Keywords: watchdog timer, watchdog circuit, windowed, reset, adjustable watchdog, capacitor adjustable watchdog

APPLICATION NOTE 1926

Watchdogs Improve System Reliability—How to Choose the Right Part

Mar 26, 2003

Abstract: Watchdog timers are used to monitor and minimize code execution errors. Internal watchdog timers are subject to code execution problems, making external watchdog circuits invaluable in preventing system lockup.

This document provides assistance in selecting the right time of watchdog/supervisory product for different type of applications and how to apply the circuit without the software code.

Many circuit functions previously realized with dedicated hardware are now implemented in software, due in part to today's broad choice of low-cost microprocessors (µPs). While software is often the lowest cost and most flexible way to solve a problem, it forces the designer to take extra measures to ensure system reliability. While there is no such thing as a program without code errors, careful testing can reduce the number of errors to one to ten per 1000 lines of code. Therefore, designers must expect a minimum of 10 code errors in a typical control software program with 10,000 lines of code.

Desktop application software errors that cause a system crash are not critical since the user can reboot the system with only a minor loss of data. However, for industrial control software, the system must be able to recover from code errors without human intervention. This feature is critical for two main categories: systems that have high availability, such as servers, telephone systems, and production lines; and systems that must be highly reliable because a crash could lead to injuries, as with automobiles, medical instruments, industrial control, robots, and automatic doors. Even if neither of these criteria apply, system crash/recovery without user intervention (pressing reset or power cycling) is preferred. If a device recovers from an error without human intervention, the perceived quality of this device is good, as the user is unaware that something went wrong inside the device. A simple and effective method of achieving such improved system reliability is to use a watchdog.

The Watchdog

The watchdog is a counter that must be cleared within the watchdog timeout period. If clearing does not occur, the watchdog generates a reset to cause system reboot or creates a non-maskable interrupt (NMI), causing a program branch to a fault-recovery subroutine. Most watchdogs are edge triggered. Therefore, either a rising or a falling edge on the watchdog input (WDI) will clear the counter. The WDI pin is connected to a processor I/O pin, which is toggled by the software (**Figure 1**).
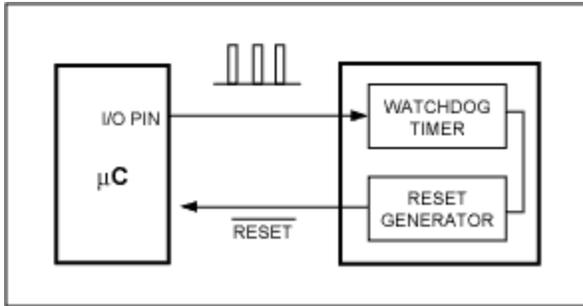
Figure 1. The microprocessor clears the watchdog timer with a pulse on the WDI pin to prevent a reset.

The command to clear the watchdog counter must occur within the main program loop (**Figure 2**). If the watchdog is not cleared, a reset occurs and the software branches to address 0000 (startup routine). Calculating the time it takes to execute the main loop is often difficult, as numerous subroutines might be called, depending on the inputs to the system. Therefore, the designer normally chooses a watchdog timeout that is much longer than the longest measured or calculated loop time.
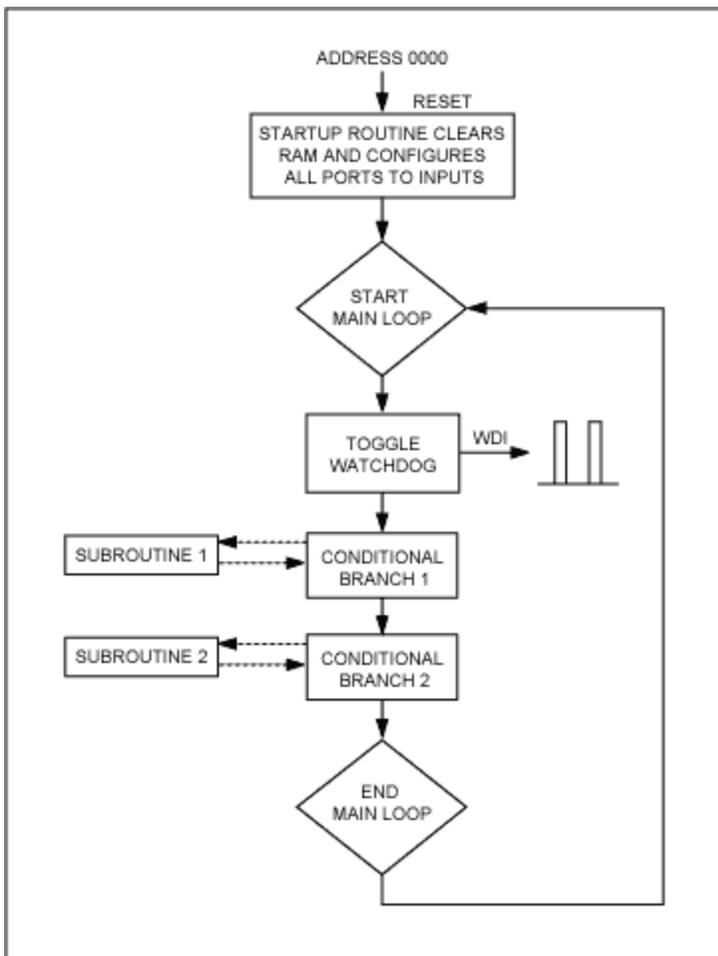

