

High Availability MonitorTM
Product Brief



High Availability Monitor Product Brief

Introduction 4

Features 5

- Detects Windows Bug Check and Linux Panic Conditions..... 5
- Operates Without OS Support 5
- Triggers Automatic Upgrades for the Platform Update Facility..... 5
- Email Notifications Automatically Sent When Problems Arise 5
- Remote Management Via Telnet and HTTP 5
- Set of Two ~70KB Firmware Application Executables, Compresses to ~70KB in ROM
 (Combined)..... 5
- OEM-Configurable in System Registry..... 5

Applications..... 6

Sample Configuration..... 6

Introduction

High Availability Monitor (HA Monitor) is a firmware application that continuously monitors the foreground operating system and application, verifying that it has not crashed. When crashes such as Blue-Screens or Black Screens or Panics occur, the HA Monitor generates an OS System Death HA event, which can be configured by the ODM/OEM to perform specific functions, including logging the failure to a system event log, sending an email alert over the network, triggering the Platform Update Facility to reload known-working software and firmware, and rebooting the target.

To accomplish this, the HA Monitor uses the Firmware® Technology's HA infrastructure, becoming a key producer of HA information as it scans the health of the foreground operating system, and a consumer of the resulting actions broadcast by the Firmware® kernel's HA subsystem according to the policies set forth by the ODM/OEM.

Fine-tuned, proprietary techniques are used to detect OS System Death in Windows systems, for those systems running Windows 98, Windows NT, Windows XP, or Windows XP Embedded. Common failures, such as Blue-Screen or Black-Screen conditions, are detected, along with other more general conditions, such as when interrupts are pending but are not being serviced within the tolerances specified by the ODM/OEM.

The HA Monitor can be remotely managed over the local network or Internet with any web browser or Telnet connection. Standard Firmware® Technology TCB user-level security is provided on remote administration.

Common applications include limiting down time to quantifiable levels (i.e., five 9's, six 9's, etc.) and ensuring users never witness an internal OS failure on visible monitors.

