Application Note 602

Title: **Windowed watchdog enhances security in automotive and industrial applications**

Product Family: **Supervisory ICs**

Part Number: EM6151, EM6152 (V6150, A6150, A6250, V6155, A6155, V6130, A6130)
Keywords: windowed watchdog, µP supervisory IC, security, automotive, LDO, power package
Date: November 28, 2005

Summary:

For applications where a system crash could cause human injury or systems requiring high availability, such as automatic doors and windows, medical applications, telephone systems and production lines, highest reliability is required. This type of system requires also seamless recovery without human intervention. Windowed watchdog circuits like the EM Microelectronic's EM6151 and EM6152 provide highest error recognition coverage in an independent circuit that can reset the system microprocessor and also inhibit any actions by mechanical actuators.

Windowed watchdogs recognize not only the error case of programs executing too slowly, for whatever reason, as a standard watchdog does, but also the case of a program executing too quickly, significantly increasing the error recognition coverage. The EM6152 products also include power supply monitoring and a robust 5V low dropout voltage regulator in the same package.

Introduction

As more and more functions involving human safety are carried out by microprocessor-controlled systems the importance of close performance monitoring is increasing. The low cost and wide choice of features for many different applications of today's microprocessors is allowing them to be used in many applications that earlier were done with dedicated hardware. While microprocessors are highly flexible problem solution tools, their functional reliability is lowered by the probability of code errors in the program. Careful and complete testing will find most errors, but 100% coverage can never be assured.

High reliability is required from systems that could cause injury if they malfunction, such as found in automotive applications, medical instruments, robots, industrial control and automatic doors. These systems must be able to recover from a crash without human assistance, pressing a reset button for example, as any human intervention would probably be too late to avoid injury.

The watchdog is a sub-system that can cause a program reset or NMI if the microprocessor does not react within a certain amount of time. This can catch a misbehaving microprocessor system in many cases. For highly sensitive applications windowed watchdogs are used which will activate when either being cleared too slowly or too quickly. This adds another class of program errors or faulty hardware behavior that will be recognized. Ideally, a watchdog-monitored system is able to restart itself back into a working state and the user will not even know that an error has occurred. To achieve this level of comfort the system must be conceived and the software programmed to be able to accept a reset at any time and to resume normal operation without any operator intervention.

Many microcontrollers offer an internal programmable watchdog with similar functionality. These watchdogs can, however, all be disabled by the software and do not provide the same protection for safety critical applications as an independent external watchdog circuit. Hence it is highly recommended to use an external watchdog and reset circuit in critical applications.

A COMPANY OF THE SWATCH GROUP

Description of Operation

Standard watchdogs are incrementing counters that set their output if their maximum value is reached. The microcontroller must reset the counter before that happens by creating a falling edge on the timer clear input. If the program execution is faulty because of a program error or external disturbance causing the program execution to be slower the maximum value will be reached and the output set active. This will catch problems such as hanging because of endless loops. It will not, however, trigger for such errors as routines returning before normal completion, which will cause the program execution to be faster.

For highest security a windowed watchdog demands that the timer clear input edge be within a certain window that is considered correct. If the signal arrives before or after this timing window it triggers the output signal to either reset the processor or activate other error handling. This type of watchdog will effectively cover both the case of a program executing too slowly and the case of a program executing to quickly. The danger of relying on a standard watchdog for high reliability applications is shown in figure 1.

