



SCS Engineering Release Notice

GCA Release Version 06.00.00.00 - SAS3FW_MASTER_DEV (SCGCQ00747307)

(SCGCQ00747307) - GCA Release Version 06.00.00.00 - SAS3FW MASTER DEV

(SCGCQ00736763) - Phase6 Beta Release Version 05.250.06.00 - SAS3FW MASTER DEV

(SCGCQ00733127) - Phase6 Beta Release Version 05.250.05.00 - SAS3FW MASTER DEV

(SCGCQ00729508) - Phase6 Alpha Release Version 05.250.04.00 - SAS3FW MASTER DEV

(SCGCQ00717285) - Phase6 Alpha Release Version 05.250.03.00 - SAS3FW MASTER DEV

(SCGCQ00710448) - Phase6 Pre-Alpha Release Version 05.250.02.00 - SAS3FW MASTER DEV

(SCGCQ00698933) - Phase6 Pre-Alpha Release Version 05.250.01.00 - SAS3FW MASTER DEV



SCS Engineering Release Notice

GCA Release Version 06.00.00.00 - SAS3FW_MASTER_DEV (SCGCQ00747307)

Defects=0, Enhancements=0 (Version Change Only)



SCS Engineering Release Notice

Phase6 Beta Release Version 05.250.06.00 - SAS3FW_MASTER_DEV (SCGCQ00736763)

Change Summary (Defects=2)

SCGCQ00734454 (DFCT) - NVDATA: The number of GPIO in Mfg Page 6 is incorrect

SCGCQ00735541 (DFCT) - IOP: Config space read during startup can cause firmware lockup



SCS Engineering Release Notice

Phase6 Beta Release Version 05.250.06.00 - SAS3FW_MASTER_DEV (SCGCQ00736763)

Total Defects Resolved (2)

| (SCGCQ00734454) | Defect 1/2 |
|-----------------|------------|
|-----------------|------------|

| | |
|------------------------|---|
| HEADLINE: | NVDATA: The number of GPIO in Mfg Page 6 is incorrect |
| DESC OF CHANGE: | Corrected the number of GPIO in Mfg Page 6. |
| TO REPRODUCE: | Read Mfg Page 6. |
| ISSUE DESC: | The number of GPIO in Mfg Page 6 is incorrect |

| (SCGCQ00735541) | Defect 2/2 |
|-----------------|------------|
|-----------------|------------|

| | |
|------------------------|---|
| HEADLINE: | IOP: Config space read during startup can cause firmware lockup |
| DESC OF CHANGE: | Changed code to not enable critical interrupts until after firmware enables the config space registers. |
| TO REPRODUCE: | The host should boot the system and release the controller from reset. Within about 600ms, the host should attempt to read the MSIx register (offset 0xC0) repeatedly. Firmware will lock up and the heartbeat LED will stop. |
| ISSUE DESC: | If the host reads certain config space registers before firmware has been able to enable the config registers, firmware may get into an infinite loop and the controller will become unresponsive. |

Change Summary (Defects=24 Enhancements=1)

SCGCQ00676043 (DFCT) - PL: SR-IOV IOs can trigger fault 0x2667 when FastPath is disabled to a drive in firmware

SCGCQ00702670 (DFCT) - IOP: Mfg Page 6 maximum number of GPIOs definition is incorrect

SCGCQ00728016 (DFCT) - PL: Fix minor code issues found by analysis tool

SCGCQ00728091 (DFCT) - PL: Uninitialized variable being used in PL SATL Function

SCGCQ00728104 (DFCT) - IOP: ISTWI fails to initialize variable and out of bounds array access

SCGCQ00728152 (DFCT) - IOP: Diag Buffer Post request message with invalid BufferType field can cause unpredictable results

SCGCQ00728155 (DFCT) - IOP: Firmware download of complete flash could access invalid array index

SCGCQ00728677 (DFCT) - IOP: Memory move operation could access uninitialized variables

SCGCQ00728865 (DFCT) - PL: Firmware could be accessing out-of-bound array elements handling SGPIO bays

SCGCQ00728893 (DFCT) - IOP: TLB initialization may fail to identify the running memory model

SCGCQ00728894 (DFCT) - PL: Firmware could be using uninitialized pointers in SGPIO error cases

SCGCQ00728908 (DFCT) - IOP: Minor CLI defects

SCGCQ00729597 (DFCT) - PL: SAS Topology Change List Event could send indeterminate

ExpanderStatus

SCGCQ00729603 (DFCT) - Fix Task Management coding error

SCGCQ00729619 (DFCT) - IOP: Performance monitor CLI command could cause invalid array access

SCGCQ00729630 (DFCT) - Fix a coding error in clean up code.

SCGCQ00730628 (DFCT) - IOP: Incorrect MaxChainDepth in IOC Facts response with disabled local chain

HW

SCGCQ00730692 (DFCT) - IOP: Config page code null references and uninitialized variable fixes

SCGCQ00730721 (DFCT) - PL: Firmware could be accessing null pointer in port layer interrupt handler.

SCGCQ00730743 (DFCT) - PL: A diagnostic command was using the wrong size for register prints

SCGCQ00731021 (DFCT) - SAS3IR: controller is hitting 0x265d fault while creating volume when there is an inactive volume

SCGCQ00731572 (DFCT) - PL: Diagnostic CLI task management code has unreachable code

SCGCQ00731657 (DFCT) - IOP: Config page code writes uninitialized value to internal structure

SCGCQ00731663 (DFCT) - PL: Transport Layer Retry code was using a wrong value for a comparison

SCGCQ00729511 (CSET) - Replace LastHeadWrite with FLUSH_WRITE

Total Defects Resolved (24)**(SCGCQ00676043)** Defect 1/24

HEADLINE: PL: SR-IOV IOs can trigger fault 0x2667 when FastPath is disabled to a drive in firmware

DESC OF CHANGE: Added code to insert the correct virtual function number into the IO request message when firmware receives the IO from the fast path exception queue. This ensures firmware code will use the correct virtual function for future operations.

TO REPRODUCE: 1) On a SR-IOV enabled host, create and start 16 VMs and assign drives for the VMs.
2) Disable Fast Path in firmware for one of the drives visible to a VM using the UART command.
3) In the Virtual Machine, perform read IO on the fast path disabled device. ie : dd if=/dev/sdb of=/dev/null.
4) Fault 2667 is hit.

ISSUE DESC: If firmware disables FastPath for a drive and IOs are sent to it from a virtual function, firmware may fault with code 0x2667.

(SCGCQ00702670) Defect 2/24

HEADLINE: IOP: Mfg Page 6 maximum number of GPIOs definition is incorrect

DESC OF CHANGE: Modified the value of IOPIMAXES_PAGE6_GPIO_DEFS to be accurate for Invader and also accounted for the Virtual GPIOs that provide controls for Serial GPIO (SIO) Data In (DIN) and Data Out (DOUT) pins 0 and 1.

TO REPRODUCE: Visual inspection of the code.

ISSUE DESC: The value of IOPIMAXES_PAGE6_GPIO_DEFS was set for Meteor and not Invader, and Meteor has a different number of GPIOs.

(SCGCQ00728016) Defect 3/24

HEADLINE: PL: Fix minor code issues found by analysis tool

DESC OF CHANGE: Add new faults for these possible but unlikely conditions.

TO REPRODUCE: none

ISSUE DESC: Fix minor code issues found by analysis tool.

(SCGCQ00728091) Defect 4/24

HEADLINE: PL: Uninitialized variable being used in PL SATL Function

DESC OF CHANGE: Initialized the variable at function start.

TO REPRODUCE: N/A

ISSUE DESC: There was a variable in a PL SATL function that could have been used before it was initialized.

(SCGCQ00728104) Defect 5/24

HEADLINE: IOP: ISTWI fails to initialize variable and out of bounds array access

DESC OF CHANGE: Restructured the error paths to avoid using the uninitialized variable and prevent out of bounds array access.

TO REPRODUCE: Send an MPI ISTWI Toolbox request where the DevIndex field into Manufacturing Page 8's ISTWI Device Info array contains an invalid Bus Number.

ISSUE DESC: There are several error handling paths that could cause an uninitialized variable to be used, or a variable to access beyond the bounds of an internal array.

(SCGCQ00728152) Defect 6/24

HEADLINE: IOP: Diag Buffer Post request message with invalid BufferType field can cause unpredictable results

DESC OF CHANGE: Added a condition to ensure the array is accessed only when the index variable is initialized.

TO REPRODUCE: Issue a Diag Buffer Post message with an invalid BufferType field.

ISSUE DESC: During code inspection, a problem was found in firmware where an array was indexed using a variable firmware only populates when BufferType is valid. This could cause firmware to perform unexpected actions.



SCS Engineering Release Notice

Phase6 Beta Release Version 05.250.05.00 - SAS3FW_MASTER_DEV (SCGCQ00733127)

(SCGCQ00728155) Defect 7/24

HEADLINE: IOP: Firmware download of complete flash could access invalid array index
DESC OF CHANGE: Added a check to avoid the path to the incorrect array index.
TO REPRODUCE: Download a complete flash image which is the wrong size for the flash part.
ISSUE DESC: If a firmware download request for the complete flash is sent with a image size which does not match the flash part, firmware could attempt to index an array with an out of bounds index. This could cause unpredictable behavior.

