



## congatec Application Note

<b>Affected Products</b>	All congatec products
<b>Subject</b>	congatec Watchdog features and implementation
<b>Confidential/Public</b>	Public
<b>Author</b>	EHA

## Revision History

---

Revision	Date (yyyy-mm-dd)	Author	Changes
0.1	2005.05.09	EHA	Document created
1.0	2006.06.25	HCH	Initial Release
1.1	2005.10.26	GDA	Added note about S3 (save to Ram) to Notes and Cautions section 6.
1.2	2006.01.18	GDA	Added information about the timeout values. Added information to section 5.3.1. Added note about Watchdog ACPI Event to section 6.
1.3	2006.08.25	HCH	Changed File name to match data base requirements
1.4	2006.09.22	GDA	Removed sections 5.3 and 5.3.1.
1.5	2017.02.28	BEU	Updated template and revised entire document.

## Preface

---

This application note describes the Watchdog feature found on congatec AG products. It explains the full feature set, however some items may not be applicable for systems which do not support all Watchdog features.

## Disclaimer

The information contained within this Application Note, including but not limited to any product specification, is subject to change without notice.

congatec AG provides no warranty with regard to this Application Note or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec AG assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the Application Note. In no event shall congatec AG be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this Application Note or any other information contained herein or the use thereof.

## Intended Audience

This Application Note is intended for technically qualified personnel. It is not intended for general audiences.

## Electrostatic Sensitive Device

All congatec AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec AG Limited Warranty.

## Technical Support

congatec AG technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at [www.congatec.com](http://www.congatec.com) for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at [support@congatec.com](mailto:support@congatec.com)

## Symbols

The following are symbols used in this application note.



***Notes call attention to important information that should be observed.***



***Cautions warn the user about how to prevent damage to hardware or loss of data.***



***Warnings indicate that personal injury can occur if the information is not observed.***

## Copyright Notice

Copyright © 2005, congatec AG. All rights reserved. All text, pictures and graphics are protected by copyrights. No copying is permitted without written permission from congatec AG.

congatec AG has made every attempt to ensure that the information in this document is accurate yet the information contained within is supplied “as-is”.

## Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user’s guide, or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

## Terminology

Term	Description
Watchdog	A Watchdog is a combination of system means that support automatic recovery from an error condition such as deadlocks and system hangups.
Watchdog Timeout	A Watchdog Timeout defines the time period after which the Watchdog generates a Watchdog Event if there is no longer a response from the system.
Watchdog Event	If there is no system response within a defined time period, then the Watchdog generates a Watchdog Event. Usually this is a hardware signal such as a non-maskable interrupt or a reset signal.
Watchdog Trigger	This is the system response that forces the Watchdog to reload its timeout counter, i.e. triggering the Watchdog prevents a Watchdog Event.
BIOS Power On Self Test (POST)	This is the amount of time needed for system initialization between power-up and the start of the loading of the operating system.
Runtime	The phase of normal system operation starting with the loading of the operating system, i.e. after the POST has finished.
CMOS Setup Utility	This is the system configuration tool built into the BIOS. It controls the CMOS RAM used to save the system configuration.
CGOS API	This is the abbreviation for the congatec uniform operating system application programming interface.

## Contents

---

1	Runtime Watchdog.....	7
1.1	Runtime Watchdog Modes.....	7
1.1.1	Single Event Mode.....	7
1.1.2	Repeated Event Mode.....	7
1.1.3	Single Trigger Mode.....	7
1.1.4	Watchdog Timing Diagram.....	8
1.2	Watchdog Events.....	9
1.2.1	NMI / IRQ.....	9
1.2.2	ACPI Event.....	9
1.2.3	Reset.....	9
1.2.4	Power Button.....	9
2	Post Watchdog.....	9
3	Watchdog Configuration, Initialization, and Lifetime.....	10
3.1	Watchdog Configuration via the BIOS setup.....	10
3.2	Watchdog Configuration via the CGOS API.....	10
3.3	Initialization and Lifetime.....	10
4	Watchdog Triggering.....	11
4.1	Watchdog Triggering via the CGOS API.....	11
4.2	External Trigger Method.....	11
5	Notes and Cautions.....	12

## 1 Runtime Watchdog

---

The Runtime Watchdog is available during normal system operation and is used to recover from malfunctioning operating systems, application software or system expansions like add-in hardware or peripheral devices. It supports up to three stages. For every stage a separate timeout value and event type can be specified. The granularity of the timeout values is one millisecond and the watchdog timer may have a maximum deviation of 2%.