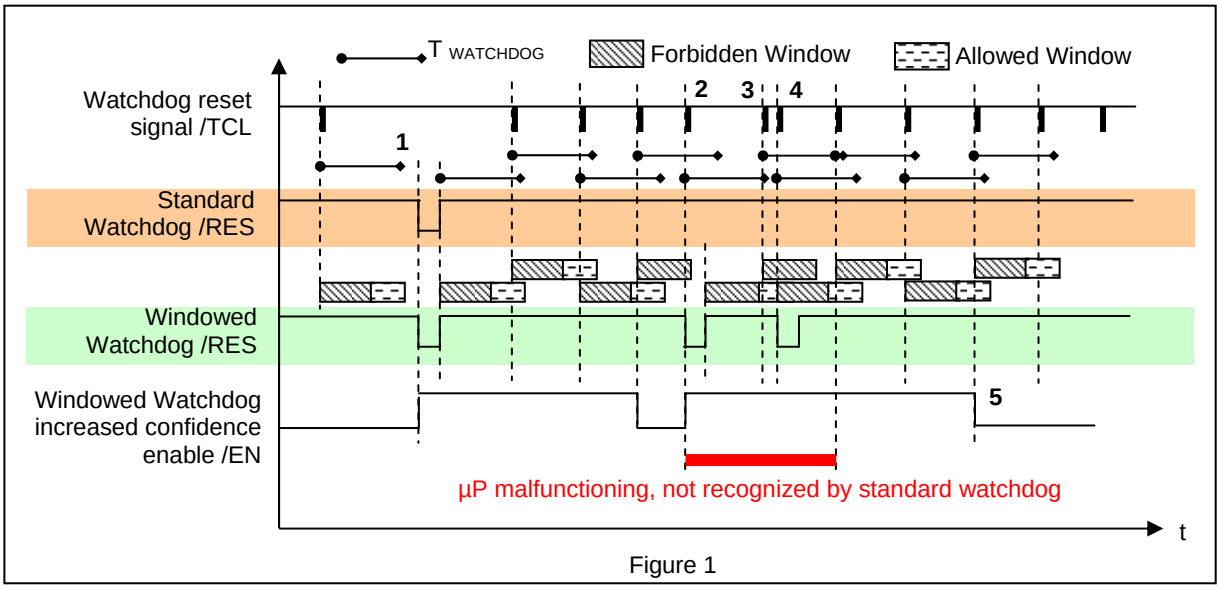

Figure 1

1) Reset after watchdog timeout
2) Reset caused by /TCL arriving too soon, during Forbidden Window
3) Timing OK
4) Reset caused by /TCL arriving too soon, during Forbidden Window
5) Enable asserted after 3 good /TCLs

For applications that could cause human injuries such as automatic car windows or doors the use of a windowed watchdog is highly indicated and it is state of the art. Many other applications can profit from the added reliability that a windowed watchdog provides.

The products EM6151/52 (the so-called “615x” family) are windowed watchdog chips that include power surveillance and an increased confidence enable output. The power-on-reset delay and the time window are programmable and the time base accuracy is guaranteed to ±10%. The EM6151 contain a windowed watchdog and reset functions. EM6152 contain in addition an internal 5V LDO voltage regulator and represent highly integrated solutions reducing chip count and circuit board area, which is ideal for systems, such as automobiles, where the intelligence is distributed over many functional units. In addition, EM6152 can also come in a power package PSOP16 and its 5V regulator can draw up to 250mA, making it an obvious choice for automotive applications. The reset output is guaranteed down to a working voltage of 1.2 volts.

The watchdog timing is broken into 2 periods. The time when the /TCL falling flank signals an error is called the Forbidden Window. The time when the /TCL input falling flank resets the timer, is accepted, is called the Allowed Window. In some documentation the Allowed Window is called the Open Window and the Forbidden Window is called the Closed Window. The time after the Allowed Window is a timeout. The 615x products allow programming the watchdog time T_{WD}. The Allowed Window is during the time ±20% of the watchdog time T_{WD}. The Forbidden Window is during the time up to 80% of T_{WD}. The watchdog timeout is at T_{WD} + 20%. Please see figure 2. If no /TCL has been received until the end of the Allowed Window the watchdog will immediately produce a reset pulse. Both a falling flank on /TCL during the Forbidden Window and the timeout after T_{WD}+20% will cause a reset to be asserted and the enable to be removed. It should be noted that the timing for the next period starts immediately from the falling flank of /TCL.