(SCGCQ00728677) Defect 8/24

HEADLINE: IOP: Memory move operation could access uninitialized variables
DESC OF CHANGE: Added checks to ensure firmware does not access uninitialized variables.
TO REPRODUCE: Found during code inspection.
ISSUE DESC: There are cases where a SGL based memory move operation could cause firmware to access uninitialized variables.

(SCGCQ00728865) Defect 9/24

HEADLINE: PL: Firmware could be accessing out-of-bound array elements handling SGPIO bays
DESC OF CHANGE: Added a condition to avoid an out-of-bound array access with an unsupported PHY number.
TO REPRODUCE: Attempt to get the bay number for a specific PHY that is larger than the supported number of PHYs.
ISSUE DESC: It is possible for a larger number of PHYs than supported to cause an out-of-bound array access when handling SGPIO bays.

(SCGCQ00728893) Defect 10/24

HEADLINE: IOP: TLB initialization may fail to identify the running memory model
DESC OF CHANGE: Added code to identify this situation and fault.
TO REPRODUCE: Found in code inspection.
ISSUE DESC: During code inspection, it was found firmware could fail to accurately identify the running memory model in an extreme corner case. This could cause unpredictable failures.

(SCGCQ00728894) Defect 11/24

HEADLINE: PL: Firmware could be using uninitialized pointers in SGPIO error cases
DESC OF CHANGE: Modified the code that could use uninitialized pointers to account for this and to always reference valid memory.
TO REPRODUCE: Send a malformed SMP GPIO Read or Write for PL to execute.
ISSUE DESC: There are pointers used when processing SGPIO related tasks, and those pointers may be used uninitialized in some error cases.

(SCGCQ00728908) Defect 12/24

HEADLINE: IOP: Minor CLI defects
DESC OF CHANGE: Added minor changes to correct these issues.
TO REPRODUCE: Found using code analysis.
ISSUE DESC: Code analysis found a few small issues in the IOP CLI code. TLB dumps may incorrectly display the user privilege flags. TFTP transfer code missed corner cases, which are not possible in current code, which could result in dereferencing NULL pointers. TFTP error outputs may display extra information in certain cases.

(SCGCQ00729597) Defect 13/24

HEADLINE: PL: SAS Topology Change List Event could send indeterminate ExpanderStatus
DESC OF CHANGE: Removed code path which could cause an invalid value to be sent in the ExpanderStatus field.
TO REPRODUCE: Found during code inspection. It is not believed this has ever happened.



SCS Engineering Release Notice

Phase6 Beta Release Version 05.250.05.00 - SAS3FW_MASTER_DEV (SCGCQ00733127)

ISSUE DESC: A corner case exists where firmware could send an indeterminate value in the ExpanderStatus field of a SAS Topology Change List Event.

(SCGCQ00729603) Defect 14/24

HEADLINE: Fix Task Management coding error
DESC OF CHANGE: Fix logic error to reflect the original intention.
TO REPRODUCE: None
ISSUE DESC: A logic error is found in task management code that could cause unforeseen error/fault.

(SCGCQ00729619) Defect 15/24

HEADLINE: IOP: Performance monitor CLI command could cause invalid array access
DESC OF CHANGE: Corrected the parameter validation code to ensure the entered values are correct.
TO REPRODUCE: In the CLI, call iop perf addl2 with the second parameter = 2. This will cause firmware to access an invalid index in an array.
ISSUE DESC: When adding a counter to the PLB performance monitor, the user could enter an invalid parameter and the code will not catch the error. This could cause accessing an invalid array index.

(SCGCQ00729630) Defect 16/24

HEADLINE: Fix a coding error in clean up code.
DESC OF CHANGE: Fix a coding error in clean up code that may cause unpredictable errors.
TO REPRODUCE: None
ISSUE DESC: Fix a coding error in clean up code that may cause unpredictable errors.

(SCGCQ00730628) Defect 17/24

HEADLINE: IOP: Incorrect MaxChainDepth in IOC Facts response with disabled local chain HW
DESC OF CHANGE: Fixed the code that populates the MaxChainDepth for B0 chip revisions.
TO REPRODUCE: Send an IOC Facts request to a B0 chip revision.
ISSUE DESC: The MaxChainDepth in an IOC Facts response is incorrect when the local chain hardware is disabled (i.e. a B0 revision).

(SCGCQ00730692) Defect 18/24

HEADLINE: IOP: Config page code null references and uninitialized variable fixes
DESC OF CHANGE: Added checks to ensure null variables are not dereferenced. Also added code to initialize variables.
TO REPRODUCE: Found during code inspection.
ISSUE DESC: There are some locations where code may access null pointers and/or use uninitialized variables.

(SCGCQ00730721) Defect 19/24

HEADLINE: PL: Firmware could be accessing null pointer in port layer interrupt handler.
DESC OF CHANGE: Added a check to prevent accessing the possible null pointer.
TO REPRODUCE: N/A
ISSUE DESC: Port layer interrupt handling code has a coding error that could lead to firmware accessing a null pointer.

(SCGCQ00730743) Defect 20/24

HEADLINE: PL: A diagnostic command was using the wrong size for register prints
DESC OF CHANGE: Corrected the error with the register size.
TO REPRODUCE: N/A
ISSUE DESC: Diagnostic code which is used to dump register values was using the wrong size for one of the registers.



SCS Engineering Release Notice

Phase6 Beta Release Version 05.250.05.00 - SAS3FW_MASTER_DEV (SCGCQ00733127)

(SCGCQ00731021) Defect 21/24

HEADLINE: SAS3IR: controller is hitting 0x265d fault while creating volume when there is an inactive volume
DESC OF CHANGE: Made the change to return the page if it is an internal request.
TO REPRODUCE: Connect Inactive volume to the controller. Create any volume. while BGI is going on observe the Fault (0x265d).
ISSUE DESC: While creating volume IR issues volume created event to the host. Host sends inquiry command to the volume. While processing inquiry command IR requests internally for raid volume page . At this time RAID volume was being used and hence returns NULL. If data accessed from this page then 265d fault is hit.

(SCGCQ00731572) Defect 22/24

HEADLINE: PL: Diagnostic CLI task management code has unreachable code
DESC OF CHANGE: Removed unreachable code.
TO REPRODUCE: Found in code analysis.
ISSUE DESC: Code analysis revealed a chunk of dead code in a function used by the diagnostic CLI to issue task abort or query task task management requests. This code should be removed.

(SCGCQ00731657) Defect 23/24

HEADLINE: IOP: Config page code writes uninitialized value to internal structure
DESC OF CHANGE: Initialized the variable.
TO REPRODUCE: Found during code inspection. Issue a config page read command to retrieve the header for a PL owned configuration page.
ISSUE DESC: When requesting the page header for PL owned pages, firmware will write an uninitialized variable to an internal structure.

(SCGCQ00731663) Defect 24/24

HEADLINE: PL: Transport Layer Retry code was using a wrong value for a comparison
DESC OF CHANGE: Transport Layer Retry code is modified to use the proper type for comparison.
TO REPRODUCE: None.
ISSUE DESC: Transport Layer Retry code was using a wrong value for a comparison



SCS Engineering Release Notice

Phase6 Beta Release Version 05.250.05.00 - SAS3FW_MASTER_DEV (SCGCQ00733127)

Total Enhancements Implemented (1)

| (SCGCQ00729511 - Port of SCGCQ00726746) | | Enhancement 1/1 |
|---|---|-----------------|
| HEADLINE: | Replace LastHeadWrite with FLUSH_WRITE | |
| NEW FUNCTIONALITY: | Reading variables back to another variable in memory was a method used to ensure a write had gone through in HW before proceeding. However, the code has been around for a long time. These reads into another variable have been replaced with PL_FLUSH_WRITE calls, which is what we use elsewhere in PL. PL_FLUSH_WRITE is also a bit faster because it doesn't have to do the write to the other variable; it does a read only. | |



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.04.00 - SAS3FW_MASTER_DEV (SCGCQ00729508)

Change Summary (Defects=14)

SCGCQ00703423 (DFCT) - Verify (16) SCSI Command is Not Failed with Expected Response When Specified LBA Exceeds the Capacity of the Medium

SCGCQ00706063 (DFCT) - Incorrect VPD Data is Obtained for VPD Page 0xB0 and 0xB2 When Drive is Under Foreground Extended Self-Test

SCGCQ00710946 (DFCT) - During SATA Drive Format, Unsupported VPD Inquiry Command is Not Failed with Expected Response

SCGCQ00711813 (DFCT) - Additional sense:Invalid cmd opcode, when read cmd sent to SATA drive in standby mode

SCGCQ00711858 (DFCT) - Fault 1901 Seen When Running Unmap IO's During Task Aborts For a SATA Drive

SCGCQ00714125 (DFCT) - System gets Hung & reboot while running IO's along with diag reset on the Controller which has Active and Inactive volumes.

SCGCQ00715211 (DFCT) - PL Fault 0x6003 While Running Heavy IO and Injecting Expander Resets on Alternating SAS Domains

SCGCQ00715239 (DFCT) - PL Fault 0x5851 is seen when running Query Task

SCGCQ00715299 (DFCT) - DID_SOFT_ERRORS are seen when Hot plug is performed on the RAID1 volume along with IOs.

