VX3035 Hardware API

Product: VX3035

Revision: 4e

Internal Project Number: PJ10003

SAP Cost Unit: 40 VPX VX3035

Date: July 11, 2013

Location: Toulon of Kontron KOM-SA Division

Signature of R&D Director
or designated representative

Signature of originator of MRD
or designated representative

Additional signatures may be added, if required by entity

1 REVISION HISTORY

Date	Re-vision	Author	Affected chapters	Comments
June 6, 2012	0e	ST	Creation	Document frame
June 28, 2012	1e	FBO	First Release	
Aug 28, 2012	2e	FBO		Update according to Alstom peer review (CF_FT DT 942-1e-PC-Kontron-300712)
			6.1	Block diagram updated (Remark n°1)
			17.1	Offset error corrected (Remark n° 3)
			17.2.11	SMI information removed since not used (Remark n°2). Note: SMI into CPLD have no relationship with Software Management Interrupt (SMI)
			7.2.2	Comment added for MSR 0x35 difference (Remark n°4)
			7.3	Chapter added related to hyperthreading (Remark n°4)
			8.2	Information added related to ECC and ECC errors injection (Remark n°5), reference to Intel documents as well.
July 2, 2013	3e	FBO	10.2	Add description of TOM register for Max memory
			8.6	Add chapter 8.6 => consideration on TSC, HPET and APIC timer
			9.3	Add AMT consideration on VX3035
			17	Update CPLD Description for registers 0x3, 0x4, 0x15 (Note), 0x34, 0x56, 0x5B, 0x70, 0x73 This is an upgrade from Kontron Internal documentation FT.SF.212-11e (2012-06-15) to FT.SF.212-13e (2012-12-04)
			7.2.2	Introduce BIOS ID13127/ new SETUP and corresponding MSR values.
July 11, 2013	4e	FBO	7.2.2	Add VPX Resets output [Enabled] for BIOS ID13127 SETUP description. MSR 0x285 and 0x286 description modified and extended to MSR 280 – 286. MSR 0x285 0x286 set to 0 in MSR dump for BIOS ID13127 (power on value) MSR 0x1b2 added in comparaison table because this MSR must not be checked.
			17	CPLD specifications for CORE I7 projects, ref FT.SF.212 now in Rev 14e

2 SCOPE

This document is the hardware API of the VX3035 SBC board. It describes the general architecture and memory mapping of the card after the BIOS has been run.

References are made to circuit manufacturer documents explaining the internal registers of the devices used on this board. The associated levels of confidentiality of those documents are defined. For those registers requiring an initialization differing from the Intel reference evaluation board, due to actual VX3035 card implementation of the chipset, a detail description of the required initialization is provided.

3 ABBREVIATIONS

- API: Application programming Interface
- BIOS: Basic Input Output System
- CPLD: Complex Programmable Logic Device
- CPU: Central Processing Unit
- CRB: Customer Reference Board
- EDS: External Design Specification
- IA: Intel Architecture
- ME: Management Engine
- MSR: Machine Specific Register
- NDA: Non Disclosure Agreement
- PCH: Platform Controller HUB

4 DOCUMENT CONFIDENTIALITY CLASSIFICATION

The documents needed to describe to VX3035 registers are classified into 4 categories of confidentiality:

- NoNDA : Public
- NDA0 : NDA required with KOM-SA
- NDA1 : NDA « Intel Confidential » , « Greenliant confidential » or « Marvell confidential »
- NDA2 : NDA Intel « Restricted Secret »

This document is NDA0.