### 1.1 Runtime Watchdog Modes

The Watchdog Mode defines what happens when the Watchdog generates the event of the last defined stage. When there are several stages defined, then the Watchdog switches to the next stage after generating an event. The selected Watchdog Mode defines how the Watchdog behaves after it has generated the last defined event. Below is a list of the possible modes.

#### 1.1.1 Single Event Mode

In the Single Event Mode, the Watchdog switches off after generating the event of the last defined stage.

#### 1.1.2 Repeated Event Mode

When in the Repeated Event Mode, and after generating the event of the last defined stage, the Watchdog stays in the last stage and restarts the timeout counter.

#### 1.1.3 Single Trigger Mode

The Single Trigger Mode is a variant of the Single Event Mode. It also switches off after generating the event of the last defined stage. Additionally, it switches off when it gets triggered the first time.

## 1.1.4 Watchdog Timing Diagram

Figure 1: single stage / single event mode

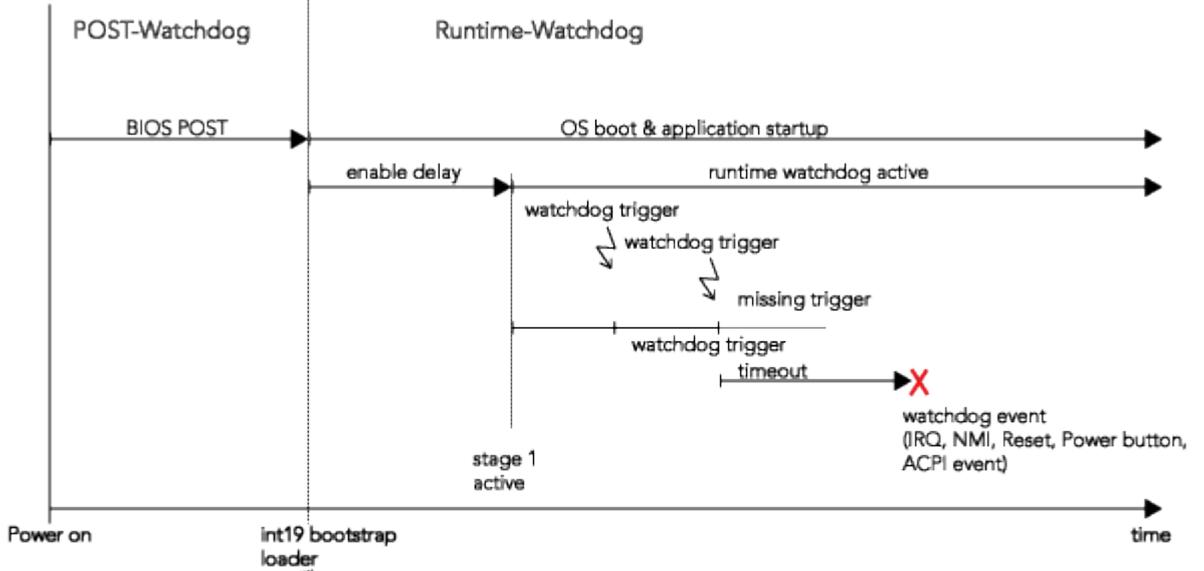
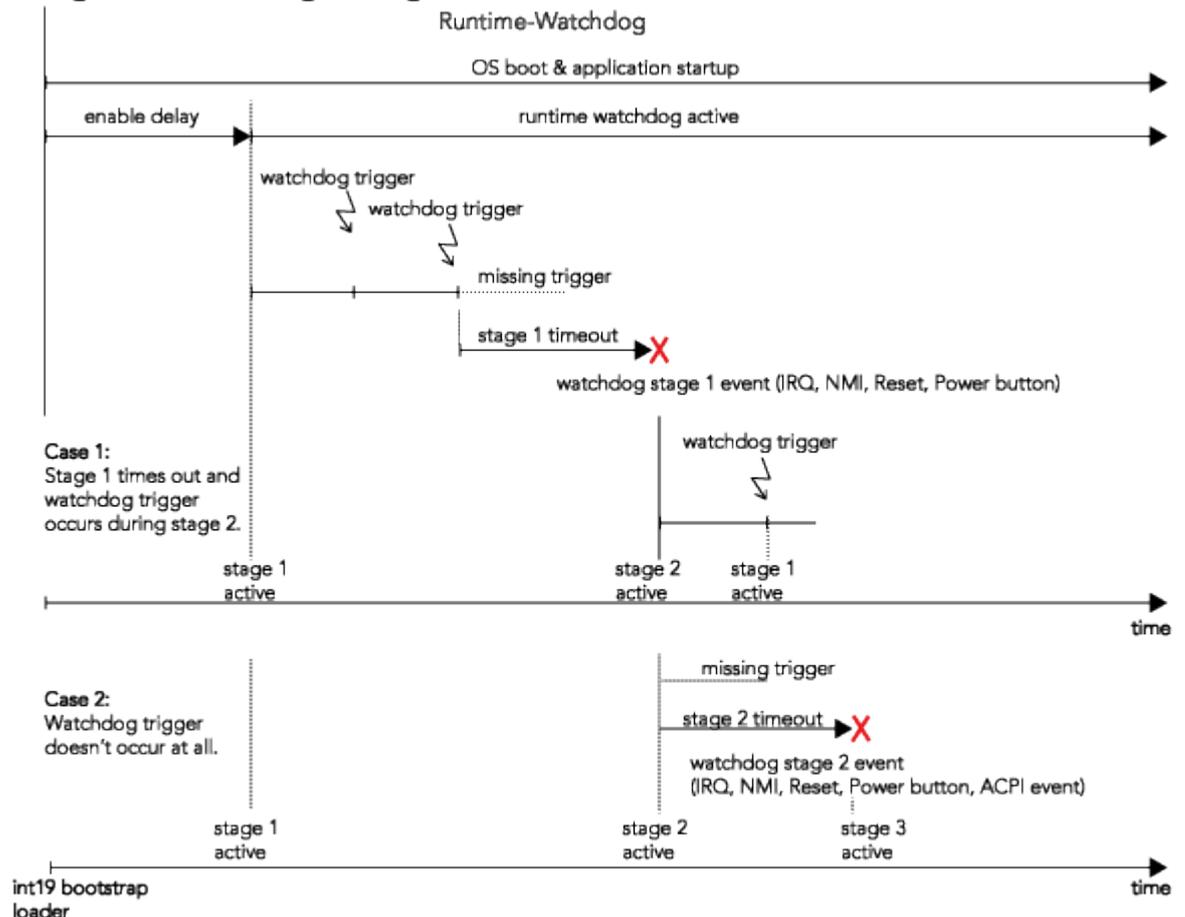