SCGCQ00715484 (DFCT) - SATL doesn't handle ATA Pass-through (16) properly when Extend bit is cleared

SCGCQ00728153 (DFCT) - IOP: DDR initialization may access invalid pointer

SCGCQ00728903 (DFCT) - Fury cards would fault with 58B4 on power up

SCGCQ00717105 (CSET) - PL: D205 fault when posting a host trace buffer during IO

SCGCQ00725110 (CSET) - sas9311-16i phase 5 nvdata error

Total Defects Resolved (14)

| (SCGCQ00703423) | | Defect 1/14 |
|-----------------|--|-------------|
| HEADLINE: | Verify (16) SCSI Command is Not Failed with Expected Response When Specified LBA Exceeds the Capacity of the Medium | |
| DESC OF CHANGE: | Modified global CDB mask for VERIFY (16) command to include bytes 2 and 3 of CDB also for considering LBA. | |
| TO REPRODUCE: | Connect a SATA Drive to SAS3 controller. Now execute a READ CAPACITY command to know the size of drive. Execute VERIFY (16) command with LBA value greater than 0xFFFFFFFFFFFF. | |
| ISSUE DESC: | When the Verify(16) command is executed with LBA=0xFFFFFFFFFFFF it fails with "Invalid Field in CDB" but it has to fail with "LBA Out of Range". In Verify (16) SCSI command, LOGICAL BLOCK ADDRESS field is 8 bytes of length starting from Byte 2 to Byte 9, the command fails with LBA Out of Range till LBA range 0xFFFFFFFFFFFF. After this range the command fails with "Invalid Field in CDB" which is incorrect. | |
| | | |
| (SCGCQ00706063) | | Defect 2/14 |
| HEADLINE: | Incorrect VPD Data is Obtained for VPD Page 0xB0 and 0xB2 When Drive is Under Foreground Extended Self-Test | |
| DESC OF CHANGE: | Moved the # define to a .h file. | |
| TO REPRODUCE: | Connect a SATA Drive to SAS3 controller. Now execute a SEND DIAGNOSTIC for Foreground extended self-test and verify that drive is under self test. Now execute all VPD request to SATA drive. Verify now that VPD data is incorrect for VPD page 0xb0 and 0xb2. The PAGE CODE and PAGE LENGTH are also incorrect. | |
| ISSUE DESC: | Setup: Avago Gen 3 HBA (Fury 8 Port) ----> SATA Drives A # define was defined in a source file instead of a .h file like it should have been. This was causing the define to show up as 0 in other source files, even though it was enabled. Ultimately, this lead to the issue of incorrect VPD page data being obtained for certain pages, while a drive was under self-test. | |
| | | |
| (SCGCQ00710946) | | Defect 3/14 |
| HEADLINE: | During SATA Drive Format, Unsupported VPD Inquiry Command is Not Failed with Expected Response | |
| DESC OF CHANGE: | ATA EPC feature supported check added to responding to ATA Commands during a format operation. | |
| TO REPRODUCE: | Setup:- HBA (Fury 8 Port) ----> SATA Drives Connect a SATA Drive which does not hava ATA EPC feature supported to SAS3 controller. Format the drive and verfiy that drive is under format. Execute a VPD inquiry to 0x8a (Power Condition VPD Page) which passes instead of failing with CC. | |
| ISSUE DESC: | During SATA Drive Format, Unsupported VPD Inquiry Command is Not Failed with Expected Response | |
| | | |
| (SCGCQ00711813) | | Defect 4/14 |
| HEADLINE: | Additional sense:Invalid cmd opcode, when read cmd sent to SATA drive in standby mode | |
| DESC OF CHANGE: | When checking for supported sata scsi commands, we were only checking the sata scsi commands supported array that does not contain read and write commands. Those commands are handled differently. I have added read and write as supported commands to the checking algorithm. | |
| TO REPRODUCE: | 1. Put drive in standby power mode 2. Issue read command 3 observe invalid command operation | |
| ISSUE DESC: | When we are trying to send read commad to a SATA drive which is in standby mode, we are getting Invalid command operation code as additional sense value. | |
| | | |
| (SCGCQ00711858) | | Defect 5/14 |
| HEADLINE: | Fault 1901 Seen When Running Unmap IO's During Task Aborts For a SATA Drive | |
| DESC OF CHANGE: | Set the device handle of the copied frame to 0 so that it doesn't get matched by a task management request. | |
| TO REPRODUCE: | Controller : Avago Gen 3 Controller - Fury 8 Port | |



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.04.00 - SAS3FW_MASTER_DEV (SCGCQ00729508)

F/W : 05.250.02.00- IT
Driver Version : 6.255.01.00
OS : Linux
Drive : SATA SSD

Reproduce :

- 1) Send a Read 10 command which will cause the IOC to terminate / abort the IO
- 2) In parallel send Unmap commands to the SSD drive

ISSUE DESC:

With a SATA passthrough command, PL firmware makes a copy of the original frame, and restores the original frame from the copy when the passthrough is complete. The problem here is that the copy gets matched by a task management request. It aborts it, but when the IOP tries to fail the IO, it doesn't know where it came from and faults with 0x1901.

(SCGCQ00714125)

Defect 6/14

HEADLINE: System gets Hung & reboot while running IO's along with diag reset on the Controller which has Active and Inactive volumes.

DESC OF CHANGE: Made change in the code to pend the request if shared page in use so that the request can be processed when shared page not in use.

TO REPRODUCE:

- Steps:
1. Boot to the OS with latest firmware.
 2. Create 2 Volumes on 1 Controller, connect 1 inactive volume.
 3. Start io's on Active Volumes Using Linux smash Utility.
 4. After io's ran for 8 to 10 minutes, start Controller reset script. (script will perform controller reset for every 20 Sec).
 5. System will be in Hung state after 10 to 15 minutes.

ISSUE DESC:

During loading the current page when there is another loading of page is occurring , IR FW was sending page with all 0's or partial data. This was leading to make driver panic the kernel intentionally and hence system was hung.

(SCGCQ00715211)

Defect 7/14

HEADLINE: PL Fault 0x6003 While Running Heavy IO and Injecting Expander Resets on Alternating SAS Domains

DESC OF CHANGE: Made a change in task management code so that the TM active bit is not cleared incorrectly in this situation.

TO REPRODUCE: Run heavy IO while injecting expander resets on alternating SAS domains every couple minutes.

ISSUE DESC: This issue involves two abort tasks for different IOs, but the same SAS drive. There is a TM active bit that PL uses to keep track of whether a TM is outstanding on a per device basis. There was a problem in task management code that was causing the TM active bit to be cleared when one of the abort tasks ended while the other was outstanding. In the case where the outstanding abort task hasn't aborted its IO yet, the IO can slip by and complete to the upper layers, leading to the 0x6003 fault.

(SCGCQ00715239)

Defect 8/14

HEADLINE: PL Fault 0x5851 is seen when running Query Task

DESC OF CHANGE: The controller firmware needs to look in multiple places when cleaning up the timed out task management.

TO REPRODUCE: Run non-destructive type task management and cause the TM to timeout.

ISSUE DESC: When running non-destructive type task management such as query task, if the TM times out, the controller firmware could fault with 0x5851.

(SCGCQ00715299)

Defect 9/14

HEADLINE: DID_SOFT_ERRORS are seen when Hot plug is performed on the RAID1 volume along with IOs.

DESC OF CHANGE: Made change to send all OPEN_FAILURE log codes as new IR log info code so that driver can retry the IO accordingly.

TO REPRODUCE: On a RHEL setup run test IO script to unplug/plug the drive with 30 sec delay,DID_SOFT error is seen on the system.

ISSUE DESC: During drive pull push IO was terminated due to which DID_SOFT errors are seen.

(SCGCQ00715484)

Defect 10/14



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.04.00 - SAS3FW_MASTER_DEV (SCGCQ00729508)

HEADLINE: SATL doesn't handle ATA Pass-through (16) properly when Extend bit is cleared
DESC OF CHANGE: When the Extend bit is cleared in ATA Passthrough (16), SATL will only look at the lower bytes of features, sector_count, lba_low, lba_mid and lba_high. It will also clear the upper bytes of those fields to 0 in the ATA return descriptor.
TO REPRODUCE: Send ATA Passthrough (16) command with Extend bit set to 0.
ISSUE DESC: When the Extend bit is cleared in ATA Passthrough (16) command, SATL is supposed to ignore the upper bytes of features, sector_count, lba_low, lba_mid and lba_high. It is also supposed to set those upper bytes to 0 in the ATA return descriptor.

(SCGCQ00728153) Defect 11/14

HEADLINE: IOP: DDR initialization may access invalid pointer
DESC OF CHANGE: If the call to get NVDATA (MFG Page 16) fails, firmware will fault, with an existing fault code that specifies which page was failed to be retrieved.
TO REPRODUCE: Found through code inspection
ISSUE DESC: If the call to get NVDATA (MFG page 16) fails, the code will currently continue, and could try to access the invalid NVDATA page.

(SCGCQ00728903) Defect 12/14

HEADLINE: Fury cards would fault with 58B4 on power up
DESC OF CHANGE: Change serdes init code back to what it was.
TO REPRODUCE: Boot into windows with Fury card.
ISSUE DESC: Fury cards would fault with 58B4 on power up.

