EDKII Update for Intel® Quark™ SoC X1000 Software

Package Version: EDKII 1.0.2

Release Notes

16 June 2014

Order Number: 330729-001US

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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.

A ”Mission Critical Application” is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm.

Any software source code reprinted in this document is furnished for informational purposes only and may only be used or copied and no license, express or implied, by estoppel or otherwise, to any of the reprinted source code is granted by this document.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor%5Fnumber/

Code Names are only for use by Intel to identify products, platforms, programs, services, etc. (“products”) in development by Intel that have not been made commercially available to the public, i.e., announced, launched or shipped. They are never to be used as “commercial” names for products. Also, they are not intended to function as trademarks.

Intel, the Intel logo, and Quark are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Contents

Tables

Revision History

Date	Revision	Description
16 June 2014	001	This document describes an EDKII 1.0.2 Update to the parent Intel® Quark™ SoC X1000 Software Release 1.0.1 package.

§ §

1.0 Description of Release

The EDKII 1.0.2 is a component of its parent Intel® Quark™ SoC X1000 software release, package version 1.0.1. Refer to the Intel® Quark™ SoC X1000 Software Release Notes for detailed information on release 1.0.1.

The EDKII 1.0.2 Update is required for developers who wish to follow the new Intel® Quark™ SoC BIOS boot policy of booting from external media first or for those wishing to build EDKII in a Windows* build environment or wishing to avail of the other new features listed in Section 1.1.

For instructions on building and running the release software, see the Intel® Quark™ SoC X1000 Board Support Package (BSP) Build and Software User Guide, which has been updated to coincide with the EDKII 1.0.2 update.

These release notes include all issues associated with the entire Intel® Quark™ SoC X1000 Software Release 1.0.1, including EDKII 1.0.2 related issues.

1.1 New Features in the EDKII 1.0.2 Update Release

Note: The features below are all provided by the BIOS/Firmware.

- BIOS changed to boot from external media before SPI flash payload for conformance with classic BIOS boot order.
- BIOS will endeavour to recover SPI flash contents without the need for user input via the system console if the platform jumper/strap to force firmware recovery is applied.
- Support for the EDKII VS2008x86 (Microsoft* Visual Studio*) tool chain option has been added.
- BIOS instantiates ACPI Device objects for on-board I^{2}C and SPI devices (a new BIOS build requirement for the ACPI5.0 compatible `iasl` compiler).
- Galileo (Fab D, blue PCB) specific: BIOS instantiates the ACPI GPIO Client Device object for Intel® Quark™ SoC GPIOs and Cypress IO Expander GPIOs (a new BIOS build requirement for the ACPI5.0 compatible iasl compiler).
- Galileo (Fab D, blue PCB) specific: BIOS routes out Intel® Quark™ SoC Uart0 signals to IO header pins by default.
- Legacy SPI Flash Recovery is implemented and tested.
  Note: In the Intel® Quark™ SoC X1000 Software Release Notes for package release 1.0.0 and 1.0.1, this is incorrectly documented as “not implemented”.

1.2 Limitations

The software package has the following limitations:

- S3 support is implemented but not validated. It is not recommended for use in this release.

- Automatic version number updating during the update/recovery process is not implemented. Rollback protection (preventing downgrading to a previous software version) requires the version number of a software module to be greater or equal to the corresponding version number stored in the SPI flash. Support to update the version number stored in SPI flash if the corresponding software module is being updated, has not been added.
- UEFI 2.3.1 Secure Boot support is not implemented.
- Support for multiple keys is not included in this release.

1.3 EDKII Update 1.0.2 Package

```
Quark_EDKII_v1.0.2.tar.gz
```

1.4 Related Documentation

The documents in Table 1 provide more information about the software in this release.

Note: Changebars in the following table indicate documents that were created or updated for the EDKII 1.0.2 Update release.