Figure 2. This figure shows a typical program flow with the WDI signal generated within the main loop.

Figure 3 shows the watchdog and reset signal for normal operation (watchdog is cleared within timeout period). In **Figure 4**, a reset is generated after the watchdog counter reaches the timeout. Industry-

standard watchdog circuits have timeouts in the 100ms to 2s range, although there are adjustable and customized watchdogs covering a much wider range (30ms to minutes). If the execution time of the main loop is too long for the watchdog, the designer can implement multiple watchdog-toggle commands within different sections of the main loop or use a device with longer timeout.
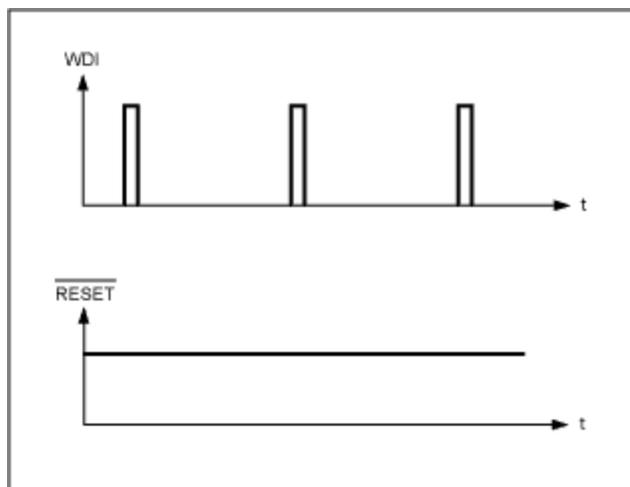

Figure 3. If the WDI pin is always toggled within the watchdog timeout, no reset is generated.
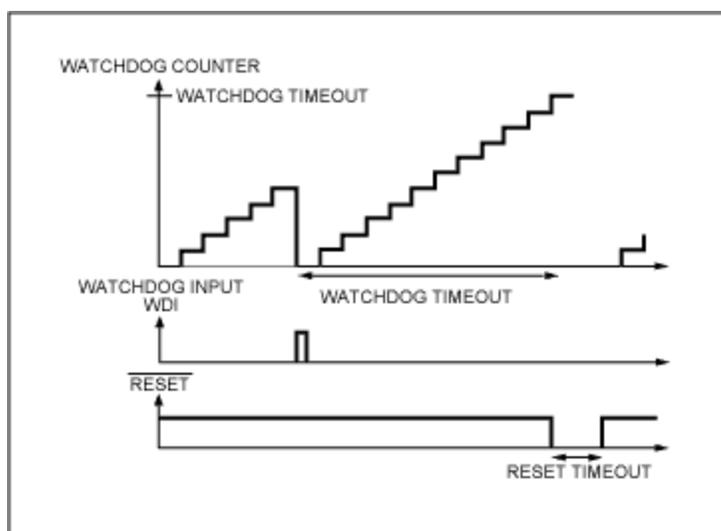

Figure 4. As soon as the watchdog counter reaches the timeout value, a reset is generated.