(SCGCQ00717105 - Port of SCGCQ00707374) Defect 13/14

HEADLINE: PL: D205 fault when posting a host trace buffer during IO
DESC OF CHANGE: The wrong data size was being returned when sending data to the host buffer. Modified the code to return the correct amount of data sent to the host buffer.
TO REPRODUCE: Run script in Linux that starts IO to attached device(s) then registers, releases, reads, unregisters a host trace buffer.
ISSUE DESC: Seeing a D205 fault when running a script that registers, releases, reads and unregisters a host trace buffer while running Medusa IO. The fault does not occur every time.

(SCGCQ00725110 - Port of SCGCQ00721158) Defect 14/14

HEADLINE: sas9311-16i phase 5 nvdata error
DESC OF CHANGE: Added closing Tag </GPIODefinition_37>
TO REPRODUCE: Use SAS2Parser to concatenate nvdata image.
ISSUE DESC: Tag <GPIODefinition_37> is not properly closed in sas9311-16i phase 5 nvdata.

Change Summary (Defects=22 Enhancements=4)

- SCGCQ00683222 (DFCT) - PL: SR-IOV: Sense data for VFs written to the wrong host address
- SCGCQ00688470 (DFCT) - SAS3IRFW: Fault 8901 is seen once the volume is roamed to Fury card.
- SCGCQ00702665 (DFCT) - Invader hits 0x5805 fault when breaking active expander links.
- SCGCQ00703433 (DFCT) - WRITE SAME(10) and WRITE SAME(16) SCSI commands are not working for the last LBA of SATA Drive
- SCGCQ00705308 (DFCT) - With VALID bit set INFORMATION field in Sense data is not populated for WRITE LONG(16) SCSI Command
- SCGCQ00705320 (DFCT) - Fault 0x4203 When WRITE AND VERIFY (16) Command Is Executed to SATA Drive For LBA Out of Range
- SCGCQ00706963 (DFCT) - Read/Write 16 or 32 commands are Not Failed with Descriptor Format Sense Data when LBA is greater than 4 bytes.
- SCGCQ00707233 (DFCT) - READ CAPACITY(10) SCSI command to a SATA drive returns unexpected data
- SCGCQ00710138 (DFCT) - Unsupported POWER CONDITION Field in SCSI Start Stop Unit Command Not Failed with Check Condition
- SCGCQ00710168 (DFCT) - IOP: MCTP: Miscellaneous transmission path issues
- SCGCQ00710445 (DFCT) - Module Specific Resets 0 is missing the PBAM AI bit
- SCGCQ00710478 (DFCT) - IOP: MCTP: Handle allocation failure for received packet and additional post-processing cleanup
- SCGCQ00712499 (DFCT) - PL: Target Mode: Error check fails to test correctly
- SCGCQ00712688 (DFCT) - ATA Translation of sector count in sense data is inconsistent for READ DMA pass-through cmd
- SCGCQ00713288 (DFCT) -
- SCGCQ00713442 (DFCT) - IOP: SR-IOV: VF access to BIOS pages unexpectedly restricted
- SCGCQ00713624 (DFCT) - IOP: MCTP: Log Entry Added event triggered from wrong event
- SCGCQ00715317 (DFCT) - IOP: CLI command to dump L1 data cache causes 0x265D fault
- SCGCQ00705388 (CSET) - PL: Identify SSD topology restrictions cause fault 0xD10F when device access is disabled
- SCGCQ00709545 (CSET) - PL: Identify SSD code fails to test for IO start failure
- SCGCQ00709546 (CSET) - PL: Incorrect use of IOP LogInfo code
- SCGCQ00710440 (CSET) - sas9300-16i phase 5 nvdata errors
- SCGCQ00701936 (CSET) -
- SCGCQ00707806 (CSET) - Intruder: (IOP) Update some IOP event handling prints to reflect more useful info
- SCGCQ00709547 (CSET) -
- SCGCQ00709548 (CSET) - PL: Topology restrictions should wait for the entire topology to be discovered

Total Defects Resolved (22)

| (SCGCQ00683222) | | Defect 1/22 |
|-----------------|---|-------------|
| HEADLINE: | PL: SR-IOV: Sense data for VFs written to the wrong host address | |
| DESC OF CHANGE: | Modified a piece of code which determines the address to copy the sense data to. This code made an incorrect assumption regarding the function number, so the upper 32 bits of the sense buffer address was pull from what the physical function specified, not what the virtual function specified. This caused firmware to DMA the sense buffer to the wrong portion of memory. | |
| TO REPRODUCE: | Start the physical and virtual functions. The virtual funtion should have its sense buffer located in a different 4GB memory region from the physical function. Issue IOs from the virtual function that will be returned by the drive with sense data. Firmware will reply to the IO request indicating sense data is availble, but the sense data memory contains invalid data. | |
| ISSUE DESC: | When the virtual function host looks at an IO which is returned from the drive with sense data, the sense data is blank. This could also manifest itself as an IO/MMU fault. | |
| | | |
| (SCGCQ00688470) | | Defect 2/22 |
| HEADLINE: | SAS3IRFW: Fault 8901 is seen once the volume is roamed to Fury card. | |
| DESC OF CHANGE: | Changed the IOC page 6 constructor handling to call the fixed page constructor so that IOC page 6 cannot be shared with the other pages like RAID volume page and RAID Physdisk page. | |
| TO REPRODUCE: | <ol style="list-style-type: none">1. Create Raid10 volume with 6 SAS Drives. Wait till the BGI completes.2. Run IOs on the volume for 15 mins to 20 mins3. Pull non-Adjustment drives4. Volume will be in Degraded State. Now do a unclean Shutdown.5. Roam the volume to the other system. | |
| | Expected result: The Fault 8901 should not be seen. Observed result: 8901 Fault is seen. | |
| ISSUE DESC: | When a volume is roamed to other SAS3 card , 0x8901(Shared page buffer is already in use) fault was occurring. When a volume was roamed Host would request many page like IOC page6, RAID volume page, RAID Physdisk page etc., IOC page 6 page request was leading to fault since this page was being shared with the RAID volume and RAID physdisk page. | |
| | | |
| (SCGCQ00702665) | | Defect 3/22 |
| HEADLINE: | Invader hits 0x5805 fault when breaking active expander links. | |
| DESC OF CHANGE: | Back out SCGCQ00644555. | |
| TO REPRODUCE: | Run heavy I/O and break active expander links. | |
| ISSUE DESC: | Invader hits 0x5805 fault around 24 hours into the test. | |
| | | |
| (SCGCQ00703433) | | Defect 4/22 |
| HEADLINE: | WRITE SAME(10) and WRITE SAME(16) SCSI commands are not working for the last LBA of SATA Drive | |
| DESC OF CHANGE: | Modified WRITE SAME(10) and WRITE SAME(16) command handling to support the execution of WRITE SAME(10) and WRITE SAME(16) to the last LBA of the SATA drive. | |
| TO REPRODUCE: | Connect a SATA Drive to the controller, execute a read capacity command to know the size of drive and then execute the WRITE SAME(10) & WRITE SAME(16) command to last LBA of the drive. | |
| ISSUE DESC: | When executing the WRITE SAME(10) or WRITE SAME(16) to the last LBA of the drive, the command fails with logical block out of range which is incorrect. | |
| | | |
| (SCGCQ00705308) | | Defect 5/22 |
| HEADLINE: | With VALID bit set INFORMATION field in Sense data is not populated for WRITE LONG(16) SCSI Command | |
| DESC OF CHANGE: | Modified WRITE LONG(16) command handling in SATL to populate INFORMATION field with the LBA information for the out of range LBA case. | |
| TO REPRODUCE: | Connect SATA drive to the SAS3 controller and send WRITE LONG(16) command to SATA drive with the out of range LBA value in CDB. | |
| ISSUE DESC: | Execute WRITE LONG(16) SCSI command which results in check condition(for an out of range LBA case) and in this case as part of sense data the VALID bit is set to 1 but corresponding INFORMATION field is not populated. | |