Copyright © 2004, EM Microelectronic-Marin SA

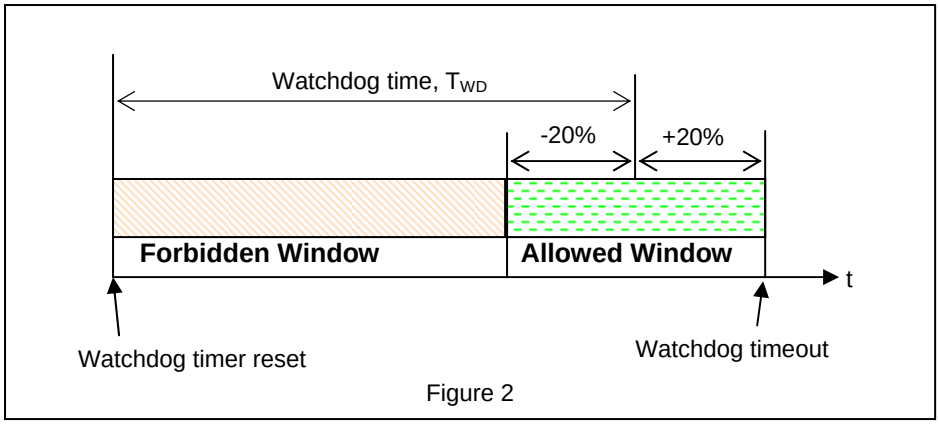

Figure 2

The operation of a 615x product and their increased confidence Enable output is shown in figure 3.

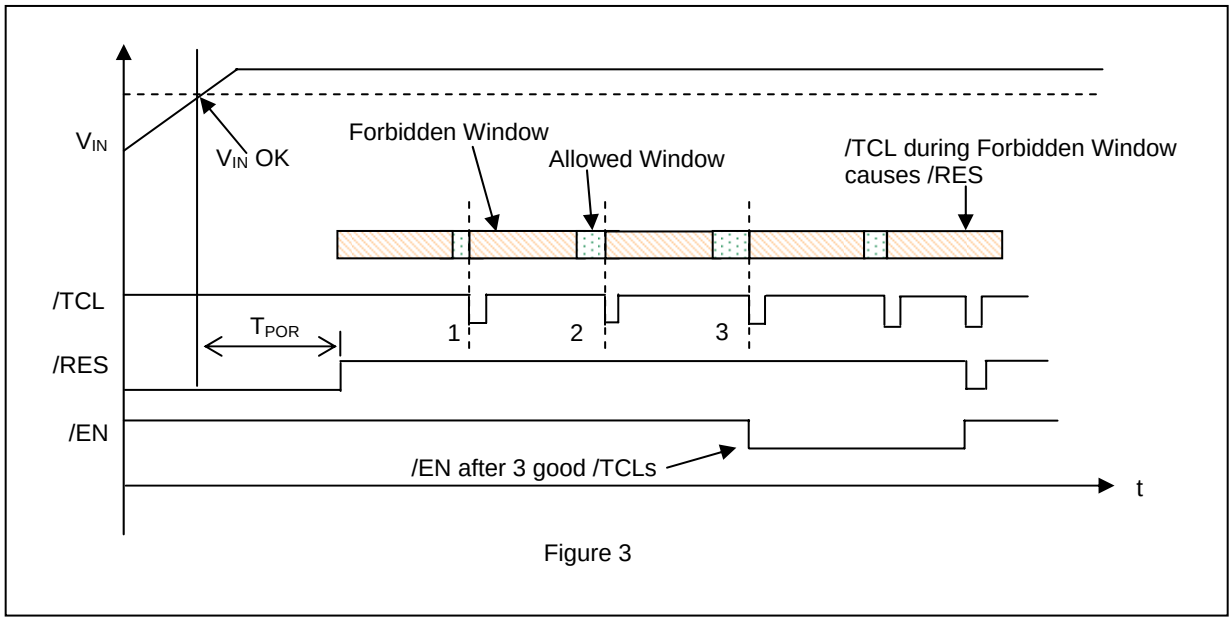

Figure 3

1) After the power supply voltage enters the good voltage range the reset is held for another $T_{POR}=T_{WD}$ ms.
2) The increased confidence enable output /EN goes active after 3 successful watchdog cycles. It can now be assumed that the microprocessor is functioning properly.
3) If the /TCL watchdog input arrives during the Forbidden Window time a reset is caused and enable removed.
4) The next Forbidden Window starts immediately when a /TCL has been seen.
5) If the watchdog times out, i.e. the Allowed Window comes to an end without seeing a /TCL signal, a reset is caused (not shown on this diagram).