5 ASSOCIATED DOCUMENTS

- Cougar Canyon CRB, Huron River Embedded Mobile Platform, User's Guide November 2010 Revision 0.9 #457573, status NDA1
- VX3035 User's Guide CA.DT.A95 NoNDA

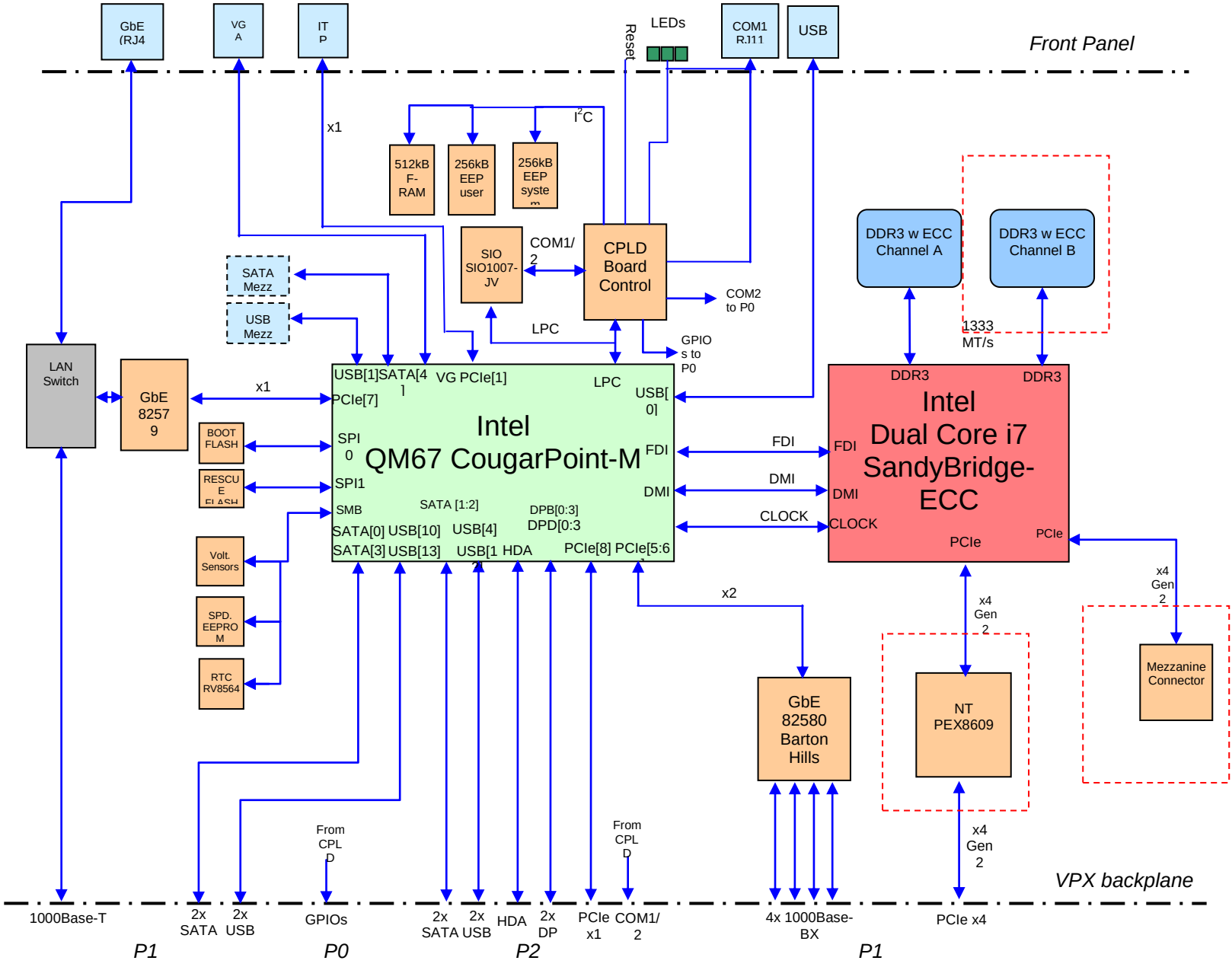
6 ARCHITECTURE OVERVIEW OF THE VX3035

This chapter describes the global architecture of the VX3035 CPU Board.

6.1 VX3035 Functional block diagram

The following image gives the VX3035 Functional block. Refer to VX3035 User's Guide for a full hardware detailed description with the list of features.

Note: Red dash rectangles indicate component presence is dependant of the board options



6.2 VX3035 SETUP

The considered VX3035 has the following SETUP characteristic

- Memory Channel B: DIMM Disabled. So 2 GB of RAM are available
- VPX switch 8609 set to Reset or not equipped
- C State Disabled
- CPU Freq set to 1.6 GHz
- Turbo mode disabled

All included registers dump on VX3035 are done in this configuration.