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.03.00 - SAS3FW_MASTER_DEV (SCGCQ00717285)

| (SCGCQ00705320) | | Defect 6/22 |
|------------------------|---|-------------|
| HEADLINE: | Fault 0x4203 When WRITE AND VERIFY (16) Command Is Executed to SATA Drive For LBA Out of Range | |
| DESC OF CHANGE: | Added an additional check in SATL to account for this situation. | |
| TO REPRODUCE: | Send a SCSI WRITE AND VERIFY 16 command to a SATA drive. Use a 16 byte CDB and specify an LBA of 0xFFFFFFFFFFFFFFFF and transfer length of 1. When this command is sent repeatedly, a 0x4203 fault should result. | |
| ISSUE DESC: | In the SATL handle write verify function, addition of the (far out of range) LBA and transfer length caused a 64 bit variable to roll over, resulting in a value the appeared to be valid. As a result, the command wasn't failed by firmware when it should have been. | |

| (SCGCQ00706963) | | Defect 7/22 |
|------------------------|--|-------------|
| HEADLINE: | Read/Write 16 or 32 commands are Not Failed with Descriptor Format Sense Data when LBA is greater than 4 bytes. | |
| DESC OF CHANGE: | Firmware was calling an incorrect function to handle the failed I/O. | |
| TO REPRODUCE: | Send Read (16) command with LBA set to 0xFFFFFFFFFFFFFFFF. | |
| ISSUE DESC: | READ/WRITE 16 or 32 commands are Not Failed with Descriptor Format Sense Data when LBA is greater than 4 bytes. Firmware would incorrectly send the fixed format sense data. | |

| (SCGCQ00707233) | | Defect 8/22 |
|------------------------|--|-------------|
| HEADLINE: | READ CAPACITY(10) SCSI command to a SATA drive returns unexpected data | |
| DESC OF CHANGE: | Modified READ CAPACITY(10) handling in SATL to return proper data as part of response. | |
| TO REPRODUCE: | Connect a SATA drive to SAS3 controller and execute READ CAPACITY(10) SCSI command to the SATA drive. | |
| ISSUE DESC: | While executing READ CAPACITY(10) command to a SATA drive, we can notice that as part of response 8 bytes of parameter data is received along with the unexpected data which is incorrect as per the SAT spec. | |

| (SCGCQ00710138) | | Defect 9/22 |
|------------------------|---|-------------|
| HEADLINE: | Unsupported POWER CONDITION Field in SCSI Start Stop Unit Command Not Failed with Check Condition | |
| DESC OF CHANGE: | Added code to SATL to check for unsupported power condition values sent in a SCSI start stop unit command. | |
| TO REPRODUCE: | Send a SCSI start stop unit command with unsupported power condition field (for example, 0xC) to a SATA drive that supports the extended power condition feature set. Observe it is not failed with check condition, illegal request, invalid field in CDB. | |
| ISSUE DESC: | For a SATA drive that supports the extended power condition feature set, a SCSI start stop unit command sent with an unsupported power condition field is not failed with check condition, illegal request, invalid field in CDB like SAT3 specifies. | |

| (SCGCQ00710168) | | Defect 10/22 |
|------------------------|---|--------------|
| HEADLINE: | IOP: MCTP: Miscellaneous transmission path issues | |
| DESC OF CHANGE: | Made several simple fixes that impacted both the packet contents and the packet flow. | |
| TO REPRODUCE: | None. | |
| ISSUE DESC: | There were miscellaneous issues with the transmission path in MCTP that impacted both the packet contents and the flow. This includes using the MCTP VDM Buffer feature to transmit response messages with more than 2 packets, and proper clean-up of MCTP Control requests. | |

| (SCGCQ00710445) | | Defect 11/22 |
|------------------------|--|--------------|
| HEADLINE: | Module Specific Resets 0 is missing the PBAM AI bit | |
| DESC OF CHANGE: | Added the PBAM AI bit to the structure. | |
| TO REPRODUCE: | None. | |
| ISSUE DESC: | A structure for Module Specific Resets 0 register is missing the PBAM AI bit | |



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.03.00 - SAS3FW_MASTER_DEV (SCGCQ00717285)

(SCGCQ00710478) Defect 12/22

HEADLINE: IOP: MCTP: Handle allocation failure for received packet and additional post-processing cleanup
DESC OF CHANGE: Added code to properly stop allocating resources and drop the packet for the first error handling issue.
Added code to properly clean-up after processing an MCTP Control request when a failure occurs.
TO REPRODUCE: Found by code inspection.
ISSUE DESC: There is a code path for receiving a packet where a resource allocation failure is not being handled correctly. Another error handling issue occurs with clean-up after processing an MCTP Control request.

(SCGCQ00712499) Defect 13/22

HEADLINE: PL: Target Mode: Error check fails to test correctly
DESC OF CHANGE: Corrected the bad error check so it functions the way it should.
TO REPRODUCE: Found during code inspection.
ISSUE DESC: During a code inspection, a bug was found in some error handling code such that the error it was intended to detect would not detect the error.

(SCGCQ00712688) Defect 14/22

HEADLINE: ATA Translation of sector count in sense data is inconsistent for READ DMA pass-through cmd
DESC OF CHANGE: Firmware was looking at the wrong place for the amount of data transferred.
TO REPRODUCE: Send ATA passthrough command 85 0d 2e 00 00 00 01 00 00 00 00 00 00 40 c8 00 multiple times.
ISSUE DESC: ATA passthrough command with data transfer may return wrong sector count in the sense data.

(SCGCQ00713288) Defect 15/22

(SCGCQ00713442) Defect 16/22

HEADLINE: IOP: SR-IOV: VF access to BIOS pages unexpectedly restricted
DESC OF CHANGE: Updated the permissions on these pages to reflect the requirement.
TO REPRODUCE: Attempt to read or write to the BIOS pages from a virtual function.
ISSUE DESC: According to MPI, the virtual functions should have access to their own copies of the MPI BIOS pages, however the requests are rejected.

(SCGCQ00713624) Defect 17/22

HEADLINE: IOP: MCTP: Log Entry Added event triggered from wrong event
DESC OF CHANGE: Fixed the code to trigger from the Log Entry Added event.
TO REPRODUCE: Perform an action to generate a Log Entry Added event. Notice that this is not correctly passed to the MCTP interface.
ISSUE DESC: The Log Entry Added code to log the event with the MCTP interface is triggered by the wrong event (Log Data) instead of Log Entry Added.

(SCGCQ00715317) Defect 18/22

HEADLINE: IOP: CLI command to dump L1 data cache causes 0x265D fault
DESC OF CHANGE: Added an instruction to ensure a register is set to zero so the CPU does not attempt to access a random address in memory.
TO REPRODUCE: 1) Execute CLI command 'iop l1 dcd' to dump the L1 data cache.
2) Fault 0x265D is hit.
ISSUE DESC: When issuing the iop l1 dcd command, it may cause firmware to fault with code 0x265D.

(SCGCQ00705388 - Port of SCGCQ00702988) Defect 19/22



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.03.00 - SAS3FW_MASTER_DEV (SCGCQ00717285)

HEADLINE: PL: Identify SSD topology restrictions cause fault 0xD10F when device access is disabled
DESC OF CHANGE: Added code to clear an IO timer for IOs which are blocked.
TO REPRODUCE: Boot the system without any SSD devices attached and some approved HDD devices. PL will discover and report the devices, and if the host issues an IO, it will be rejected. Shortly afterward, firmware will fault with code 0xD10F.
ISSUE DESC: On boot when all devices are blocked, fault 0xD10F can be triggered if a host IO is sent to the PL.

(SCGCQ00709545 - Port of SCGCQ00702716)

Defect 20/22

HEADLINE: PL: Identify SSD code fails to test for IO start failure
DESC OF CHANGE: Added code to handle an unsuccessful return value from the function.
TO REPRODUCE: Found during code inspection.
ISSUE DESC: A particular location in code is not testing the return value from a function and may cause firmware to not fully identify a device.

(SCGCQ00709546 - Port of SCGCQ00709517)

Defect 21/22

HEADLINE: PL: Incorrect use of IOP LogInfo code
DESC OF CHANGE: Added a new PL LogInfo definitions and change the incorrect PL usages. The new defines are the same as the IOP equivalents, so no observable changes in behavior will occur.
TO REPRODUCE: Found by code inspection.
ISSUE DESC: Portions of PL firmware use a LogInfo code defined by IOP firmware. This breaks PL/IOP boundaries. No actual problems have been observed.

(SCGCQ00710440 - Port of SCGCQ00710287)

Defect 22/22

HEADLINE: sas9300-16i phase 5 nvdata errors
DESC OF CHANGE: Added the appropriate closing tags.
TO REPRODUCE: Cannot concatenate with FW using sas2parser
ISSUE DESC: Tags <GPIODefinition_37> and <RESOURCE_INITIATORS> are not closed properly



SCS Engineering Release Notice

Phase6 Alpha Release Version 05.250.03.00 - SAS3FW_MASTER_DEV (SCGCQ00717285)

Total Enhancements Implemented (4)

(SCGCQ00701936 - Port of SCGCQ00697961)

Enhancement 1/4

(SCGCQ00707806 - Port of SCGCQ00707767)

Enhancement 2/4

HEADLINE: Intruder: (IOP) Update some IOP event handling prints to reflect more useful info

NEW FUNCTIONALITY: Update some IOP event handling prints to reflect more useful info

(SCGCQ00709547 - Port of SCGCQ00706229)

Enhancement 3/4

(SCGCQ00709548 - Port of SCGCQ00707329)

Enhancement 4/4

HEADLINE: PL: Topology restrictions should wait for the entire topology to be discovered

NEW FUNCTIONALITY: This slight design change will hold off restricting access to allowed HDD until 15 seconds after the first port enable is received. This will allow ample time for PL to discover the topology, accounting for spin up and link up delays, looking for a SSD to unlock the HDDs.