The increased confidence enable output can be used to gate motor signals, for instance, to immediately stop the motor movement when the processor behavior can not be trusted and only allow it again when there is confidence that the processor is running properly.

Copyright © 2004, EM Microelectronic-Marin SA

Along with their windowed watchdog functions, EM6151 includes an accurate, protected 5V low-dropout voltage regulator and all the features of a standard voltage supervisory circuit as shown in figure 4.

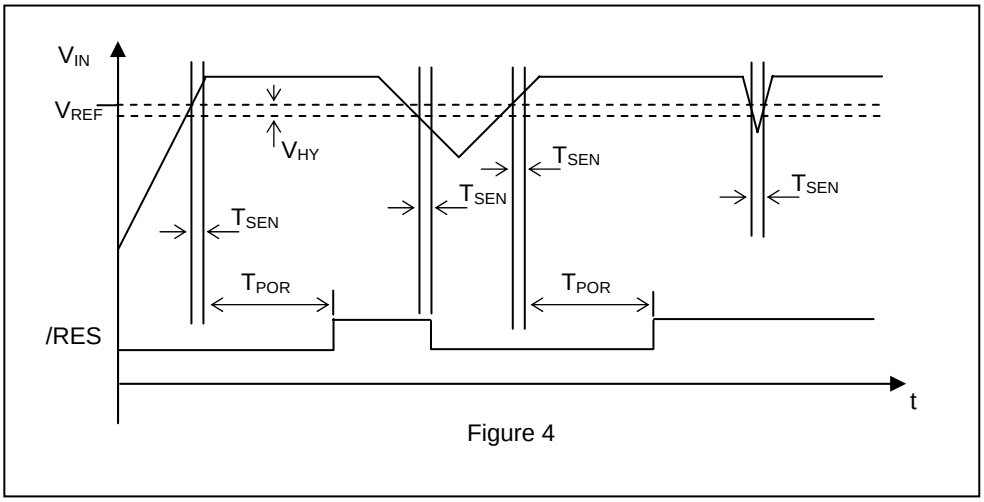

Figure 4

Applications

A standard application example for A6150/A6250 is shown in figure 5

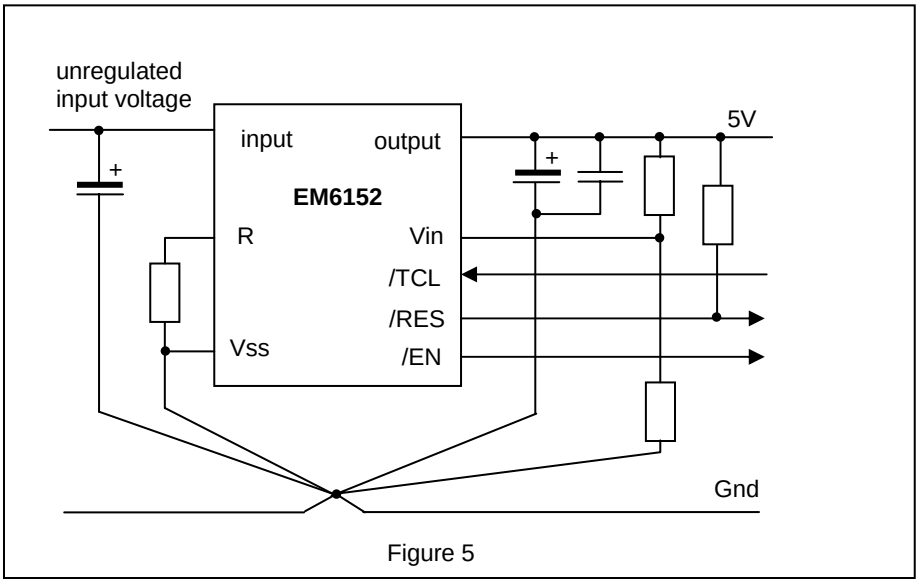

Figure 5

It is important to note that for the EM6152 specifically, as with any voltage regulator, the PCB layout is very important to the success of the design. The routing of the decoupling capacitors to the supply and ground traces or planes must be clean and short. Circuitous paths increase the circuit inductance and possibly increase the cross coupling between inputs and outputs. Clean separation between logic supply and the power portion of the circuitry is especially important in circuits controlling electrical motors with the large spikes that they will produce on the power supply lines. Please see EM Microelectronic AppNote 600 for more details on this subject and for the correct specifications of decoupling capacitors.

