Intel® Telco Alarms Manager 2.3

User's Guide

Revision 1.7

June 6, 2007

Telecom Server Division

Revision History

Date	Revision Number	Modifications
03/08/2005	1.4	Updates for TIGNC2U – Initial Revision
12/01/2005	1.5	Updates for TIGI2U
06/26/06	1.6	Updates for TIGW1U
06/06/07	1.7	Corrections added for Event Listener Agent

Disclaimers

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

The Telco Alarms Manager may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Table of Contents

List of Tables

1. Introduction

Telco Alarms Manager (TAM) is a set of telecom server software components designed to manage the alarms state of the server and indicate health status via the local Telco Alarm Panel (TAP) in the front of the server as well as remotely via dry contact relays in the rear of the server. The TAM Service is the primary service that runs and receives alarm requests from multiple entities, such as the TAM Event Listener, Intel® System Management Software (ISMS) (formerly Intel® Server Management, abbreviated as ISM), and other applications which have registered with TAM.

Additionally, the Telco Alarms Manager delivers several APIs that permit direct access to the TAP (Telco Alarms Panel). Application developers who wish to manage the alarms state from within their application can do so by using these APIs which bypass the TAM Service's management of the state machine.

2. Configuration Requirements

Supported Hardware:

- Intel® Telco/Industrial Grade Server TIGI2U
- Intel® Telco/Industrial Grade Server TIGW1U

Supported Operating Systems:

TIGW1U

- Red Hat* Enterprise Linux 4 (x86) Update 4
- Red Hat* Enterprise Linux 4 (x86_64) Update 4 0 EM64T
- SuSE Linux ES 9 IA32 – SP3
- SuSE Linux ES 9 EM64T – SP3
- Microsoft Windows* Server 2003 IA32
- Microsoft Windows* Server 2003 EM64T

TIGI2U

- Red Hat* Enterprise Linux 3
- Red Hat* Enterprise Linux 4
- SuSE Linux 9
- Microsoft Windows* Advanced Server 2003

Software Components:

- TAM Software – Packaged in Linux as tam-2.3-*x.*<*architecture*>.rpm and packaged in Windows as a Microsoft Installer file (.MSI), TAMSetup.msi. TAM Software is only beneficial for monitoring baseboard and operating system components if Firmware TAM is disabled)

- IPMI Driver – The IPMI driver is a requirement if TAM is installed. If TAM is installed from the platform's Deployment CD, the IPMI driver is installed automatically.*

- Server Management Software - Intel Server Manager 8.x (ISM) or Intel System Management Software (ISMS). This is a required component for the TIGI2U server platform and should be installed prior to installing TAM software. Server Management Software is optional software for the TIGW1U server platform.

3. Installation

TAM 2.3 is packaged on the platform's Deployment CD. If you are installing Server Management Software, It is recommended to install Server Management Software prior to installing TAM. Please see prior section 2 – Software Components for more information.

To run installation directly from CD:

Installation can be started from the "Welcome" page that automatically starts when the CD is mounted or inserted. From the welcome page, select the target operating system under the "Software & Drivers" or "Drivers and Utilities" tab. Select the Telco Alarms Manager installation.

* This is true for the Windows operation system only.

4. Telco Alarms Manager Event Agents

4.1 Overview

TAM is designed to work with software or modules that register with TAM. This registered software is referred to as event agents. These event agents relay information to TAM so that any problems that occur on a system are indicated by the LEDs on the alarm panel. A set of TAM event agents is delivered as part of the TAM software package which are described in the following sections.

4.2 Event Listener Agent

The Event Listener Agent is a service or daemon that runs if Firmware TAM is disabled. This agent monitors events recorded in the server's SEL (System Event Log). The event listener agent was introduced with the TIGW1U server and wasn't available for TIGI2U. TIGI2U depends on the EMS Event Agent described in the following section, 4.3.