Figure 2: multi stage / single event mode



## 1.2 Watchdog Events

The following is a description of possible Watchdog Events.

### 1.2.1 NMI / IRQ

This Watchdog Event generates an interrupt. Depending on the system implementation this may be a non-maskable interrupt (NMI) or a normal interrupt request (IRQ).



*Not all products support NMI / IRQ.*

### 1.2.2 ACPI Event

This Watchdog event generates an ACPI system control interrupt. Depending on the Watchdog ACPI event setting in the BIOS setup program, this interrupt will either cause a system shutdown or restart. See section 5 “Notes and Cautions” for more information about the ACPI Event.

### 1.2.3 Reset

This Watchdog Event generates a platform reset signal. After generating the reset signal the Runtime Watchdog gets switched off and no further Watchdog stages will be processed.

### 1.2.4 Power Button

This Watchdog Event generates a power button signal. Depending on the system state and configuration, this can invoke a system shutdown, switch off the system or power up the system.

## 2 Post Watchdog

---

The POST Watchdog is available during the system initialization process and is used to recover from a malfunction of system expansions like add-in hardware or peripheral devices. If enabled the POST Watchdog is started immediately after system power up and automatically switched off when the POST is finished and the system is ready to load the operating system. If the system does not finish the POST within the time period defined by the POST Watchdog timeout, then the Watchdog generates a reset signal to reboot the system. The granularity of the timeout value is one millisecond and the watchdog timer may have a maximum deviation of 2%.