A technique that prevents the system from being stuck in a parasitic loop is to set the relevant I/O pin high at the beginning of the main loop, and to set it low in another section of the main loop. If the software gets stuck in a parasitic loop at the start of the main loop, the watchdog times out and the system recovers, as WDI remains high (**Figure 5**). If a low-high-low pulse is used (as in Figure 2), the watchdog will be cleared, but the system will remain stuck. A more sophisticated scheme might be necessary for programs with multiple tasks that require monitoring. Each task sets a flag, and the watchdog is only toggled if all flags are set. The duration of all tasks must be shorter than the watchdog timeout period. Figures 2 and 5 might seem simplistic compared to actual programs, but they illustrate the relevant concepts. Other potential problems in more complex systems, such as memory leakage and stack overflow, should also be monitored. This is beyond the scope of this article, but is typically done by using suitable design procedures, performing a careful code review, and employing specialized software
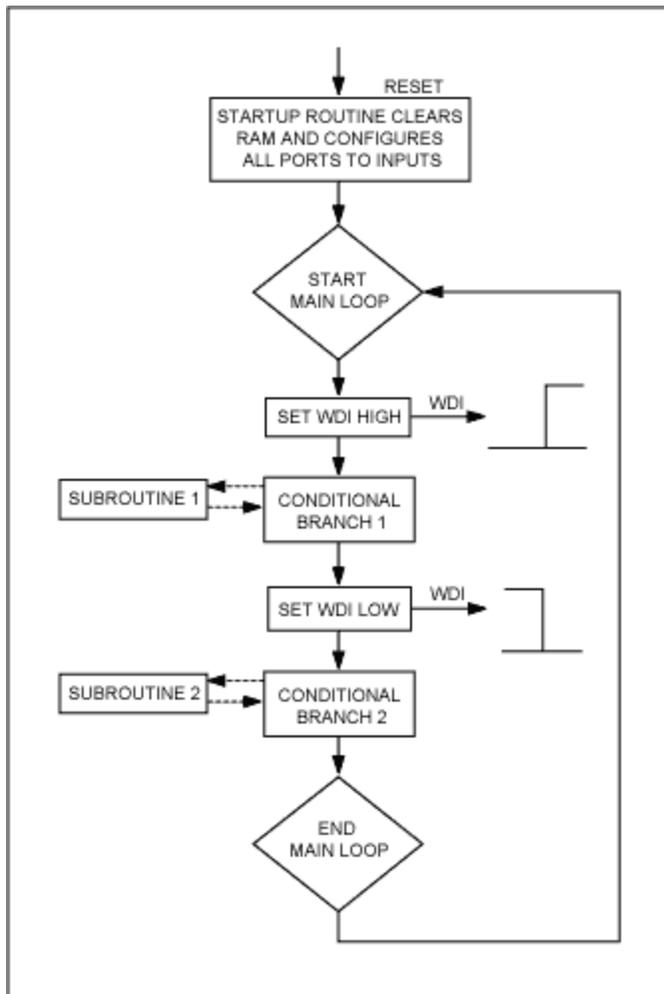
tools.

Figure 5. An improved program flow has two separate watchdog-toggle commands, which generate a rising-and a falling-edge signal on the WDI pin. This prevents the program from being stuck in a parasitic loop.

Internal vs. External Watchdog

Many µPs have an integrated programmable watchdog that can be disabled under software control. The internal watchdog is prone to code errors, so does not provide the same protection as an independent external watchdog. For safety-critical applications (i.e., automatic doors, medical devices, robots), the internal watchdog is unacceptable. Regulating bodies demand use of a separate, external watchdog. Thus, it is good practice to use an external watchdog to reduce the risk of critical system failures.

Simple Watchdog Plus Reset

Since a watchdog timeout normally resets the system, most watchdogs are integrated with a µP reset that also monitors the processor supply voltage. The reset is activated either by the watchdog or by an undervoltage condition. The MAX823-MAX825 family shown in **Figure 6** combines these two functions and is available with standard reset voltages, one nominal watchdog, one reset-timeout, and only 6µA current consumption. These devices are available in the ultra-small SC70 package.
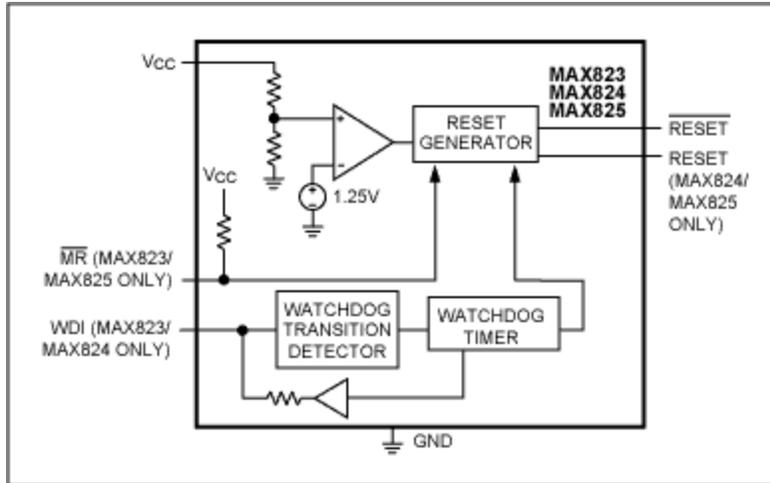
Figure 6. The MAX823-MAX825 family integrates two popular functions: watchdog and reset.

