FUJITSU

PRODUCT FACTS
Watchdog

Several Fujitsu Technology mainboards for industrial and semi-industrial applications provide a
HW watchdog for improved system reliability.
This document describes the possible implementation options (BIOS POST Watchdog, BIOS Boot Watchdog,
and Operating System Runtime Watchdog)

Brief Description

■ PC systems that need to meet highest reliability and availability requirements (e.g. in industrial and
mission-critical environments) can be designed using the "Watchdog" feature of Fujitsu Technology Solutions
industrial and semi-industrial mainboards.

■ This functionality is coupled with the autonomous System Monitoring controller on boards that are
equipped with the Silent Fan function. The integrated microcontroller is fully independent on CPU and
software; thus, it can serve as a reliable Watchdog to monitor regular "Watchdog Reset" events which
have to be performed by operating system tasks or by the SystemGuard utility. In case these retrigger
events fail to arrive on time, a malfunction of hardware or software has to be assumed; then the system
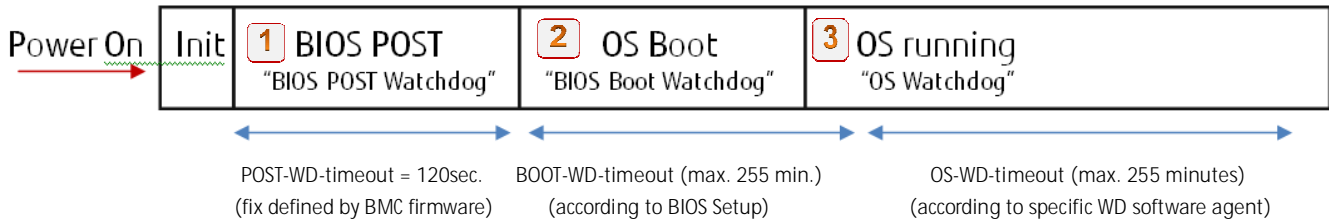is restarted.

WATCH DOG

Benefits

■ Additional reliability for industrial and mission-critical PC systems

■ The Watchdog itself is independent on the operating system and any application software; thus, it stays fully functional even in case of major
hardware and software failures

■ Additional BIOS POST Watchdog and/or BIOS BOOT Watchdog support for selected mainboard models

■ Easy setup of Watchdog functionality possible via BIOS Setup and SystemGuard utility

■ Integration in customer applications through programming interface (Windows API or Linux "lm-sensors" implementation)

Watchdog Implementation

BIOS POST Watchdog, BIOS (OS) Boot Watchdog, and Operating System Runtime Watchdog.
Please note that the implementation of the various Watchdog features depends on the mainboard model.
All three watchdogs are physical identical, but they are handled from different application levels

The following diagram shows the sequence after powering on the system:

POST-WD-timeout = 120sec.   BOOT-WD-timeout (max. 255 min.)   OS-WD-timeout (max. 255 minutes)
(fix defined by BMC firmware)   (according to BIOS Setup)   (according to specific WD software agent)

- After the mainboard is powered on, some basic hardware initializations (e.g. System Monitoring controller) are performed --> "Init".

- As soon as the System Monitoring controller ("BMC") is initialized, the BIOS POST Watchdog is enabled. As this feature is hard-wired within the BMC (selected mainboards only!), it cannot be disabled by the user. **1**
  The timeout is fixed to 120 sec by the BMC firmware.
  Note: The BIOS POST watchdog may improve the system startup under critical environmental conditions like temperatures below 0℃.
  If the system doesn´t perform the BIOS POST within 120 sec, the BIOS POST Watchdog restarts the system until it runs BIOS POST (POST = PowerOnSelfTest).

- After the BIOS POST is passed, the BIOS checks the "BIOS Boot Watchdog" setting in BIOS Setup. This can be disabled (timeout set to 0) or enabled (timeout set to 1…255 minutes). Dependent on this setting, the Watchdog is switched off or re-initialized according to the selected timeout. **2**
  If the system fails to boot within the selected timeout, the Watchdog will restart the system.