4.3 EMS Event Agent

ISM's and ISMS's EMS (Event Management System) Event Agent is installed by TAM. EMS is the event management architecture for ISM versions 8.x and higher and ISMS 1.x and higher. EMS monitors and provides information on several baseboard, hardware, and OS components. Any exceeded thresholds or alerts that it receives are mapped and forwarded to TAM, which illuminates corresponding status LEDs on the alarm panel. The following is a summary of some of the hardware components monitored by the EMS. Please refer to ISM documentation for more detailed information.

- Fan (failure, speed)
- Memory (single and multi-bit errors, ECC errors)
- Processor (thermal trips, internal errors, and caches)
- Temperature (baseboard and processor temperature)
- Voltage (standby, baseboard, and processors)
- Power supplies (presence, redundancy, and temperature)
- Network (network configuration and connection information)
- Storage (hard disk drives, CD-ROM drives, and RAID devices)
- Chassis (intrusion)

4.4 SNMP Event Agent

The SNMP Event Agent listens for configured SNMP (Simple Network Management Protocol) traps. Any traps that the local server receives can be mapped in configuration file and forwarded to TAM which illuminates corresponding status LEDs on the alarm panel. The SNMP Event Agent is delivered as a component TAM.

5. Modes, Models, and Mapping

5.1 TAM Modes

TAM supports three different modes to send alarm data to the alarm panel: software-based, firmware-based, and OEM-managed. In the software-based mode, alarm processing is managed via software TAM API calls. TAM Software uses the software-based mode since it makes calls to TAM APIs. Please refer to the Telco Alarms Manager 2.x External Product Specification for TAM API information. In the firmware-based mode, alarm processing is managed via the BMC (Baseboard Management Controller), and in the OEM-managed mode, alarm processing and management is accomplished by making TAP API calls. Please refer to the Telco Alarms Manager 2.x External Product Specification for TAP API information.

Table 1 lists the modes and platforms that are supported or unsupported.

Table 1. Intel® Telco Alarms Manager 2.1 Modes

Hardware Platform	Mode		
	Software-based	Firmware-based	OEM-Managed
Intel® Telco/Industrial Grade Server TIGI2U	Supported	Supported	Supported
Intel® Telco/Industrial Grade Server TIGW1U	Supported	Supported*	Supported*

5.2 Alarm Models

TAM supports two models, “Most Severe” and “All Severities”. If TAM is running in firmware-based mode the alarm model can be changed by flashing the system’s SDRs (Sensor Data Records). Please refer to the BMC TAM EPS for SDR information. If TAM is running in software-based mode, the alarm model can be configured by modifying the `tamconfig` file and setting ALL_SEVERITIES_MODEL to yes or no. TAM must be restarted in order for this change to take effect.

Linux: `/usr/local/tam/tamconfig`

Windows: `<TAMTargetDirectory>\tamconfig.dat`

* This platform has a mBMC on the baseboard. This feature is only supported if a Management Module is added to the server. The Management module has a Sahallee BMC which allows this feature to work.

- **Most Severe Alarm Model** – Only the most critical alarm LED is illuminated. For example, if a minor alarm is present and a major alarm occurs, the minor alarm data will be retained in the alarm database; only the major alarm LED will be illuminated. If the condition that set the minor alarm previously still exists when the major alarm is cleared, the minor alarm will once again become illuminated. The “Most Severe” model is the default alarm model.

- **All Severities Alarm Model** – All alarm LEDs for which alarm data exist will illuminate. This behavior facilitates the illumination of multiple LEDs simultaneously.

5.3 Alarm Severities

Severity modifications are dependent upon the Event Agent’s configuration. The Event Agents analyze events from the hardware and software applications, and map the sensor severity to a Telco Alarm severity. The Event Agents then make calls to the TAM with the alarm information for alarm table entry and LED illumination. Table 1 lists descriptions for each alarm panel LED. Table 2 lists how the ISM, ISMS, and SNMP Event Agents’ severities map to TAM LED severities.