Table 1. Related Documentation

Document Name	Reference Number
EDKII Update for Intel® Quark™ SoC X1000 Software Release Notes (this document) NEW	339676
Intel® Quark™ SoC X1000 Software Release Notes	330232
Intel® Quark™ SoC X1000 Board Support Package (BSP) Build and Software User Guide	329687
Intel® Quark™ SoC X1000 Software Developer's Manual for Linux*	330235
Intel® Quark™ SoC X1000 Secure Boot Programmer's Reference Manual	330234
Intel® Quark™ SoC X1000 UEFI Firmware Writer's Guide	330236
Intel® Galileo Board User Guide	330237
Source Level Debug using OpenOCD/GDB/Eclipse on Intel® Quark SoC X1000 Application Note https://communities.intel.com/docs/DOC-22203	330015
Intel® Quark™ SoC X1000 Datasheet https://communities.intel.com/docs/DOC-21828	329676
Intel® Quark™ SoC X1000 Core Developer's Manual https://communities.intel.com/docs/DOC-21826	329679
Intel® Quark™ SoC X1000 Core Hardware Reference Manual https://communities.intel.com/docs/DOC-21825	329678
Clanton Hill and CAN Getting Started Guide This document is provided to selected customers only; contact your Intel representative.	545350

1.5 Licensing

This package contains source code licensed under one or more open source licenses. Consult the COPYING, README, or LICENSE files in the appropriate subdirectory. Intel does not make any representations or warranties, express or implied, including without limitation, any warranty of fitness for any purpose, merchantability or non-infringement.

The package also includes executable binaries provided under Intel Proprietary License (IPL) as listed in Table 2. The IPL license file is in the same directories as the binaries in the package.

Table 2. License Files

Location	Description
...\QuarkSocPkg\QuarkNorthCluster\Binary\QuarkMicrocode\RMU.bin	Microcode for the Intel® Quark™ SoC X1000. (RMU: Remote Management Unit)
...\QuarkSocPkg\QuarkNorthCluster\Binary\Quark2Microcode\RMU.bin	Microcode for a future generation Quark SoC.

2.0 Known Issues

This section lists all issues associated with the entire Intel® Quark™ SoC X1000 Software Release 1.0.1, including EDKII 1.0.2 related issues. Known issues coinciding with the EDKII 1.0.2 Update release are shown with changebars.

Table 3. Known Issue Summary

2.1 38292 - Cannot force MMC into 4-bit mode due to kernel bug

Title	Cannot force MMC into 4-bit mode due to kernel bug
Id	38292
Implication	There is a kernel bug that is seen when forcing MMC into 4-bit mode. If you use the command: modprobe sdhci debug_quirks=0x400000 Only one bit is set: SDHCI_QUIRK_FORCE_1_BIT_DATA, bit 22 The board fails to initialize; returning these errors: - 110 timeout - 5 I/O error
Workaround	Use the command: modprobe sdhci debug_quirks=0x8400000 This sets: SDHCI_QUIRK_FORCE_1_BIT_DATA, bit 22 SDHCI_QUIRK_MISSING_CAPS, bit 27

2.2 45539 - SDMediaDevice.efi is setting older 25 MHz cards to 50 MHz

Title	SDMediaDevice.efi is setting older 25 MHz cards to 50 MHz
Id	45539
Implication	25MHz SD cards will not be recognized or usable.
Workaround	Use 'Fast' 50MHz capable SD cards.

2.3 46834 - UART interrupt handler not restored after resume from S3

Title	UART interrupt handler not restored after resume from S3
Id	46834
Implication	Suspected race condition between 8250 restore code and interrupt handler. Following resume from S3, 8250 will be in polled mode, not interrupt mode.
Workaround	Do not enter into S3 (unsupported).

2.4 48226 - eSRAM driver cannot map code required to do mapping

Title	eSRAM driver cannot map code required to do mapping
Id	48226

2.4 48226 - eSRAM driver cannot map code required to do mapping

Implication	eSRAM driver depends on code internally and externally in order to map things into eSRAM. During the mapping process, over-layed sections of DRAM become NULL for a time. It is not possible to eSRAM overlay code to itself be overlayed.
Workaround	Do not try to overlay any of the following kernel symbols: intel_cln_esram_* intel_cln_sb_* memcpy spin_lock spin_unlock spin_lock_irqsave spin_unlock_irqrestore pci_read_config_dword pci_write_config_dword

2.5 53887 - Deadlock in bluetooth stack - inherited from upstream kernel

Title	Deadlock in bluetooth stack - inherited from upstream kernel
Id	53887
Implication	When using the bluetooth software stack, a potential deadlock message can be found in /var/log/messages. Could potentially cause a lock-up but this has yet to be shown.
Workaround	None.