7 CPU REGISTERS

7.1 Reference documentation for CPU registers

CPU registers are described in the following manuals:

- MSR (Machine Specific Registers): Intel document 64-IA-32-Architecture Software Developper Manual, #325462 May2012 (4175 pages), status NoNDA. These registers are either MSR-IA32 or MSR-Core2 and are described vol C, chapter 34.
- IMC (Integrated Memory Controller): Intel Document CPU_SandyBridge_EDS_Vol2_July 2011 #445465 (302 pages) Chapter 2.13 to 2.16, status NDA2. These registers are dedicated to the DRAM memory controller integrated into the CPU.
- Registers EDS (External Design Specification): External Design Specification #445465 volume 2/2, Revision 2.2, July 2011, status NDA1. This document describes the processor configuration registers.

7.2 Registers dependant on VX3035 architecture implementation

This chapter describes the CPU specific register settings which are dependent on the architecture implementation at the card level and differ from the standard Intel evaluation board.

7.2.1 Modifications for VX3035

Kontron modifications are related to

- Management of CPU frequency
- CPU alarm setup module to enable/disable system shutdown if alerts occur
- Enable Thermal Reporting for MCH, CPU, PCH

7.2.2 Differences in MSR CPU register

➢ VX3035 With BIOS ID12171

Here are the MSR values for VX3035 ECL10000 on BIOS ID12171 (with SETUP modified as indicated in chapter 6.2). Values are obtained using Intel Implementation Test Suite (BITS)

```
BIOS Implementation Test Suite (BITS)
bits-750, build ID 929bc206ff340a9811ad631646ac6e85959be3de

Processor signature 0x206a7, detected CPU as Sandy Bridge
SMBIOS information:
0: BIOS vendor 'American Megatrends Inc.' version 'ID12171' date '06/19/2012'
1: System manufacturer 'Kontron' product 'VX3035' version 'EC10000_0184302001000000
'
==== MSR consistency test ====
  MSR 0x6: 0x40
  MSR 0x17: 0x10000000000000
  MSR 0x1b: 0xfee00800
  MSR 0x2a: 0x0
  MSR 0x2e: 0x0
  MSR 0x33: 0x0
  MSR 0x35: 0x20004
  MSR 0x3a: 0x5
  MSR 0x3e: 0x0
  MSR 0x8b: 0x1800000000
  MSR 0x9b: 0x0
  MSR 0xc1: 0x0
```

```
MSR 0xc2: 0x0
MSR 0xc3: 0x0
MSR 0xc4: 0x0
MSR 0xce: 0x80068011600
MSR 0xe2: 0x8400
MSR 0xe4: 0x20414
MSR 0xfe: 0xd0a
MSR 0x132: 0xffffffffffffffff
MSR 0x133: 0xffffffffffffffff
MSR 0x134: 0xffffffffffffffff
MSR 0x13c: 0x0
MSR 0x174: 0x0
MSR 0x175: 0x0
MSR 0x176: 0x0
MSR 0x179: 0xc07
MSR 0x17a: 0x0
MSR 0x186: 0x0
MSR 0x187: 0x0
MSR 0x188: 0x0
MSR 0x189: 0x0
MSR 0x194: 0x10000
MSR 0x19a: 0x0
MSR 0x19b: 0x0
MSR 0x19d: 0x0
MSR 0x1a0: 0x4000850089
MSR 0x1a2: 0x640e00
MSR 0x1a4: 0x0
MSR 0x1a6: 0x0
MSR 0x1a7: 0x0
MSR 0x1a8: 0x0
MSR 0x1aa: 0x400000
MSR 0x1ad: 0x1919191d
MSR 0x1b0: 0x0
MSR 0x1b1: 0x883d0100
MSR 0x1b2: 0xcbb700
MSR 0x1c6: 0x3
MSR 0x1c8: 0x0
MSR 0x1d9: 0x0
MSR 0x1db: 0x0
MSR 0x1dc: 0x0
MSR 0x1e1: 0x1
MSR 0x1f0: 0x74
MSR 0x1f2: 0x7b000006
MSR 0x1f3: 0xff800800
MSR 0x1fc: 0x40045
MSR 0x200: 0x6
MSR 0x201: 0xf80000800
MSR 0x202: 0x7c000000
MSR 0x203: 0xffc000800