Table 2. TAM LED Descriptions

TAM Alarm Panel LEDs	Description
MINOR (MNR)	A non-service-affecting condition. Corrective action should be taken in order to prevent a more serious fault.
MAJOR (MJR)	A service-affecting condition that requires an urgent action.
CRITICAL (CRT)	A service-affecting condition that requires an immediate action.
POWER (PWR)	Only active for power or voltage events.
DISK (DSK)	Activated during disk activity.
(NIC)	Activated during network activity.
(ON)	Activated when system is powered on. Not activated when system is powered off.

Table 3. Event Agent Severity Mapping

TAM Alarm Panel LEDs	ISM Event Agent	ISMS Event Agent	Event Listener Agent	SNMP Event Agent
MINOR (MNR)	non-critical	Warning	Non-critical	Configured in SNMP Event Agent configuration file.
MAJOR (MJR)	Critical	Critical	Critical	
CRITICAL (CRT)	Non-recoverable			
POWER (PWR)	Set for alarms related to power or voltage			
DISK (DSK)				
(NIC)				
(ON)				

6. Configuration

6.1 Server Management Integration

ISM 8.x and ISMS 1.x leverage LANDesk which is a Java-based application used to monitor baseboard, system, and OS events on servers. When TAM is installed after ISM, TAM event agents are installed that integrate with the ISM EMS. This allows events from ISM to automatically be mapped to the server's alarm panel LEDs.

In order to receive critical, major, or minor LED alerts for baseboard and system events, no user action is required as long as

- TAM (firmware mode) was enabled when prompted during the server's SDR flash program. Firmware Mode is the default TAM mode.

  or

- If TAM (firmware mode) was disabled when prompted during the server's SDR flash program, the IPMI driver, TAM Software, and if the platform is TIGI2U - ISM/ISMS need to be installed.

6.2 SNMP Trap forwarding to TAM

TAM installs a snmplistener service and a configuration file. This service and configuration file work together to filter and map SNMP traps to the alarm panel LEDs. Please refer to the following sections to setup filtering and mapping for SNMP trap messages to the Telco Alarm Panel LEDs.

Linux: /usr/local/tam/etc/trap2tam.conf

Windows: `<TAMTargetDirectory>\`snmptraplistener.ini.

The service, "SNMP Trap Listener Service" parses this file whenever a trap message is received from the local server. If the trap is configured in the trap2tam configuration file, the severity is translated according to the configuration file, the event gets added to the alarms manager database, and the appropriate TAM LED is activated.

6.2.1 Linux SNMP Trap Forwarding Configuration

Linux leverages the snmptrapd daemon to filter traps. Please refer to the man page for snmptrad for complete configuration information. The following line must exist in /etc/snmp/snmptrapd.conf in order to forward traps to TAM:

`traphandle <TRAPOID> /usr/local/tam/etc/trap2tam`Example:

```
traphandle  UCD-SNMP-MIB::ucdExperimental.990.0.17 /usr/local/tam/etc/trap2tam
```

The trap2tam binary reads /usr/local/tam/etc/trap2tam.conf in order to map severities from the SNMP severity to a TAM severity. Once a severity is mapped for an event, the TAM APIs are called to enable the appropriate TAM LED. Please refer to Appendix B in this document for information on configuring trap2tam.conf.

6.2.2 Windows SNMP Trap Forwarding Configuration

TAM installs the "SNMP Trap Listener Service" which listens, filters, and maps traps to the TAM severities. The only configuration required is setting up the configuration file snmptraplistener.ini. Please refer to Appendix B in this document for a preview and instructions of the snmptraplistener.ini file.

6.2.3 TAMTEST – Telco Alarm Manager Debug Utility

When TAM is installed, a tool is installed to help with monitoring and testing alarm records stored in the alarm manager database.

Linux: `/usr/local/tam/bin/tamtest`

Windows: `<TAMTargetDirectory>\tamtest.exe`

Running this tool without parameters will display the help menu below which describes the tools capabilities:

```
Usage: tamtest <-cmd> <args>

<cmd> is defined as follows

-g <appKeyString> <appDescription> <clearFlag> . Get generator ID

-a <genInfo> <alarmId> <severity>  . . . . . . . Add TAM record

-r <genInfo> <alarmId> . . . . . . . . . . . . . Remove TAM record

-p . . . . . . . . . . . . . . . . . . . . . . . Get panel state

-q <genInfo> <alarmId>   . . . . . . . . . . . . Query for specific alarm(s

-d <dumpFileName>  . . . . . . . . . . . . . . . Dump alarms to file

-c . . . . . . . . . . . . . . . . . . . . . . . Get BMC TAM Config Info

-s . . . . . . . . . . . . . . . . . . . . . . . Get BMC TAM Status Info
```

Appendix A: Glossary

This appendix contains important terms used in the preceding chapters.