2.6 57071 - Galileo board is unavailable after host computer sleeps

Title	Galileo board is unavailable after host computer sleeps
Id	57071
Implication	When the Galileo board is connected to a host computer that enters sleep mode, and the host is woken, the Galileo board will be unavailable on USB. This behavior is caused by the Gadget Serial driver and is seen on all OSes (Linux, Windows, Mac OS).
Workaround	There is no workaround, you must reboot the Galileo board.

2.7 58381 - Attempting to unload a Linux driver which is in use causes console to freeze

Title	Attempting to unload a Linux driver which is in use causes console to freeze
Id	58381
Implication	When a driver is in use (like for instance SD/MMC mass storage device when an SD card is mounted) and user tries to remove it using 'modprobe -r mmc_block' then existing console hangs. Existing console is not usable until board rebooted or mass storage device unmounted from other console.
Workaround	Make sure the driver is not use before trying to unload. For instance unmount mass storage device first, then unload mmc_block driver.

2.8 58453 - pch_udc driver crash on reload

Title	pch_udc driver crash on reload
Id	58453

2.8 58453 - pch_udc driver crash on reload

Implication	When ehci_pci, ehci_hcd, pch_udc, g_serial drivers are loaded and user executes: modprobe -r g_serial modprobe -r pch_udc modprobe pch_udc then pch_udc driver crashes. Problem seen on Galileo board. Driver is unusable until board rebooted.
Workaround	Unload first ehci-pci driver to revert to USB1.1, then g_serial and pch_udc drivers can be unloaded or reloaded.

2.9 60003 - Legacy RTC 'Valid' time bit is set even though RTC contains invalid time

Title	Legacy RTC 'Valid' time bit is set even though RTC contains invalid time
Id	60003
Implication	Legacy RTC 'Valid' time bit is set even though RTC contains invalid time. Any software that trusts the 'Valid' bit without any sanity checks on the time/date may be using a corrupt date/time.
Workaround	None.

2.10 60147 - Quark enumerates incorrect device class as a USB CDC ACM device

Title	Quark enumerates incorrect device class as a USB CDC ACM device
Id	60147
Implication	As a USB CDC ACM device, the Quark SoC enumerates a USB Device descriptor with Class, SubClass and DeviceProtocal 02, 00, and 00 respectively. This is incorrect given that the Quark CDC ACM setup uses Interface Association Descriptors. The USB specification recommends different values in the device descriptor when using IADs, consequently, Windows may generate errors. The values in the device descriptor should be EFh, 02h, 11h, respectively.
Workaround	None.

2.11 60803 - BIOS error when using 2G MMC card

Title	BIOS error when using 2G MMC card
Id	60803
Implication	2G Transcend MMC card (TS2GMMC4) is not recognised or is unusable.
Workaround	Use alternative MMC card.

2.12 61236 - Real Time Clock update issue (sh: %4Y%2m%2d%2H%2M: bad number)

Title	Real Time Clock update issue (sh: %4Y%2m%2d%2H%2M: bad number)
Id	61236

2.12 61236 - Real Time Clock update issue (sh: %4Y%2m%2d%2H%2M: bad number)

Implication	The initscripts provided in poky release 1.4 do not support the simplified date program used by busybox. This shows an error in the boot log and may prevent Linux from reading time from the RTC clock and from saving time to it.
Workaround	Go to the /etc/init.d/ directory on the target system. In both the bootmisc.sh and save-rtc.sh scripts there, search for: date -u +%4Y%2m%2d%2H%2M and replace with: date -u +%Y%m%d%H%M

2.13 63520 - SMBIOS fields are currently incorrect for the Quark reference platforms

Title	SMBIOS fields are currently incorrect for the Quark reference platforms
Id	63520
Implication	Only SMBIOS Type0 and Type2 fields have been validated to be correct. Software using any other SMBIOS entries may be using incorrect information.
Workaround	Only use validated SMIOS table entries.

2.14 64263 - Error detecting Western Digital USB 3.0 hard drive

Title	Error detecting Western Digital USB 3.0 hard drive
Id	64263
Implication	Western Digital USB3.0 HDD not recognized or usable.
Workaround	Use alternative USB HDD.