MSR 0x204: 0x7b000000
MSR 0x205: 0xfff000800
MSR 0x206: 0x100000006
MSR 0x207: 0xfff800800
MSR 0x208: 0x100600000
MSR 0x209: 0xfffe00800
MSR 0x20a: 0xffe00005
MSR 0x20b: 0xfffe00800
MSR 0x20c: 0x0
MSR 0x20d: 0x0
MSR 0x20e: 0x0
```

```
MSR 0x20f: 0x0
MSR 0x210: 0x0
MSR 0x211: 0x0
MSR 0x212: 0x0
MSR 0x213: 0x0
MSR 0x250: 0x6060606060606060
MSR 0x258: 0x6060606060606060
MSR 0x259: 0x0
MSR 0x268: 0x5050505050505050
MSR 0x269: 0x5050505050505050
MSR 0x26a: 0x0
MSR 0x26b: 0x0
MSR 0x26c: 0x0
MSR 0x26d: 0x5050505050505050
MSR 0x26e: 0x5050505050505050
MSR 0x26f: 0x5050505050505050
MSR 0x277: 0x7040600070406
MSR 0x280: 0x0
MSR 0x281: 0x0
MSR 0x282: 0x0
MSR 0x283: 0x0
MSR 0x284: 0x0
MSR 0x285: 0x0
MSR 0x286: 0x0
MSR 0x2e0: 0x0
MSR 0x2e7: 0x1
MSR 0x2ff: 0xc00
MSR 0x305: 0x0
MSR 0x345: 0x31c3
MSR 0x38d: 0x0
MSR 0x38e: 0x8000000000000000
MSR 0x38f: 0xf
MSR 0x390: 0x0
MSR 0x391: 0x0
MSR 0x392: 0x0
MSR 0x393: 0x0
MSR 0x394: 0x0
MSR 0x395: 0x0
MSR 0x396: 0x3
MSR 0x397: 0x0
MSR 0x3b0: 0x0
MSR 0x3b1: 0x0
MSR 0x3b2: 0x0
MSR 0x3b3: 0x0
MSR 0x3f1: 0x0
MSR 0x3f6: 0xffff
MSR 0x400: 0x1f
MSR 0x401: 0x0
MSR 0x402: 0x0
MSR 0x403: 0x0
MSR 0x404: 0x3
MSR 0x405: 0x980000000000000
MSR 0x406: 0x0
MSR 0x407: 0x86
MSR 0x408: 0x3
MSR 0x409: 0x0
MSR 0x40c: 0x7
MSR 0x40d: 0x0
MSR 0x40e: 0x0
MSR 0x40f: 0x0
```

```
MSR 0x410: 0x7
MSR 0x411: 0x0
MSR 0x414: 0x3f
MSR 0x415: 0x20000000000000
MSR 0x416: 0xfef97fc0
MSR 0x417: 0x5040000086
MSR 0x418: 0x3f
MSR 0x419: 0x20000000000000
MSR 0x41a: 0xfef97f80
MSR 0x41b: 0x1040000086
MSR 0x480: 0xda040000000010
MSR 0x481: 0x7f00000016
MSR 0x482: 0xfff9fffe0401e172
MSR 0x483: 0x7fffff00036dff
MSR 0x484: 0xffff000011ff
MSR 0x485: 0x100401e5
MSR 0x486: 0x80000021
MSR 0x487: 0xffffffff
MSR 0x488: 0x2000
MSR 0x489: 0x667ff
MSR 0x48a: 0x2a
MSR 0x48b: 0xff00000000
MSR 0x48c: 0xf0106114141
MSR 0x48d: 0x7f00000016
MSR 0x48e: 0xfff9fffe04006172
MSR 0x48f: 0x7fffff00036dfb
MSR 0x490: 0xffff000011fb
MSR 0x4c1: 0x0
MSR 0x4c2: 0x0
MSR 0x4c3: 0x0
MSR 0x4c4: 0x0
MSR 0x502: 0x0
MSR 0x600: 0x0
MSR 0x601: 0x1814149480000380
MSR 0x602: 0x1814149480000118
MSR 0x603: 0x80303030
MSR 0x604: 0x80646464
MSR 0x606: 0xa1003
MSR 0x609: 0x0
MSR 0x60a: 0x889c
MSR 0x60b: 0x88b5
MSR 0x60c: 0x88c7
MSR 0x610: 0x80fa001480c8
MSR 0x614: 0xf010000c000c8
MSR 0x638: 0x0
MSR 0x63a: 0x0
MSR 0x640: 0x0
MSR 0x642: 0x10
MSR 0x6e0: 0x0
MSR 0x700: 0x0
MSR 0x701: 0x0
MSR 0x702: 0x0
MSR 0x703: 0x0
MSR 0x704: 0x0
MSR 0x705: 0x0
MSR 0x706: 0x0
MSR 0x707: 0x0
MSR 0x708: 0x0
MSR 0x709: 0x0
MSR 0x710: 0x0
```

```
MSR 0x711: 0x0
MSR 0x712: 0x0
MSR 0x713: 0x0
MSR 0x714: 0x0
MSR 0x715: 0x0
MSR 0x716: 0x0
MSR 0x717: 0x0
MSR 0x718: 0x0
MSR 0x719: 0x0
MSR 0x720: 0x0
MSR 0x721: 0x0
MSR 0x722: 0x0
MSR 0x723: 0x0
MSR 0x724: 0x0
MSR 0x725: 0x0
MSR 0x726: 0x0
MSR 0x727: 0x0
MSR 0x728: 0x0
MSR 0x729: 0x0
MSR 0xc0000080: 0x0
MSR 0xc0000081: 0x0
MSR 0xc0000082: 0x0
MSR 0xc0000083: 0x0
MSR 0xc0000084: 0x20200
MSR 0xc0000100: 0x0
MSR 0xc0000101: 0x0
MSR 0xc0000102: 0x0
MSR 0xc0000103: 0x0
```