## 3 Watchdog Configuration, Initialization, and Lifetime

---

### 3.1 Watchdog Configuration via the BIOS setup

The setup program for the BIOS provides a BIOS submenu that is used to configure the Watchdog. Any changes done in the BIOS setup will take effect on the next boot just before the OS is launched.



*See the BIOS setup program description of your particular congatec AG product for a detailed list of the options.*

### 3.2 Watchdog Configuration via the CGOS API

congatec AG products provide the CGOS API to configure and initialize the Runtime Watchdog. Changing the parameters via the CGOS API will take effect immediately. Please keep in mind that any Runtime Watchdog configuration done via the CGOS API will be overwritten by the Watchdog parameters that have been set using the BIOS setup program when the system reboots.



*See the CGOS API documentation (CGOSAPIm1x.pdf), which can be found on the congatec website at [www.congatec.com](http://www.congatec.com), for a more detailed description.*

### 3.3 Initialization and Lifetime

If the POST Watchdog is enabled, then it is initialized and started every time the system powers up or reboots. It stays active until the system reaches the end of POST. The POST Watchdog is switched off automatically before the system starts loading the operating system. Additionally, the POST watchdog is switched off automatically when invoking the BIOS setup or when entering a BIOS boot menu.

If the Runtime Watchdog is enabled via the BIOS setup, then it is initialized and started automatically at the end of POST. Additionally, it can be initialized and started at any time during runtime via the CGOS API. Except for when in the Single Trigger Mode, the Runtime Watchdog stays active as long as it gets triggered and the system continues to run. The Watchdog can be switched off at any time during runtime via the CGOS API. The Watchdog switches off automatically when being triggered in single trigger mode or after generating a RESET event.

## 4 Watchdog Triggering

---

Triggering the Watchdog within the Watchdog Timeout interval prevents the Watchdog from generating an event. When there are several Watchdog stages defined, then triggering the Watchdog also forces the Watchdog back to the first stage. There are different methods of triggering the Watchdog. Below you will find a description of each trigger method.

### 4.1 Watchdog Triggering via the CGOS API

The usual method of triggering the watchdog is through the use of the CGOS API.



*See the CGOS API documentation (CGOSAPIm1x.pdf), which can be found on the congatec website at [www.congatec.com](http://www.congatec.com), for a more detailed description.*

### 4.2 External Trigger Method

Some congatec AG products support triggering the Watchdog via an external trigger signal called WDTRIG.



*See the user's guide of your particular congatec AG product for details about which connector the WDTRG is located on, pin number and signal requirements.*

## 5 Notes and Cautions

### Note

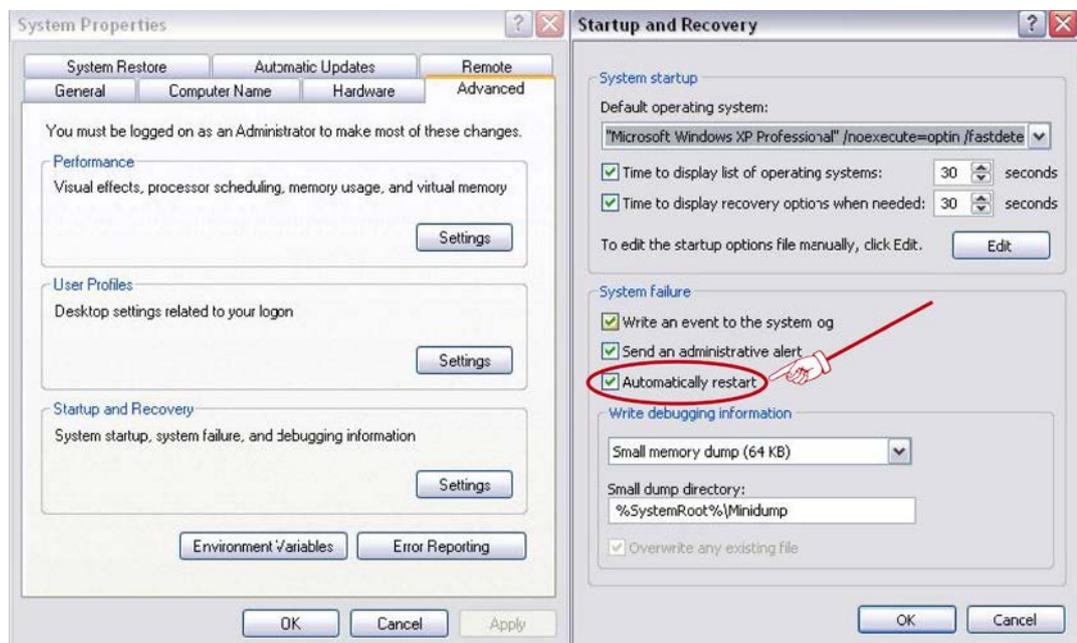
*In ACPI mode, it is not possible for a "Watchdog ACPI Event" handler to directly restart or shutdown the OS. For this reason, the congatec BIOS will do one of the following:*