2.15 64428 - Legacy Resume Well GPIO registers showing hardware default values after cold boot on Clanton Hill board

Title	Legacy Resume Well GPIO registers showing hardware default values after cold boot on Clanton Hill board
Id	64428
Implication	During Automating testing, certain Quark SoC Legacy Bridge Resume Well GPIO registers have shown hardware defaults after system cold boot. These registers include: Resume Well GPIO Input/Output Select (RGIO)—Offset 24h Resume Well GPIO Trigger Negative Edge Enable (RGTNE)—Offset 30h Resume Well GPIO GPE Enable (RGGPE)—Offset 34h Software and hardware components dependent on SoC resume well GPIOS may fail. This includes Battery Charge Enable Output, Main Battery Valid Input, Accelerometer Wake Input, PCIe reset output, WiFi disable output and GPS Antenna Enable Output. Registers have always shown correct values after a system warm boot.
Workaround	None.

2.16 65706 - Hot plug of USB key intermittently fails

Title	Hot plug of USB key intermittently fails
Id	65706
Implication	USB key is not recognized or is unusable.
Workaround	Disconnect and reconnect the USB key.

2.17 65952 - USB Errors seen with Sandisk Cruzer 4GB Flash Drive

Title	USB Errors seen with Sandisk Cruzer 4GB Flash Drive
Id	65952
Implication	USB Key 'Sandisk Cruzer 4GB' is not recognized or is unusable in BIOS.
Workaround	Use alternative USB key.

2.18 66053 - Poor USB write performance caused by automounter

Title	Poor USB write performance caused by automounter
Id	66053
Implication	Automounting of USB memory is done with the '-o sync' flag by default. For VFAT filesystems (the default on USB and SD memory), there is a performance degradation which causes a typical write to take about 5 minutes.
Workaround	One workaround is to search and replace '-o sync' with '-o flush' in the /usr/bin/automount.sh file. However, the copy command will return before the write is complete. If the USB memory device is removed before the write is complete, the board may be in an unbootable state.

2.19 66218 - Nonfunctional USB key may break the detection for other functional USB keys on Clanton Hill

Title	Nonfunctional USB key may break the detection for other functional USB keys on Clanton Hill
Id	66218
Implication	This issue is seen only when non-functional USB key is connected to J1. Note that J12 (USB port0) and functional USB key connected to J10 (USB port1 via hub). Issue is not seen when positions are swapped.
Workaround	Only connect functional USB devices (USB devices that EDKII can function with without errors) to the system.

2.20 66803 - Recovery boot intermittently stalls during PCI enumeration

Title	Recovery boot intermittently stalls during PCI enumeration
Id	66803
Implication	An intermittent system hang has been observed when booting a recovery image. This hang occurs during PCI enumeration. This hang has only been observed on a Cross Hill platform and happened 4 times out of 10 attempts.
Workaround	Retry the recovery process.

2.21 69965 - Quark EDKII default exception handler entry point is not valid

Title	Quark EDKII default exception handler entry point is not valid
Id	69965
Implication	If the system hits an exception (divide by zero for example) during Quark EDKII boot then the system will vector to the default exception handler at address 0xFFFFFFE4. As there is no valid exception handler at this address, system behavior is undefined.
Workaround	None.

2.22 70897 - SPI flash corruption can cause a system built without the SECURE_LD build option to become un-recoverable

Title	SPI flash corruption can cause a system built without the SECURE_LD build option to become un-recoverable
Id	70897
Implication	The RMU.bin area of SPI flash is not currently protected by the Protected BIOS Range Registers (RCBA + 3080h -> RCBA + 308Bh). The RMU.bin is a critical component that is required for the Recovery boot path. If the RMU.bin image in SPI flash gets corrupted during SPI flash updates, then the system will be unrecoverable and unable to boot.
Workaround	Avoid updating this area of SPI flash on unsecure systems.

2.23 70961 - Clanton Hill: If ETH0 is disconnected, ETH1 will not automatically pick up an address from DHCP

Title	Clanton Hill: If ETH0 is disconnected, ETH1 will not automatically pick up an address from DHCP
Id	70961
Implication	There are two PHYs on the Clanton Hill board. If ETH0 is disconnected and ETH1 is connected to the network with DHCP available, an address for ETH1 is not retrieved automatically.
Workaround	Enter the command 'ifup ETH1' to manually retrieve an address.

2.24 73738 - CrossHill: cannot access USB stick if you boot Linux from SD card or USB stick when both devices plugged in during power on

Title	CrossHill: cannot access USB stick if you boot Linux from SD card or USB stick when both devices plugged in during power on
Id	73738
Implication	Issue seen on Cross Hill platforms only. If both SD card and USB key are connected to the board during power on, the USB key cannot be accessed.
Workaround	Insert removable device later after boot.

