-voltage watchdog timer devices. Thus, if the downstream circuitry fails due to a hardware (HW) or software failure, these supervisory circuits continue to operate independently.

Making the IC even more immune to HW failures, the active-low reset output (active-low RESET), watchdog trigger input (WDI), enable input (EN) and the external voltage monitoring input (RESET IN) are 20V rated, to withstand a short-circuit to a car battery voltage. This feature provides a robust barrier against downstream high voltage electrical failures and guarantees the switch-over to redundant circuitry securely in this condition.

Depending on the security level needed, the MAX16997/MAX16998 can provide either standard timeout watchdog capabilities or a time-windowed watchdog function. Timeout watchdog variants ensure that the timer's clear signal occurs within the watchdog time; otherwise, they will activate the system reset. Thus, they will detect a software failure, such as code executing too slowly or a slow-running crystal oscillator. The time-windowed watchdog can recognize more faults. It ensures that the timer's clear signal occurs within the correct time window. Therefore, it can additionally detect errors, such as code executing too quickly or a fast-running oscillator.

The timing for reset delay and watchdog time can be programmed independently using one external capacitor for each function. The ratio for the open watchdog window is factory set to 50% or 75% of the watchdog time. In addition, the reset threshold voltage is programmable using an external resistor voltage divider.

The MAX16997 can read the KL15 status (EN), and activates the internal supervisor timer only if ignition is on. Here the initial watchdog time out period is prolonged by a factor of eight to give a microcontroller sufficient time to start up.

Active-low RESET is asserted low whenever the active-low RESETIN voltage falls below its reset threshold or the watchdog trigger input (WDI) reads a bad trigger. Active-low ENABLE is pulling low if the WDI input reads a bad trigger signal three consecutive times. After the µC has cleared the watchdog

(WDI pin) three consecutive periods successfully active-low ENABLE will get high again.

The MAX16997/MAX16998 come in an 8-pin µMAX® package and are fully specified over the automotive temperature range (-40°C to +125°C).

Conclusion

To ensure that automotive systems fail safely and can continue to operate in reduced functionality mode, redundancy and/or limp-home modes are needed. Products such as the MAX16997/MAX16998 will clearly provide a simple means to implement limp-home functionality in automotive systems.

µMAX is a registered trademark of Maxim Integrated Products, Inc.

Related Parts		
MAX16997	High-Voltage Watchdog Timers with Adjustable Timeout Delay	Free Samples
MAX16998	High-Voltage Watchdog Timers with Adjustable Timeout Delay	Free Samples

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 4210: http://www.maximintegrated.com/an4210
APPLICATION NOTE 4210, AN4210, AN 4210, APP4210, Appnote4210, Appnote 4210