Factory-Preset Watchdog Families

The MAX6316-MAX6322 family offers a choice of 26 factory-preset reset voltages, four nominal-watchdog and four nominal-reset timeouts, and four output configurations (see Table 1).

Table 1. Features of Selected Supervisory Products

Application	Family	Voltage Monitoring	Watchdog Timeout (min)	Reset Timeout (min)	Special Features
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 reset outputs
	MAX6721-MAX6767		25.6s startup		
Windowed	MAX6323/ MAX6324 Dual	Factory-preset 2.5V, 3V, 3.3V, or 5V	1.5ms to 719ms (min); 10ms to 1.3s	100ms	Eight factory-trimmed options; timeout reset pulses accepted only within the defined

Mode	(max) window	window

Capacitor-Adjustable Watchdogs

If the application requires a flexible watchdog timeout, the designer can use an adjustable circuit. The MAX6746-MAX6753 family offers either factory-preset or voltage-divider-programmable reset voltages, as well as external capacitor adjustment of watchdog and reset timeouts. **Figure 7** shows a typical operating circuit where:

- the reset voltage is determined by the voltage divider R1/R2,
- the reset timeout is determined by the capacitor to set the reset timeout (C_{SRT}), and
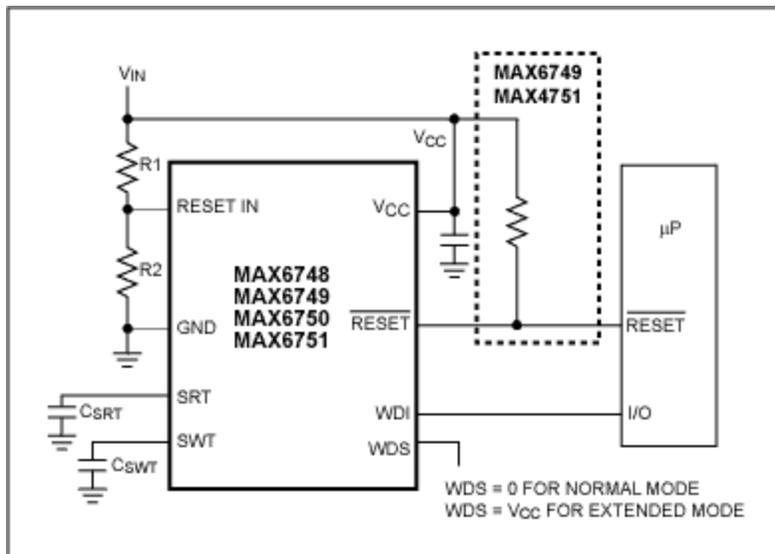- the watchdog timeout is set by the capacitor to set the watchdog timeout (C_{SWT}).

Figure 7. This figure shows a typical application circuit for the capacitor-adjustable watchdog family MAX6346-MAX6353.

Figure 8 shows the watchdog-timeout range for C_{SWT} values from 100pF to 100nF. With this wide range of available watchdog timeouts, the designer has a solution for any application. The MAX6301-MAX6304 family has basically the same features as the MAX6746-MAX6753 family, but is available in SO and DIP packages.
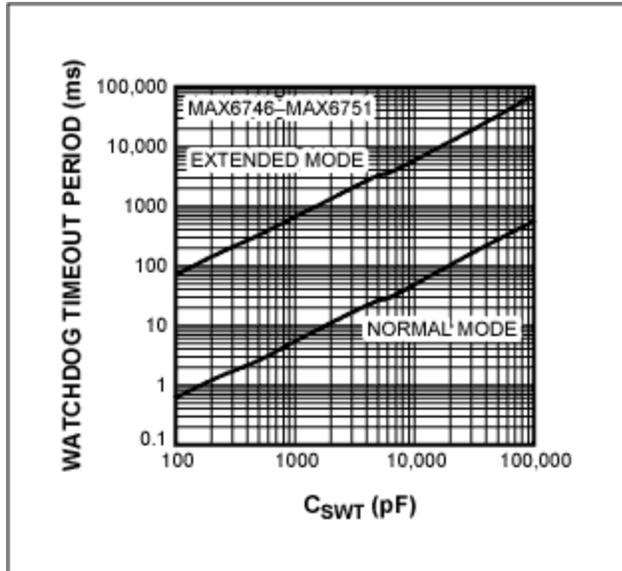
Figure 8. This figure shows the wide range of available watchdog timeouts.