2.25 73848 - Spurious 'unmounting /media/realroot' error message

Title	Spurious 'unmounting /media/realroot' error message
Id	73848
Implication	When booting from mass storage the following error is returned in the boot log: umount: can't umount /media/realroot: Device or resource busy This occurs for images booted from mass storage devices.
Workaround	None; this error can be ignored.

2.26 74444 - No value returned in EventLogLastEntry output parameter in EFI_TCG_HASH_LOG_EXTEND_EVENT Service of EFI_TCG_PROTOCOL

Title	No value returned in EventLogLastEntry output parameter in EFI_TCG_HASH_LOG_EXTEND_EVENT Service of EFI_TCG_PROTOCOL
Id	74444

2.26 74444 - No value returned in EventLogLastEntry output parameter in EFI_TCG_HASH_LOG_EXTEND_EVENT Service of EFI_TCG_PROTOCOL

Implication	UEFI Applications / Bootloaders using the EFI_TCG_PROTOCOL installed by software release 1.0.1 will not receive any value in the EventLogLastEntry output parameter in EFI_TCG_HASH_LOG_EXTEND_EVENT Service of EFI_TCG_PROTOCOL. This is a known issue with -r13937 of the EDKII SecurityPkg.
Workaround	Do not use value in EventLogLastEntry after calling EFI_TCG_HASH_LOG_EXTEND_EVENT Service of EFI_TCG_PROTOCOL.

2.27 75161 - Boot log error: memory range cannot be reserved

Title	Boot log error: memory range cannot be reserved
Id	75161
Implication	When booting, the following error is displayed in boot logs: [0.996963] pnp: PnP ACPI init [0.996963] ACPI: bus type pnp registered [1.003633] system 00:00: [mem 0xe0000000-0xe1ffffff] has been reserved [1.011283] system 00:00: [mem 0xfed1c000-0xfed1ffff] has been reserved [1.018649] system 00:00: [mem 0x000c0000-0x000dffff] has been reserved [1.026093] system 00:00: [mem 0x000e0000-0x000fffff] could not be reserved
Workaround	This error message will not affect board operation and can be ignored.

2.28 75172 - Clanton Hill: USB Error messages reported when booting debug build of EDKII

Title	Clanton Hill: USB Error messages reported when booting debug build of EDKII
Id	75172
Implication	The following error messages are reported during boot on Clanton Hill with a debug build of EDKII: Error Count : 3 EhcControlTransfer: error - Device Error, transfer - 2 However, no functional USB issues are observed and USB is working as expected. Issue is currently under investigation.
Workaround	None.

2.29 75539 - Legacy GPIO driver does not detect multiple, synchronous interrupts

Title	Legacy GPIO driver does not detect multiple, synchronous interrupts
Id	75539

2.29 75539 - Legacy GPIO driver does not detect multiple, synchronous interrupts

Implication	Error was observed during testing on the Legacy GPIO, when interrupts are generated at the same time for multiple pins. The setup is as follows: One GPIO pin is set as an output (GPIO_X), two are set as inputs (GPIO_Y, GPIO_Z). All pins are connected together. GPIO_Y and GPIO_Z are set to interrupt on a rising edge. GPIO_X is set to 1. The output behavior is as follows: GPIO_Y interrupt count increases by one in /proc/interrupts. GPIO_Z interrupt count does not change in /proc/interrupts. This behavior is not observed in the I2C/GPIO driver.
Workaround	This can be fixed by following the method used in the I2C/GPIO driver. First the register is read only once and the mask is saved locally. All bits are then cleared together and each interrupt is addressed using the local mask.

2.30 77401 - Clanton Hill board hangs after checking or setting speed of ttyQRK0 (stty)

Title	Clanton Hill board hangs after checking or setting speed of ttyQRK0 (stty)
Id	77401
Implication	On the Clanton Hill board when trying to use stty, sometimes the command hangs and nothing happens. This is likely due to the port being stuck because it's waiting for one of the modem control lines to be asserted. When the CAN microcontroller on the Clanton Hill board is reset, it sends some data over UART. Then when the stty command is run, the system gets stuck.
Workaround	Reset the Fujitsu CAN microcontroller again to restore the system.