*For Shutdown: An over temperature notification is executed. This causes the OS to shut down in an orderly fashion.*

*For Restart: An ACPI fatal error is reported to the OS.*

*It depends on your particular OS as to how this reported fatal error will be handled when the Restart function is selected. If you are using Windows, there is a setting that can be enabled to ensure that the OS will perform a restart when a fatal error is detected. The system will restart after a very brief blue-screen.*

*You can enable this setting by going to the "System Properties" dialog box and choosing the "Advanced" tab. Once there, choose the "Settings" button for the "Startup and Recovery" section. This will open the "Startup and Recovery" dialog box. In this dialog box under "System failure", there are three check boxes that define what Windows will do when a fatal error has been detected. In order to ensure that the system restarts after a "Watchdog ACPI Event" that is set to 'Restart', you must make sure that the check box for the selection "Automatically restart" has been checked. If this option is not selected, Windows will remain at a blue-screen, after a "Watchdog ACPI Event" that has been configured for 'Restart', has been generated. The following is a Windows screenshot showing the proper configuration.*



 Note

*By using several Watchdog stages, it is possible to escalate the Watchdog actions. For example, the Watchdog could generate an interrupt as a first event giving some interrupt handler of the application the chance to recover from an error condition. If this handler also fails to trigger the Watchdog, then the Watchdog may generate a reset signal to restart the system.*



## Caution

*Be careful when selecting a POST Watchdog timeout value. It should be taken into account that the power up time of peripheral devices may vary or option ROMs, such as LAN boot ROMs, may prolong the POST process. Choosing a POST Watchdog timeout value that is too short may be counterproductive. Instead of ensuring that only a recovery from a true malfunction is implemented, the system may reset periodically without a valid reason as a result of an incorrect Watchdog Timeout value.*

 Note

*It doesn't make any sense to select Watchdog Event RESET together with Repeated Event Mode because the Watchdog switches off immediately after generating the first reset signal due to the fact that a repeated reset signal is not supported.*

 Note

*It's possible that two Watchdog stages with Power Button Events could be used to configure defined system on/off times.*

 Note

*The Single Trigger Event may be useful for application software, which cannot use the CGOS API but still want to ensure that the operating system boots completely and starts the application code. In that case, the BIOS setup must be used to configure the Runtime Watchdog in Single Trigger Mode with one stage and event RESET. Together with a POST watchdog, this guarantees that the system is restarted until it makes it to the application code. The only thing the application code has to do is switch off the watchdog via a trigger event*

 Note

*Some congatec AG products support the power state S3 (suspend to RAM). On these particular products, the watchdog configuration is not saved when entering the S3 state nor is it restored when resuming from the S3 state. Generally, the watchdog is switched off after resuming from the S3 state. Applications which allow*

*the S3 power state but also require watchdog operation must reinitialize the watchdog when the system resumes from S3. For this, it may be necessary to register with the S3 resume notification of the operating system. A similar problem arises with operating systems supporting the power state S4 (suspend to disk), also known as hibernation mode. However, when resuming from the S4 state the runtime watchdog will continue to operate using the parameters that were defined with the BIOS setup. Any re-configurations done by an application before entering the S4 state are lost. Again, the application must register with the resume notification of the operating system if this behavior is not acceptable.*