Pin-Selectable Watchdogs with Longer Startup/Timeout

If the startup routine is long (see Figure 2), a watchdog with two different timeouts is desirable: a longer initial timeout and a shorter timeout for normal operation. The MAX6369-MAX6374 family has a pin-programmable startup delay selectable from 200ms to 60s and a watchdog timeout range of 30ms to 60s. Some versions offer a first-edge activation of the watchdog to provide a solution for even longer startup routines. For these chips, the watchdog is disabled during startup and is activated by the first edge from the relevant I/O pin of the µP.

Watchdogs with Multiple Supply Voltages

For systems with dual supply voltages, the MAX6358-MAX6360 family can monitor two standard voltages, and offers a watchdog with a long startup as well as a normal timeout. For systems with three supply voltages or that require both active-high and active-low reset functions the designer can use the MAX6721-MAX6729 family. These parts have a dual-mode watchdog with long startup plus normal timeouts. They monitor either two standard supply voltages (MAX6721-MAX6722) or two standard plus a third adjustable supply voltage (MAX6723-MAX6724). These are available with manual-reset input, power-fail comparator, dual reset outputs, and RESET and active-low RESET outputs.

Windowed Watchdogs for Ultra-High Reliability

For ultra-high reliability, the designer can use the MAX6323/MAX6324 windowed watchdogs. With these parts, the pulse clearing the watchdog must occur within a well-specified time window. A valid pulse may come as early as 1.5ms after the last pulse or could arrive as late as 10ms after the last pulse (see Table 1 for additional ranges). With the MAX6323/MAX6324 the system recovers from parasitic loops, which can generate a fast-pulse train if the clear-watchdog command is within the loop. These pulses would clear a normal watchdog and no reset would be generated. This can be avoided with windowed watchdogs, as they require a minimum delay between watchdog pulses. Typical applications for these devices are anti-lock brake systems or other automotive circuits, industrial and medical applications where high safety requirements apply, or applications where system availability is critical.

Conclusion

Since every software program has code errors, the designer must ensure that the system does not lock up. Noise and EMI can also affect data in the system and lead to unpredictable system behavior. A

watchdog is a simple, inexpensive way to improve system reliability. An external watchdog protects the system from being stuck and resets the µP if WDI is not toggled within the watchdog timeout period. With today's wide choice of watchdogs, the designer is sure to find a device-requirement match.

Related Parts		
MAX6301	+5V, Low-Power, µP Supervisory Circuits with Adjustable Reset/Watchdog	Free Samples
MAX6304	+5V, Low-Power, µP Supervisory Circuits with Adjustable Reset/Watchdog	Free Samples
MAX6316	5-Pin µP Supervisory Circuits with Watchdog and Manual Reset	Free Samples
MAX6322	5-Pin µP Supervisory Circuits with Watchdog and Manual Reset	Free Samples
MAX6323	µP Supervisory Circuits with Windowed (Min/Max) Watchdog and Manual Reset	
MAX6324	µP Supervisory Circuits with Windowed (Min/Max) Watchdog and Manual Reset	
MAX6358	Dual/Triple-Voltage µP Supervisory Circuits	Free Samples
MAX6360	Dual/Triple-Voltage µP Supervisory Circuits	Free Samples
MAX6721	Dual/Triple Ultra-Low-Voltage SOT23 µP Supervisory Circuits	
MAX6723	Dual/Triple Ultra-Low-Voltage SOT23 µP Supervisory Circuits	
MAX6724	Dual/Triple Ultra-Low-Voltage SOT23 µP Supervisory Circuits	
MAX6729	Dual/Triple Ultra-Low-Voltage SOT23 µP Supervisory Circuits	Free Samples
MAX6746	µP Reset Circuits with Capacitor-Adjustable Reset/Watchdog Timeout Delay	Free Samples
MAX6753	µP Reset Circuits with Capacitor-Adjustable Reset/Watchdog Timeout Delay	Free Samples
MAX823	5-Pin Microprocessor Supervisory Circuits with Watchdog Timer and Manual Reset	Free Samples
MAX824	5-Pin Microprocessor Supervisory Circuits with Watchdog Timer and Manual Reset	Free Samples
MAX825	5-Pin Microprocessor Supervisory Circuits with Watchdog Timer and Manual Reset	Free Samples