2.31 77507 - Galileo Gen2 only: IRQs missed if pulses too close together on GPIO expanders

Title	Galileo Gen2 only: IRQs missed if pulses too close together on GPIO expanders
Id	77507

2.31 77507 - Galileo Gen2 only: IRQs missed if pulses too close together on GPIO expanders

Implication	On the Galileo Gen2 boards, there is a PCAL9555A GPIO expander that provides interrupt support for some of the digital I/O header pins. Those pins are IO2-3 and IO14-9, and also the shield reset button. If those pins are configured to generate interrupt notifications, and if the rate of interrupt trigger events (e.g. falling/rising edge signals on the pin) exceeds a combined rate of approximately 1000 interrupt events per second, the interrupt notifications from the PCAL9555A may stop working. Notifications for subsequent interrupt events will not be received by software. Possible implications: * 'Change-mode' interrupts (where an interrupt is generated on either a rising or a falling edge input signal) should be used on IO2-3 only if the rate of interrupts is likely to exceed 1000 per second. For other interrupt modes (falling edge only, rising edge only, low level, high level), it is possible to use SoC GPIO pins instead which are also connected to IO2-3. * Interrupts should be used on IO14-19 only if the rate of interrupts is likely to exceed 1000 per second. However, due to the presence of 1uF capacitors on these pins and their effect on signal rise/fall times, it is unlikely that these pins would be used for high-rate interrupt signalling. * The shield reset input is intended for use with a manually-pressed reset button on an Arduino shield. In that scenario, the rate of button presses is unlikely to exceed 1000 per second. However, there is a chance that signal bounce from the mechanical switch could conceivably trigger this scenario.
Workaround	It is possible to restore interrupt functionality by reading the current input values from any GPIO pin(s) on the PCAL9555A that are configured to generate interrupts. This will effectively 'clear' the outstanding interrupts and allow new interrupt notitications to be detected by software.

2.32 77674 - Parity error checking is performed even when set to ignore errors

Title	Parity error checking is performed even when set to ignore errors
Id	77674
Implication	If parity checking is set on Quark via stty with the ignpar setting (ignore incoming packages with parity error), incoming packages with parity error are not ignored as expected.
Workaround	Handle parity errors at an application level instead of depending on the stty ignpar setting.

2.33 77914 - UART DMA: incrementation of an array in an ifdef statement causes driver to crash

Title	UART DMA: incrementation of an array in an ifdef statement causes driver to crash
Id	77914
Implication	Removing CONFIG_SERIAL_QUARK_UART_CONSOLE from the kconfig causes an array in the UART driver to not increment. As a result, both ports are not properly addressed, which then causes the driver to crash.
Workaround	Do not build the kernel without CONFIG_SERIAL_QUARK_UART_CONSOLE

2.34 78401 - Sketch performance impacted when USB serial cable is removed

Title	Sketch performance impacted when USB serial cable is removed
Id	78401

2.34 78401 - Sketch performance impacted when USB serial cable is removed

Implication	After a sketch has been downloaded to the board, and the USB cable that was used to download the sketch is removed, the LED blinking slows and becomes erratic. Also, clloader is stuck with stale file handles and the console cannot be used.
Workaround	This is a known issue with the clloader and related to other open issues on the gadget-serial interface. High performance sketches are more affected than lower ones. This issue was seen when designing sketches that will operate without USB cable.

2.35 78550 - Some USB keys not recognised by Quark EDKII recovery on Galileo and Galileo Gen2

Title	Some USB keys not recognised by Quark EDKII recovery on Galileo and Galileo Gen2
Id	78550
Implication	Recovery process will fail on Galileo and Galileo Gen2 with these USB keys. Currently the following USB keys have been seen to fail: 1) Sandisk cruzer 4GB 2) Transend 4GB
Workaround	Two potential workarounds have been identified: (1) Connect a USB hub to the Galileo Gen2 USB port and then connect the failing USB key(s) to the USB hub. The USB keys have been observed to pass in this configuration (2) Select a different USB key

2.36 78738 - I2C/GPIO level-triggered interrupts cause system hang

Title	I2C/GPIO level-triggered interrupts cause system hang
Id	78738
Implication	System hangs during testing level-triggered interrupt handling in the I2C/GPIO driver (intel_qrk_gip). After loading the driver, the GPIO pin level goes low (verified with multimeter) and stays low. The interrupt fires and the system hangs forever (no response on shell via serial or ssh).
Workaround	Reboot the board.