Change Summary (Defects=14 Enhancements=13)

- SCGCQ00683795 (DFCT) - SATA Init Problem Causing 0x6230 Controller Fault
- SCGCQ00699027 (DFCT) - Problem in PL Diagnostic Code that Prints FPE VF Exceptions
- SCGCQ00703302 (DFCT) - PL: Target mode IO sends reply using wrong Hashed SAS Address
- SCGCQ00704291 (DFCT) - Controller firmware returns unexpected SCSI response when NACA bit is set to 1 for unmap and security protocol in/out commands
- SCGCQ00706016 (DFCT) - During SATA Drive Format or self test, One Extra Byte of Data is Provided When Inquiry VPD "Supported VPD Pages VPD Page" is requested
- SCGCQ00706052 (DFCT) - PL: CDB checking was not done properly for devices under format or self-test
- SCGCQ00706055 (DFCT) - During SATA Drive Format or self test, firmware does not handle Allocation Length of zero for INQUIRY SCSI Command Properly
- SCGCQ00706800 (DFCT) - SRIOV IT: SAS Topology Change List Event data has entries for devices which are not mapped to the VFs
- SCGCQ00709712 (DFCT) - IOP: Fault 0x265D hit when booting controller with attached enclosure
- SCGCQ00697065 (CSET) - Report Luns Command to a SATA drive fails with CheckCondition/Invalid Field in CDB when Allocation length set to Zero
- SCGCQ00697071 (CSET) - 0x58A1 fault occurs while issuing MUR to a target mode controller with outstanding IOs
- SCGCQ00699057 (CSET) - Fault 0x6230 While Running Heavy IOs and Cable Breaking
- SCGCQ00699059 (CSET) - Fault 6230 While Disabling Expander Phys and Running Stress in Multi-Path Failover Environment
- SCGCQ00707315 (CSET) - SAS3 SCS IT/IR firmware fails to hostboot
- SCGCQ00569175 (ENHREQ) - MPI 2.0: Add product-specific Flag bit to Clean Tool
- SCGCQ00574358 (ENHREQ) - MPI2: Allow UEFI and BIOS to be Enabled/Disabled individually
- SCGCQ00654921 (ENHREQ) - IR - MCTP over PCIe Support - RAID Action code needs to use SGL information in iopiMemoryMove
- SCGCQ00685820 (ENHREQ) - MPI 2.5: distribute Target Command Buffers Received across multiple reply queues
- SCGCQ00689555 (ENHREQ) - IOP SRIOV: During controller boot-up, make PortEnable replies to VFs wait until PF is ready
- SCGCQ00691019 (ENHREQ) - IOP: MCTP: Add support for MPI FW Upload Request
- SCGCQ00695575 (ENHREQ) - NVDATA: Increase maximum supported ManPage13 entries from 16 to 32
- SCGCQ00696232 (ENHREQ) - Allow MaxChainDepth as a configurable parameter in Manufacturing Page 9
- SCGCQ00699048 (ENHREQ) - IOP: MCTP: Register for events to filter without asynchronous event datagram
- SCGCQ00700829 (ENHREQ) - MPI 2.5: BIOS Page 1 additions
- SCGCQ00705414 (ENHREQ) - IOP: Deassert the HSB_N line when NVSRAM is available
- SCGCQ00709549 (ENHREQ) - PL Target Mode: Implement multi reply queue handling of command buffers
- SCGCQ00701937 (CSET) -



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.02.00 - SAS3FW_MASTER_DEV (SCGCQ00710448)

Total Defects Resolved (14)

(SCGCQ00683795) Defect 1/14

HEADLINE: SATA Init Problem Causing 0x6230 Controller Fault
DESC OF CHANGE: Changed the code in a SATA init callback function to not clear out the context area of the command frame.
TO REPRODUCE: Connect a SATA drive to the controller through an AA-Mux. The controller will immediately hit the 0x6230 fault.
ISSUE DESC: Certain IOs and operations, such as SATA initialization, are timed by controller firmware. There was a problem in SATA initialization code where the timer information got mistakenly cleared. This meant the timer could not be removed, ultimately leading to the 0x6230 fault.

(SCGCQ00699027) Defect 2/14

HEADLINE: Problem in PL Diagnostic Code that Prints FPE VF Exceptions
DESC OF CHANGE: Fixed the coding error in the PL diagnostic function and made the code easier to understand.
TO REPRODUCE: Use the CLI interface to dump the FPE exception queue for a given VF, at a time when the exception queue is not empty (if it's empty, nothing will happen).
ISSUE DESC: In a diagnostic function which prints the entries in the FPE exception queue for a given VF, there was a coding mistake that resulted in firmware trying to read addresses that were far outside the allocated range for the queue.

(SCGCQ00703302) Defect 3/14

HEADLINE: PL: Target mode IO sends reply using wrong Hashed SAS Address
DESC OF CHANGE: Reverted to the original method of inserting the hashed SAS address into the reply frame.
TO REPRODUCE: Create several LUNs on the target and start the initiator.
ISSUE DESC: Under some circumstances, target mode IOs may have a reply sent which has the incorrect hashed SAS address in it, which can lead to timed out IOs on the initiator.

(SCGCQ00704291) Defect 4/14

HEADLINE: Controller firmware returns unexpected SCSI response when NACA bit is set to 1 for unmap and security protocol in/out commands
DESC OF CHANGE: Use proper masks to check for unsupported/reserved bits with in CDBs.
TO REPRODUCE: Issue unmap command with NACA bit set.
ISSUE DESC: Firmware was supposed to terminate the command with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB when NACA bit is set in the CDB.

(SCGCQ00706016) Defect 5/14

HEADLINE: During SATA Drive Format or self test, One Extra Byte of Data is Provided When Inquiry VPD "Supported VPD Pages VPD Page" is requested
DESC OF CHANGE: Firmware needs to determine if extended power condition feature is supported by the drive and return appropriate page length for "Supported VPD Pages VPD Page".
TO REPRODUCE: Start format or self test on a sata drive.
Issue Inquiry with EVPD bit set and page code set to "Supported VPD Pages VPD Page"
ISSUE DESC: During SATA Drive Format or self test, firmware could provide one extra byte of data when Inquiry VPD "Supported VPD Pages VPD Page" is issued.

(SCGCQ00706052) Defect 6/14

HEADLINE: PL: CDB checking was not done properly for devices under format or self-test
DESC OF CHANGE: Perform CDB checking like we already do in normal SATL handling.
TO REPRODUCE: Start format unit command on a sata drive.
Send Report LUNS command with NACA bit set.
ISSUE DESC: CDB checking was not done properly for devices under format or self-test. This results in firmware returning good status even when unsupported bits are set.



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.02.00 - SAS3FW_MASTER_DEV (SCGCQ00710448)

(SCGCQ00706055) Defect 7/14

HEADLINE: During SATA Drive Format or self test, firmware does not handle Allocation Length of zero for INQUIRY SCSI Command Properly

DESC OF CHANGE: Initialize a local variable to zero when handling inquiry command during format or self test.

TO REPRODUCE: Start Format or self test on a sata drive.
Issue inquiry command with allocation length set to 0.

ISSUE DESC: During SATA Drive Format or self test, firmware may return non-zero transferCount in the scsi io error reply even though Allocation Length is set to zero for INQUIRY SCSI Command.

(SCGCQ00706800) Defect 8/14

HEADLINE: SRIOV IT: SAS Topology Change List Event data has entries for devices which are not mapped to the VFs

DESC OF CHANGE: Added another case to the filtering operation for SAS Topology Change Events before the message is sent up to the host.

TO REPRODUCE: Attach at least three drives. Give a VF permission to see two of those drives, but ensuring to leave one drive not visible whose DevHandle is between the two that are visible. The SAS Topology Change Event will show the non-visible drive with a status of No Change.

ISSUE DESC: When the driver PF sets up drive permissions, there is case where a VF has permission to see drives whose DevHandles are not adjacent, and the devices between are exposed to the VF. Any drives between those will be seen with a status of No Change.

(SCGCQ00709712) Defect 9/14

HEADLINE: IOP: Fault 0x265D hit when booting controller with attached enclosure

DESC OF CHANGE: Corrected a piece of code which attempted to prevent accessing uninitialized parts of code which was accidentally programmed with incorrect logic.

TO REPRODUCE: 1. FLASH the controller with version 05.250.02.00 IT or IR Firmware.
2. Power Off the system.
3. Connect the JBOD or Enclosure to the Controller.
4. Power On the system.
5. Observe that the Controller will fault with code 0x265D.

ISSUE DESC: Firmware will fault with code 0x265D when it is booted with an attached enclosure.

(SCGCQ00697065 - Port of SCGCQ00615518) Defect 10/14

HEADLINE: Report Luns Command to a SATA drive fails with CheckCondition/Invalid Field in CDB when Allocation length set to Zero

DESC OF CHANGE: The controller firmware will now complete the report lun command successfully with no data transfer if the allocation length is set to zero.

TO REPRODUCE: Send report lun to the controller firmware with allocation length set to zero.

ISSUE DESC: The controller firmware was behaving according to SPC3. If the allocation length for report lun is less than 16 bytes, it would fail the command with invalid field in CDB. SPC4 does not have the 16 byte requirement for report lun allocation length.

(SCGCQ00697071 - Port of SCGCQ00680151) Defect 11/14

HEADLINE: 0x58A1 fault occurs while issuing MUR to a target mode controller with outstanding IOs

DESC OF CHANGE: To reply to commands on the command received queue, the code has been changed to look at the full 64 bit address for the command buffers.

TO REPRODUCE: Issue MUR to a target mode controller while there are IOs still in the command received queue.