Acronym	Definition
API	Application Programming Interface
BMC	Baseboard Management Controller
ECC	Error Checking Correction
EMS	Event Management System
IPMI	Intelligent Platform Management Interface
ISM	Intel® Server Management
ISMS	Intel® System Management Software
LED	Light Emitting Diode
LRA	Local Response Agent
mBMC	Mini-BMC
OSD	On-Screen Display
PDU	Protocol Data Units
RAID	Redundant Array of Inexpensive Disks
SDR	Sensor Data Record
SNMP	Simple Network Management Protocol
TAM	Telco Alarms Manager
TAP	Telco Alarm Panel

Appendix B: snmptraplistener.ini & trap2tam.conf

' The purpose of this configuration file is to filter snmptraps and map the snmptrap severity to the
' major, minor, and critical severities of the Telco Alarm Manager states. This SNMP mapping
' only functions correctly if the trap sends or represents a severity and if the trap sends a clearing
' (ok status) trap or trap variable. Please refer to the syntax and example below.
'
' [EVENT _ID]: Enter an event identification number for the trap in the brackets. This number
' should be between 0 and 254.
'
' OID: Enter the trapoid as a value for the OID key.
'
' SevType: If the severity for the trap is reported in a trap variable, enter "variable-based"
' for the value of the SevType key. The EVENT_ID for this trap should never be
' repeated.
' If the severity for the trap is reflected by the trap itself, enter "trap-based" for
' the value of the SevType key. The EVENT_ID for this trap should match other
' traps that are associated to this trap event.
'
' ClearFlag: If this event should remain in the Telco Alarm Manager database after rebooting
' the server, enter "false" as the value for the ClearFlag key; otherwise enter "true"
'
' SevVar: If SevType is set to "variable-based", enter the variable number that reports the
' severity. For example, if it is the first variable, enter "0" as the SevVar value. If
' SevType is set to "trap-based", leave this value blank.
'
' OK: If SevType is set to "trap-based" and this is a clearing trap, enter "true" as the

```
'                   value; otherwise, enter false.  If SevType is set to "variable-based" enter the
'                   string (or strings seperated by commas) that clears this event.
'
' Minor:            If SevType is set to "trap-based" and this is a minor severity trap, enter "true" as the
'                   value; otherwise, enter false.  If SevType is set to "variable-based" enter the
'                   string (or strings seperated by commas) that makes this event a minor event.
'
' Major:            If SevType is set to "trap-based" and this is a major severity trap, enter "true" as the
'                   value; otherwise, enter false.  If SevType is set to "variable-based" enter the
'                   string (or strings seperated by commas) that makes this event a major event.
'
' Critical:         If SevType is set to "trap-based" and this is a critical severity trap, enter "true" as the
'                   value; otherwise, enter false.  If SevType is set to "variable-based" enter the
'                   string (or strings seperated by commas) that makes this event a critical event.
'
' Example Configuration:
[10]
oid =1.3.6.1.4.1.2021.13.990
sevtype = variable-based
clearflag = true
sevvar = 0
ok = 0,1
minor = 2,3
major = 4,5
critical = 6,7
'
' [11]
' oid = 1.3.6.1.4.1.2021.13.990.17
```

' sevtype = trap-based

' clearflag = true

' sevvar =

' ok = true

' minor = false

' major = false

' critical = false

'

' [11]

' oid = 1.3.6.1.4.1.2021.13.990.18

' sevtype = trap-based

' clearflag = true

' sevvar =

' ok = false

' minor = false

' major = true

' critical = false