- **3** The OS has been started. If the OS Boot Watchdog is enabled (timeout set to 1…255 minutes in BIOS Setup) it must be switched off now or retriggered continuously (= OS Watchdog) by a specific OS application (=WD software agent), otherwise the system will be reset after the timeout.

How to handle the different watchdog levels

- BIOS POST Watchdog
  - Ø   No user interaction possible – POST Watchdog is always enabled!

- BIOS Boot Watchdog
  - Ø   Set Watchdog in BIOS Setup
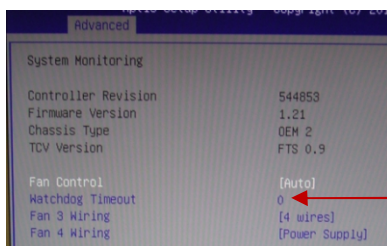
0 = WD disabled
1 – 255 = WD enabled (timeout = 1 – 255 minutes)

■ OS Watchdog

Ø   Use "Watchdog software agent" to stop or retrigger the Watchdog during OS runtime
     Note: This "agent" needs to be provided by the customer, dependent on his needs.
     For easy access to the watchdog functions, the Windows API (BMCAPI) or the related Linux driver (lm-sensors) can be used:
     e.g. ftp://ftp.ts.fujitsu.com/pub/Mainboard-OEM-Sales/Products/Mainboards/Industrial&ExtendedLifetime/D3071-S_D3076-S/IndustrialTools_D307x-S/

Ø   For easy testing, the SystemGuard tool provides access to the OS Watchdog. After enabling the Watchdog, SystemGuard retriggers the Watchdog continuously. In case the system freezes, SystemGuard does no longer provide the retrigger signal and the Watchdog resets the system after the timeout.
     Note: When SystemGuard is closed, the Watchdog is stopped in order to avoid an unwanted system reset!
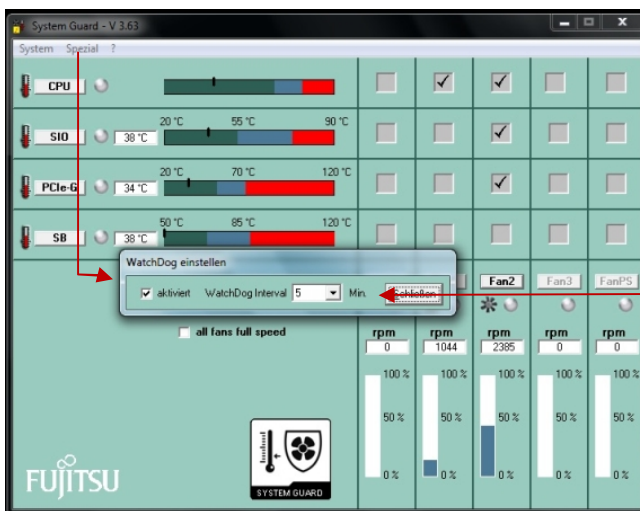
Menu "Special":
   --> Enable Watchdog
   --> Set timeout to 1 – 8 minutes

Link to latest SystemGuard software: ftp://ftp.ts.fujitsu.com/pub/Mainboard-OEM-Sales/Services/Software&Tools/Common-Mainboard-Tools/SystemGuard/

Supported Mainboards

Mainboard	BIOS POST Watchdog	BIOS Boot Watchdog	OS Watchdog
D3162-A/B	--	--	X
D3128-B	X	X	X
D3076-S	X	X	X
D3071-S	X	X	X
D3062-A/B	--	--	X
D3003-S	--	X	X
D2963-S	--	--	X
D2836-S	--	--	X
D2831-S	--	--	X
D2778-D	--	--	X
D2703-S	--	--	X

Contact

FUJITSU Technology Solutions
Mainboard OEM Sales
E-mail: OEM-Sales@ts.fujitsu.com
www.fujitsu.com/fts/products/computing/pc/accessories/mainboards/
ftp://ftp.ts.fujitsu.com/pub/Mainboard-OEM-Sales

2012-04-12 CE EN