2.37 80328 - 8MB Manufacture binary created by EDKII standalone build has a fixed value for the least significant data byte of the MFH image version number item.

Title	8MB Manufacture binary created by EDKII standalone build has a fixed value for the least significant data byte of the MFH image version number item.
Id	80328
Implication	EDKII platform .fdf build file contains a Master Flash Header (MFH) data block. One of the items (MFH item id 0x19) is the gobal image version number. The data for this item consists of four bytes. In usual interpretation these four bytes specify the Quark BSP source release used to build the Spi flash image with one byte identifying the release candidate number. For standalone EDKII builds the release candidate byte is always the value 0x99 and not the real value. Customers modifying source code and building their own releases must design their own versioning scheme as well; the Intel one is only provided as a reference example.
Workaround	

2.38 80408 - Serial terminal to FDTI header may boot pause

Title	Serial terminal to FDTI header may boot pause
Id	80408

2.38 80408 - Serial terminal to FDTI header may boot pause

Implication	During boot, characters on serial cable may cause the boot process to boot. Problem appears rarely and when it does boot can be progressed by hitting any key. Problem is not present if serial console is not open in host pc or serial cable is not connected. Normal prompts to select recovery are not compromised by this workaround.
Workaround	Do not attach serial cable in production environments to an open console during boot. Or if problem does occur, hit return for boot to continue.

2.39 80428 - Capsules created by the ""Building the EDKII Firmware"" of the Quark BSP Build and Software User Guide do not contain Spi Image Version.

Title	Capsules created by the ""Building the EDKII Firmware"" of the Quark BSP Build and Software User Guide do not contain Spi Image Version.
Id	80428
Implication	Capsules created the ""Building the EDKII Firmware"" of the Quark BSP Build and Software User Guide do not contain Spi Image Version. Boards updated with these capsules will still show original Spi Image Version and non EDKII flash assets will remain intact. The Single Image Version value stored in Spi Flash is not sufficient to support capsules that only do a partial update of Spi Flash.
Workaround	None.

2.40 81395 - meta-quark SD image fails to build due to x264 git history rewritten by Videolan project

Title	meta-quark SD image fails to build due to x264 git history rewritten by Videolan project
Id	81395
Implication	Building meta-quark fails with the following error: ERROR: Function failed: Fetcher failure: Fetch command failed with exit code 128, output: fatal: reference is not a tree: 1cffe9f406cc54f4759fc9eeb85598fb8cae66c7 This happens because the Videolan project has rewritten the history of the official x264 git repo, changing all the git revision numbers (SHA1s) (Glaser rewrite)
Workaround	Run the following command just before running your first bitbake command: mkdir -p meta-clanton-distro/recipes-multimedia/x264 printf '%s\n' 'SRCREV=""bfed708c5358a2b4ef65923fb0683cefa9184e6f""' > meta-clanton-distro/recipes-multimedia/x264/x264_git.bbappend This will override the git version that the x264 project deleted from their history with a new and equivalent one.

2.41 81508 - Illegal (AES) instruction reported in libgcrypt used by wpa_supplicant

Title	Illegal (AES) instruction reported in libgcrypt used by wpa_supplicant
Id	81508

2.41 81508 - Illegal (AES) instruction reported in libgcrypt used by wpa_supplicant

Implication	The libgcrypt build config files systematically produce AES-NI/PADLOCK x86 instructions in object code, even on CPUs that do not support them, such as Intel(r) Quark(tm) SoCs. This causes "illegal instruction" crashes in software when using this library for certain functionality, wpa_supplicant for example.
Workaround	Before you run your first bitbake command, create a file: meta-clanton-bsp/recipes-support/libgcrypt/libgcrypt_1.5.0.bbappend with content: EXTRA_OECONF += "" --disable-aesni-support --disable-padlock-support"" This can be done with the following two commands: mkdir -p meta-clanton-bsp/recipes-support/libgcrypt/ printf '%s\n' 'EXTRA_OECONF += "" --disable-aesni-support --disable-padlock-support""' > meta-clanton-bsp/recipes-support/libgcrypt/libgcrypt_1.5.0.bbappend

3.0 Resolved Issues

This section lists issues in the entire Intel® Quark™ SoC X1000 Software Release 1.0.1 resolved since package version 1.0.0. Updates coinciding with the EDKII 1.0.2 Update release are shown with changebars.