Thermal issues must also be taken into account when doing the layout for the EM6152. The housing has a heat sink contact, a so-called “thermal slug”, which must be soldered to the PCB to achieve the thermal figures given on the data sheet. The PCB should foresee surface area as a radiator around this chip. It is best to have circuit planes on both board sides connected thermally to the slug with thermal vias to transfer the heat as efficiently as possible away from the chip. The achieved thermal resistance in any particular application is highly dependent on the physical configuration of the complete module, PCB cooling surfaces, thickness, airflow, convection, horizontal or vertical orientation, etc.

Copyright © 2004, EM Microelectronic-Marin SA

For applications requiring program control of the function supervised by this watchdog or applications where the circuitry should be turned off completely to achieve absolute lowest power consumption the simple external circuit shown in Figure 6 program on/off functionality can be added.

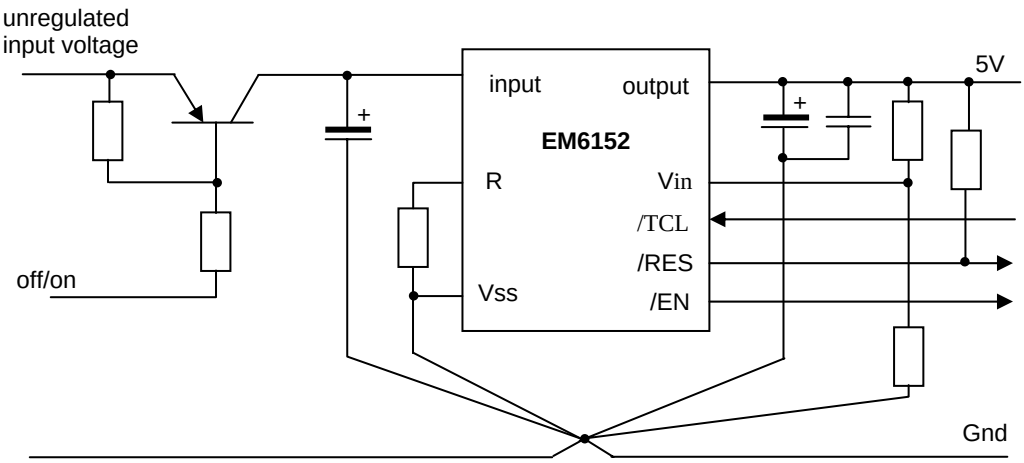

Figure 6

Conclusion

A highly integrated solution including power supply supervision, a windowed watchdog, which provides greatly improved error case coverage compared to a standard watchdog and an internal voltage regulator, the EM Microelectronic A6250 lends itself admirably for applications requiring stringent security surveillance in today's distributed intelligence automotive and industrial systems.

Just a short list of automotive application areas could include:

- Window motor control
- Sunroof motor control
- Dashboard computer systems
- Angular steering sensors
- Trunk closure systems
- Cruise control
- Spoiler automatic
- Automatic sliding door control
- Automatic transmission control
- Motor control

These components are available in the automotive temperature range, guaranteed up to 125°C. They are also available without the internal voltage regulator as the part EM6151. For ultra-low power applications using sleep mode, such as those using CAN-Bus communication where functional units can be disabled under software control, the EM6152V55, with voltage regulator, and EM6151V55, without voltage regulator, can recognize being placed in sleep mode and adapt their behavior to reduce system power consumption without loosing security.

For safety critical applications such as medicine delivery devices, medical monitoring systems, robots and automatic doors and windows, wherever they may be installed, a windowed watchdog is the component of choice to be sure to fulfill the demands of regulating bodies in terms of human safety.

EM Microelectronic-Marin SA (EM) makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in EM's General Terms of Sale located on the Company's web site. EM assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of EM are granted in connection with the sale of EM products, expressly or by implications. EM's products are not authorized for use as components in life support devices or systems.

© EM Microelectronic-Marin SA, 11/05, Rev. B