ISSUE DESC: MUR cleanup of the command buffers assumes the command buffer base address is in low memory (Upper 32 bits of the address are all 0).

(SCGCQ00699057 - Port of SCGCQ00669775) Defect 12/14

HEADLINE: Fault 0x6230 While Running Heavy IOs and Cable Breaking

DESC OF CHANGE: Made some changes to the timer code to account for this situation where the SMP cannot be fully cleaned up until later.

TO REPRODUCE: LSI Gen 3 SAS/SATA Controller - FW: 04.250.02.00
Modified version of Fedora Linux



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.02.00 - SAS3FW_MASTER_DEV (SCGCQ00710448)

1 LSI Gen 3 Cobra R C1 expander (4 SAS drives 4 SATA) -> Quarch cable breaker -> cascaded to 3 enclosures (33 SAS drives, 12 SATA)

All drives are running heavy IOs through block move test.

While IO's are running, cable breaker is connected to separate Linux host running perl script to break 1 random link every 5 seconds.

ISSUE DESC:

There was an SMP request that timed out. During hardware cleanup of the SMP request, it was found in a non-current context of Rx Context Manager, which means the cleanup couldn't be completed at that time. This also means the timer for the SMP could not be removed until later. This showed up as an IO in the expired timer bucket that wasn't accounted for, causing the fault.

(SCGCQ00699059 - Port of SCGCQ00692652)

Defect 13/14

HEADLINE: Fault 6230 While Disabling Expander Phys and Running Stress in Multi-Path Failover Environment

DESC OF CHANGE: Made a change in Tx transport layer error handling code to call the appropriate SMP engine function.

TO REPRODUCE: Topology includes:
2 LSI Gen 3 SAS/SATA controllers - FW 04.250.06.00
2 host systems running Linux
2 LSI Gen 3 expanders - FW 0.4.204.0

Each port of the controllers should make a separate path going into 1 Cobra, followed by 8 enclosures, connected in a round robin fashion, including 203 physical sas drives.

ISSUE DESC: Run heavy IOs and periodically glitch (temporarily disable) random phys on the expanders.

There's an SMP passthrough request that encounters a no destination count threshold exceeded error, which means the expander that was intended to receive the SMP couldn't be found, probably due to the glitching of expander phys being done in this test. During the cleanup of this error, the non-immediate SMP case was not accounted for, causing the wrong function to be called in the SMP engine code. This resulted in the timer for the SMP not being removed. When the timer bucket expired, controller firmware could not determine where the IO had come from, resulting in a fault.

(SCGCQ00707315 - Port of SCGCQ00695527)

Defect 14/14

HEADLINE: SAS3 SCS IT/IR firmware fails to hostboot

DESC OF CHANGE: Lowered the priority of the VPD interrupt so the controller boot-up process during hostboot could run without the VPD interrupt interfering.

TO REPRODUCE: Erase a controller's firmware. Boot to either an UEFI or DOS shell. Attempt to flash firmware with sas3flash, which will hostboot. The hostboot will fail.

ISSUE DESC: In systems that use the Vital Product Data (VPD) in PCIe, hostbooting with IT/IR firmware is failing. The VPD interrupt during the system boot was not being cleared due to no firmware running on the card. The VPD interrupt continued to trigger and prevented with the normal boot-up operations during hostboot.



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.02.00 - SAS3FW_MASTER_DEV (SCGCQ00710448)

Total Enhancements Implemented (13)

(SCGCQ00569175) Enhancement 1/13

HEADLINE: MPI 2.0: Add product-specific Flag bit to Clean Tool
NEW FUNCTIONALITY: For the Clean Tool, reserved bit 26 of the Flags field for product specific use.

(SCGCQ00574358) Enhancement 2/13

HEADLINE: MPI2: Allow UEFI and BIOS to be Enabled/Disabled individually
NEW FUNCTIONALITY: Defined additional bits in the BiosOptions field of BIOS Page 1 to allow for finer control of X86 BIOS and UEFI BSD.

(SCGCQ00654921) Enhancement 3/13

HEADLINE: IR - MCTP over PCIe Support - RAID Action code needs to use SGL information in iopiMemoryMove
NEW FUNCTIONALITY: Added code to use the SGL information passed in MPI message . Modified the call to iopiMemoryMove by sending appropriate flag values in RAID action and Config request code.

(SCGCQ00685820) Enhancement 4/13

HEADLINE: MPI 2.5: distribute Target Command Buffers Received across multiple reply queues
NEW FUNCTIONALITY: Added MinMSIxIndex and MaxMSIxIndex fields to CommandBufferPostBase Request. This allows host to specify a range of MSI-x index values the IOC can use when posting a Target Command Buffer Reply Descriptor to a Reply Descriptor Post Queue.

(SCGCQ00689555) Enhancement 5/13

HEADLINE: IOP SRIOV: During controller boot-up, make PortEnable replies to VFs wait until PF is ready
NEW FUNCTIONALITY: In an SR-IOV enabled IT firmware, when a diagnostic reset occurs from the PF, it was possible for IT firmware to reply to the Port Enable from VFs before the PF has set up the permissions for the drives. One symptom in Linux was the target identification number used in the VFs would increase. This ER adds a SAS IO Unit Control operation, VF Permissions Set, that the driver uses to synchronize with IT firmware. Until operation has occurred, IT firmware will wait on sending the Port Enable replies to the VFs.

(SCGCQ00691019) Enhancement 6/13

HEADLINE: IOP: MCTP: Add support for MPI FW Upload Request
NEW FUNCTIONALITY: Support was added in MCTP for the MPI FW Upload Request. Common usages include obtaining package information about the firmware on a controller, and copying the entire firmware image.

(SCGCQ00695575) Enhancement 7/13

HEADLINE: NVDATA: Increase maximum supported ManPage13 entries from 16 to 32
NEW FUNCTIONALITY: The number of SGPIO entries in ManPage13 was extended from 16 to 32. This gives customers more options on how to instruct IT/IR firmware to control SGPIO LEDs based on the MPI slot status.

(SCGCQ00696232) Enhancement 8/13

HEADLINE: Allow MaxChainDepth as a configurable parameter in Manufacturing Page 9
NEW FUNCTIONALITY: Manufacturing Page 9 now has a MaxChainDepth field. This value is reported through the IOCFacts Reply's MaxChainDepth. If 0 is placed in this field for Manufacturing Page 9, then the default value (currently 0x80) is used.



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.02.00 - SAS3FW_MASTER_DEV (SCGCQ00710448)

(SCGCQ00699048)

Enhancement 9/13

HEADLINE: IOP: MCTP: Register for events to filter without asynchronous event datagram
NEW FUNCTIONALITY: Added a new feature to the SCS MCTP's Event Notification Request. Before this request only enabled registration to receive an asynchronous event. Now this request also filters events in the various logging mechanisms, and has a bit to suppress all asynchronous events.

(SCGCQ00700829)

Enhancement 10/13

HEADLINE: MPI 2.5: BIOS Page 1 additions
NEW FUNCTIONALITY: For BIOS Page 1, added SSUTimeout field, and added Product Name String Format bits to the BiosOptions field.

(SCGCQ00705414)

Enhancement 11/13

HEADLINE: IOP: Deassert the HSB_N line when NVSRAM is available
NEW FUNCTIONALITY: When NVSRAM is available, i.e. the Enable NVSRAM flag in Manufacturing Page 11, IT/IR firmware will deassert the HSB_N line for NVSRAM chips in case older chips are used or the HSB_N line is connected to a newer NVSRAM chip.

(SCGCQ00709549)

Enhancement 12/13

HEADLINE: PL Target Mode: Implement multi reply queue handling of command buffers
NEW FUNCTIONALITY: Adds the functionality to support issuing command buffers to multiple reply queues when they are received from the initiator.

(SCGCQ00701937 - Port of SCGCQ00697973)

Enhancement 13/13



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.01.00 - SAS3FW_MASTER_DEV (SCGCQ00698933)

Change Summary (Defects=10 Enhancements=6)

SCGCQ00659825 (DFCT) - SATL is not returning ATA status return descriptor correctly after processing ATA passthrough command

SCGCQ00683190 (DFCT) - IOP: SR-IOV: Phy Changed events improperly filtered from SAS Topology Change List Event

SCGCQ00684852 (DFCT) - With VALID bit set INFORMATION field in Sense data is not populated for WRITE SAME(16) command

SCGCQ00685000 (DFCT) - WRITE SAME(10) command with UNMAP bit set in CDB doesn't behave as expected

SCGCQ00685854 (DFCT) - IOP: SR-IOV: Config page access denied from VFs

SCGCQ00692885 (DFCT) - PL: SATL Firmware doesn't return sector count in status return descriptor properly for non-data transfer ATA passthrough commands

SCGCQ00694683 (DFCT) - IOP: SR-IOV: Some SAS IO Unit Control messages from VFs are incorrectly rejected

SCGCQ00696238 (CSET) - 0x6004 fault on during controller reset test

SCGCQ00696408 (CSET) - Negotiated Physical Link Rate in SAS IO Unit Page 0 may not be correct after pulling a cable

SCGCQ00697506 (CSET) - IO error and stop when hot plug a HDD from RAID1

SCGCQ00644555 (ENHREQ) - PL: clear interrupt when AWT hits max value

SCGCQ00679104 (ENHREQ) - IOP: MCTP: Get Version, Get MessageType Support, and Get UUID MCTP Control Commands

SCGCQ00685827 (ENHREQ) - IOP: Target Mode performance improvements

SCGCQ00685828 (ENHREQ) - PL: Trace Buffer Manager performance improvements

SCGCQ00686570 (ENHREQ) - PL: Target Mode performance improvements

SCGCQ00689826 (ENHREQ) - NVDATA: Adding NVDATA configurations for Active Cable Management



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.01.00 - SAS3FW_MASTER_DEV (SCGCQ00698933)

Total Defects Resolved (10)

(SCGCQ00659825) Defect 1/10

HEADLINE: SATL is not returning ATA status return descriptor correctly after processing ATA passthrough command
DESC OF CHANGE: SATL firmware will now return the status return descriptor properly along with the correct sector count.
TO REPRODUCE: Issue an ATA passthrough command with this CDB.