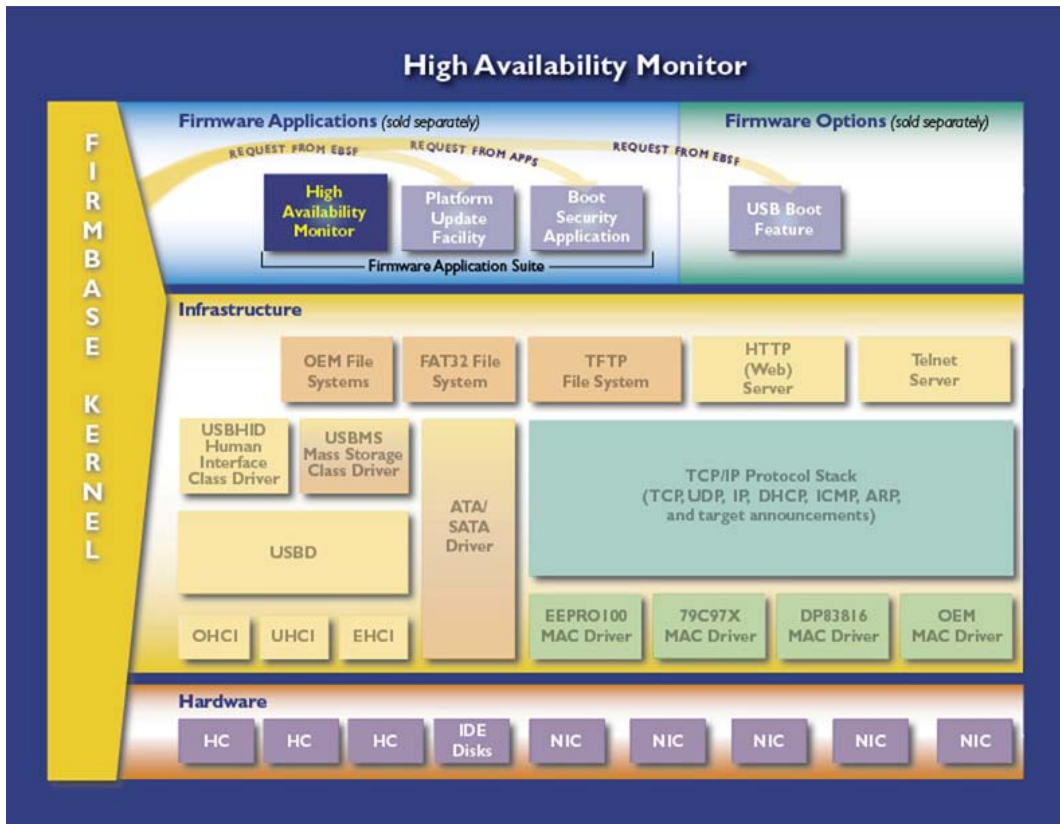


Figure 1. System Component View

Features

Detects Windows Bug Check and Linux Panic Conditions

HA Monitor supports detection of the Windows Bug Check condition on Windows NT and Windows XP, including single processor and multiprocessor kernels. For Linux systems, kernel panics are automatically detected in kernels 2.4 and 2.6.

Operates Without OS Support

As with all firmware applications that employ Firmware® Technology, the HA Monitor does not require any OS to perform its functions; it does not operate within the foreground OS framework. Instead, it can detect OS failures early during OS load and initialization, and operates independently of the OS memory model, I/O model, or scheduling model.

The ability to detect OS boot failures is something that no other technology can provide.

Triggers Automatic Upgrades for the Platform Update Facility

When OS System Death is detected by the HA Monitor, it may be configured to trigger the Platform Update Facility, allowing system objects to be checked for integrity or simply replaced, as defined by ODM/OEM-specified policies.

Email Notifications Automatically Sent When Problems Arise

When OS System Death is detected by the HA Monitor, it may be configured to automatically send email via the industry-standard SMTP protocol to a mail server before rebooting or taking other action. This enables IT personnel to become aware of problems as they arise in the field so that timely action can be taken to service the unit.

Remote Management Via Telnet and HTTP

The HA Monitor allows both telnet and web clients to remotely manage the system, including the log, as well as viewing the health of system objects such as the GDT, IDT, OS processes, and the HA Monitor log, provided that the OEM has configured the TCP/IP stack in the system and the network interface is not already in use by the foreground operating system. In the case of a shared network interface, Firmware Technology can be configured by the OEM to automatically take-over the network interface on HA events such as OS system death.

Set of Two ~70KB Firmware Application Executables, Compresses to ~70KB in ROM (Combined)

Typically merged as compressed resources in the BIOS Flash ROM, HA Monitor components include the main utility (HAMON.EXE) as well as the OS Monitor (OSMON.EXE). The size of these components (roughly 70KB each) allows them to fit easily on a system BIOS ROM, either compressed or uncompressed. The application can also be loaded from FAT32 volumes residing on ATA or USB mass storage devices.

OEM-Configurable in System Registry

The HA Monitor is configurable in the system registry in two sections. The [HA] section contains the system-wide ODM/OEM HA policies that govern what HA events map to actions on specific devices. This section defines connections between producers and consumers of HA information in the system. The [HAMONITOR] section configures the HA Monitor application, defining thresholds and methods for detection of OS System Death in the system.

The rule-based nature of the HA Monitor configuration is simple and straightforward, yet allows ODMs and OEMs the ability to control policy to an exacting degree.

Applications

Ensuring that devices do not stall in an OS System Death condition is the major application for the HA Monitor. It raises the availability of the device, reduces down time in the field, and is an integral part of the total self-repairing system enabled by the Platform Update Facility.

Sample Configuration

The HA Monitor is configurable in two sections in the system registry; namely, the [HA] section, containing the system's HA policies; and the [HAMONITOR] section, containing the policies associated with OS System Death detection. The following is an excerpt of a REGISTRY.SYS file containing these sections.

```
[HA]
/dev/console.detect.ostakeover = announce
/dev/console.listen.ostakeover = resume
/dev/console.listen.osdeath = resume

/dev/hamonitor.detect.osdeath = announce
/dev/hamonitor.listen.osdeath = resume

[HAMONITOR]
MaximumInterruptLatency = 1000      # maximum interrupt latency in ms.
AuditLog = /dev/hd0/hamon.txt      # log for writing failure events.
```



Embedded Products

915 118th Ave. SE, Suite 320, Bellevue, WA 98005, 800-850-5755, 425-576-8300
www.phoenix.com, embedded_sales@phoenix.com