Table 4. Resolved Issue Summary

3.1 38542 - SPI flash tool / signing tools does not support multiple inclusions of same binary at different addresses

Title	SPI flash tool / signing tools does not support multiple inclusions of same binary at different addresses
Id	38542
Implication	When building an image using a layout.conf file that uses the same 'item_file' source in two (or more) asset descriptor blocks, the expected behavior is as follows: 1. Image is generated. 2. Two assets exist at different locations, with identical body data. 3. Even though the bodies of both assets contain identical data, the RSA signature section of each asset should contain different signatures, due to the intentionally non-deterministic nature of the signing process. What actually happens: All assets will be duplicates of the last asset listed in layout.conf, including RSA signatures and any other variables such as SVN indices. If, for example, 3 assets use the same 'item_file' source, and have SVN indices of 1, 2, and 3 respectively in layout.conf, and the one with SVN index 3 is the last one listed in layout.conf, then the other two assets that use this same 'item_file' source will also have an SVN index of 3, as well as identical RSA signatures.
Resolution	Resolved in release 1.0.1. This use case is detected and a meaningful error message explains it is not supported.

3.2 71061 - Linux boot failure on failure to remap PCIe MMIO region (256MB) from physical to virtual addressing (Sheet 1 of 2)

Title	Linux boot failure on failure to remap PCIe MMIO region (256MB) from physical to virtual addressing
Id	71061

3.2 71061 - Linux boot failure on failure to remap PCIe MMIO region (256MB) from physical to virtual addressing (Sheet 2 of 2)

Implication	V1.0.0 firmware required the operating system to map PCI express MMIO space from physical to virtual address. However, in the 1.0.0 release, the kernel called UEFI runtime service SetVirtualAddressMap() without PCI express MMIO space being mapped to virtual addresses. The impact was the system would reboot in Recovery mode earlier in kernel boot.
Resolution	Resolved in release 1.0.1.

3.3 71538 - Linux segfault when using lock prefix instruction under specific circumstances

Title	Linux segfault when using lock prefix instruction under specific circumstances
Id	71538
Implication	When a memory instruction with LOCK prefix executes and if it encounters a page fault (#PF), the state of the CPU could potentially get corrupted. Software should avoid using the LOCK prefix for instructions that may cause page fault (#PF).
Resolution	Resolved in release 1.0.1. Due to the LOCK prefix core silicon errata, the Yocto software release has patched the GNU assembler to remove LOCK instructions from code generated by the GNU toolchain. The workaround is enabled by default and no option has to be specified. All code is compiled with the workaround applied, so no binaries or libraries will include the LOCK prefix. The toolchain workaround can be verified to be in the toolchain by issuing the GNU assembler command: > as --help The help text will show the option: -mquark-strip-lock=[yes|no] strip all lock prefixes; default is yes The workaround can be explicitly set/cleared from gcc compiler using the command: gcc –Xassembler -mquark-strip-lock=[yes|no]

3.4 73384 - IRQ unhandled exception occurs when running sketch

Title	IRQ unhandled exception occurs when running sketch
Id	73384
Implication	When running sketch on Galileo board, an IRQ error occurs. Sometimes it stops with IRQ40, other times the sketch simply stops executing, leaving GPIOs stuck in whatever state they were in. The last instance, the LED was frozen on my number counter (1 digit lit). Root was available on serial console and no errors or messages in the system log.
Resolution	Resolved in release 1.0.1. Modified gadget driver (udc_pch.c) with additional logic to the pch_udc ISR for IRQ_NONE conditions to cater for valid handled interrupts (IRQ_HANDLED).

3.5 74073 - System hangs before system bootloader / payload is executed

Title	System hangs before system bootloader / payload is executed
Id	74073
Implication	If the EDKII "MemoryConfig" boot services variable is corrupted or overridden, the system bootloader / payload will not be executed. On Quark base SKU systems, the user will also notice that EDKII boot menu will not be displayed.
Resolution	Resolved in release 1.0.1.

3.6 75904 - OpenSSL version affected by 'heartbleed' defect

Title	OpenSSL version affected by 'heartbleed' defect
Id	75904
Implication	A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server. Documented here: https://www.openssl.org/news/secadv_20140407.txt
Resolution	Resolved in release 1.0.1. The OpenSSL recipe was updated to download and build a fixed version of OpenSSL.

§ §