CDB:0000: 85 0D 2F 00 00 00 01 77 77 00 77 00 77 40 25 00
ISSUE DESC: SATL firmware is not returning ATA status return descriptor correctly after processing ATA passthrough command.

(SCGCQ00683190) Defect 2/10

HEADLINE: IOP: SR-IOV: Phy Changed events improperly filtered from SAS Topology Change List Event
DESC OF CHANGE: Added code to the filtering of the SAS Topology Change List Event to check if an attached device is an expander. If it is, do not filter the Phy Changed event from the list.
TO REPRODUCE: Power off and on the second expander in a chain of two expanders and observe the events being returned.
ISSUE DESC: When using SR-IOV firmware, some Phy Changed events are being filtered inappropriately. When an expander is connected to a phy, its Phy Changed events will be removed from the SAS Topology Change List Event.

(SCGCQ00684852) Defect 3/10

HEADLINE: With VALID bit set INFORMATION field in Sense data is not populated for WRITE SAME(16) command
DESC OF CHANGE: Modified WRITE SAME(16) command handling to populate INFORMATION field with the LBA information for out of range LBA case.
TO REPRODUCE: 1.Connect Sata SSD Drive to Controller
2.send a WRITE SAME 16 command to SSD Drive with out of range LBA value in CDB.
sg_raw /dev/sda 93 08 00 00 ff ff ff ff 0a 00 00 00 01 00 00 -izero512.txt -s 512 -v
ISSUE DESC: Execute WRITE SAME(16) command which results in check condition(for an out of range LBA case) and in this case as part of sense data the VALID bit is set to 1 but corresponding INFORMATION field is not populated.

(SCGCQ00685000) Defect 4/10

HEADLINE: WRITE SAME(10) command with UNMAP bit set in CDB doesn't behave as expected
DESC OF CHANGE: Modified global CDB mask for WRITE SAME(10) command to support UNMAP and ANCHOR bits.
TO REPRODUCE: Issue WRITE SAME(10) command with the UNMAP bit set.
sg_raw /dev/sda 41 08 00 00 00 0a 00 00 01 00 -izero512.txt -s 512 -v
ISSUE DESC: If UNMAP bit is set in the WRITE SAME(10) command then the command fails with check condition:
SCSI Status: Check Condition
Sense information:
sense key:Illegal Request
Additional Sense: Invalid Field CDB

(SCGCQ00685854) Defect 5/10

HEADLINE: IOP: SR-IOV: Config page access denied from VFs
DESC OF CHANGE: Added permissions to allow the VF to read from Driver Persistent Mapping Page 0, IO Unit Page 10, SAS IO Unit Page 16, and granted write permissions for VFs to write to IOC Page 8.
TO REPRODUCE: Read or write to the affected configuration pages. The request will be denied.
ISSUE DESC: A number of pages are unable to be read and/or written by VFs incorrectly. This includes the following pages:
- Driver Persistent Mapping Page 0 (Read)
- IO Unit Page 10 (Read)
- SAS IO Unit Page 16 (Read)
- IOC Page 8 (Write)



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.01.00 - SAS3FW_MASTER_DEV (SCGCQ00698933)

(SCGCQ00692885) Defect 6/10

HEADLINE: PL: SATL Firmware doesn't return sector count in status return descriptor properly for non-data transfer ATA passthrough commands

DESC OF CHANGE: When filling out the status return descriptor, firmware needs to differentiate data and non-data transfer and return the sector count accordingly.

TO REPRODUCE: Send ATA passthrough command with a non-data transfer CDB.

ISSUE DESC: SATL Firmware doesn't return sector count in status return descriptor properly for non-data transfer ATA passthrough commands

(SCGCQ00694683) Defect 7/10

HEADLINE: IOP: SR-IOV: Some SAS IO Unit Control messages from VFs are incorrectly rejected

DESC OF CHANGE: Changed an incorrectly written conditional statement checking for unsupported operations to work as intended.

TO REPRODUCE: Issue a SAS IO Unit Control request from a VF that should be supported and observe the request is rejected with MPI2_IOCSTATUS_INVALID_FIELD.

ISSUE DESC: Some SAS IO Unit Control request operations are rejected incorrectly with MPI2_IOCSTATUS_INVALID_FIELD when they should be processed.

(SCGCQ00696238 - Port of SCGCQ00680866) Defect 8/10

HEADLINE: 0x6004 fault on during controller reset test

DESC OF CHANGE: Firmware will clear an interrupt associated with using large CDB before starting transport cleanup.

TO REPRODUCE: Send large CDB MPI SCSI IO Requests and generate task management at the same time.

ISSUE DESC: Firmware would sometimes fault with 0x6004 if host/IOP is sending Task Managements while large CDB SCSI IO Requests are in use.

(SCGCQ00696408 - Port of SCGCQ00692836) Defect 9/10

HEADLINE: Negotiated Physical Link Rate in SAS IO Unit Page 0 may not be correct after pulling a cable

DESC OF CHANGE: When doing link reset, firmware needs to clear the Negotiated Physical Link Rate field as well.

TO REPRODUCE: Initialize sas3 controller and connect a cable to a target.
Display SAS IO Unit page 0 to see the correct link rate.
Pull the cable
Display SAS IO Unit Page 0 and some phys may have stale link rate in Negotiated Physical Link Rate field

ISSUE DESC: Negotiated Physical Link Rate in SAS IO Unit Page 0 may not be correct after pulling a cable.

(SCGCQ00697506 - Port of SCGCQ00692866) Defect 10/10

HEADLINE: IO error and stop when hot plug a HDD from RAID1

DESC OF CHANGE: A new log code is added to address the issue.

TO REPRODUCE: On a RHEL setup run test IO script to unplug/plug the drive with 30 delay, IO error is seen on the system.

ISSUE DESC: IO was completing with an error during pull/push of a drive on a RAID 1 volume.



SCS Engineering Release Notice

Phase6 Pre-Alpha Release Version 05.250.01.00 - SAS3FW_MASTER_DEV (SCGCQ00698933)

Total Enhancements Implemented (6)

(SCGCQ00644555) Enhancement 1/6

HEADLINE: PL: clear interrupt when AWT hits max value
NEW FUNCTIONALITY: Hardware workaround created to interrupt when Arbitration Wait Timer (AWT) reaches max value of 16'hFFFF. The interrupt is then cleared to help minimize the AWT from constantly being re-initialized.

(SCGCQ00679104) Enhancement 2/6

HEADLINE: IOP: MCTP: Get Version, Get MsgType Support, and Get UUID MCTP Control Commands
NEW FUNCTIONALITY: Implemented the following MCTP Control Commands:
- Get MsgType Support : A list of MCTP MsgTypes supported
- Get Version: A list of MCTP versions supported for each supported MsgType
- Get UUID: Get the Unique Universal ID of the controller using the SHA1 method (method 5).

(SCGCQ00685827) Enhancement 3/6

HEADLINE: IOP: Target Mode performance improvements
NEW FUNCTIONALITY: Change code in the IOP portion of firmware to improve Target Mode performance. There are no functionality differences present.

(SCGCQ00685828) Enhancement 4/6

HEADLINE: PL: Trace Buffer Manager performance improvements
NEW FUNCTIONALITY: As part of target mode performance improvements, the firmware involved in adding an entry to the Trace Buffer Manager was identified as needing performance optimization. This only improves the performance of the PL firmware involved in adding an entry, and it does not change the expected behavior in any way, beyond changes which improve performance.

(SCGCQ00686570) Enhancement 5/6

HEADLINE: PL: Target Mode performance improvements
NEW FUNCTIONALITY: Changed the code to improve target mode IOPs performance. This should not include any functional changes, just changes in code ordering and code style to improve the execution speed.

(SCGCQ00689826) Enhancement 6/6

HEADLINE: NVDATA: Adding NVDATA configurations for Active Cable Management
NEW FUNCTIONALITY: Adding new NVDATA files to support active cable management, which includes active copper cables and optical cables. The following boards now support it:

sas9300-8e
sas9300-16e
sas9300-4i4e
sas9311-4i4e

All files that have active cable management enabled will have the abbreviation "acm" inserted into the file name, i.e. SAS9300-8e_it_acm_p.xml.

Active cable management must be actively selected by the customer. There are qualified 12G cables that report 6G functionality under active cable management, and the reported values are used.