The following MSR are excluded from dumping because they are no part of the initialization (most of them are counters or recording registers)

```
    0x0,        # IA32_P5_MC_ADDR
    0x1,        # IA32_P5_MC_TYPE
    0x10,       # IA32_TIME_STAMP_COUNTER
    0x34,       # MSR_SMI_COUNT
    0x39,
    0xE7,       # IA32_MPERF
    0xE8,       # IA32_APERF
    0x198,      # MSR_PERF_STATUS
    0x199,      # IA32_PERF_CTL
    0x19c,      # IA32_THERM_STATUS
    0x1c9,      # MSR_LASTBRANCH_TOS
    0x1dd,      # MSR_LER_FROM_LIP
    0x1de,      # MSR_LER_TO_LIP
    0x1f4,
    0x1f5,
    0x309,      # IA32_FIXED_CTR0
    0x30A,      # IA32_FIXED_CTR1
    0x30B,      # IA32_FIXED_CTR2
    0x3f8,      # Package C-state residency
    0x3f9,      # Package C-state residency
    0x3fa,      # Package C-state residency
    0x3fc,      # Core C-state residency
    0x3fd,      # Core C-state residency
    0x3fe,      # Core C-state residency
    0x60d,      # MSR_PKG_C2_RESIDENCY
    0x611,      # MSR_PKG_ENERGY_STATUS
    0x613,
```

```
    0x639,      # MSR_PP0_ENERGY_STATUS
    0x641,
    0x680,      # MSR_LAST_BRANCH_0_FROM_IP
    0x681,      # MSR_LAST_BRANCH_1_FROM_IP
    0x682,      # MSR_LAST_BRANCH_2_FROM_IP
    0x683,      # MSR_LAST_BRANCH_3_FROM_IP
    0x684,      # MSR_LAST_BRANCH_4_FROM_IP
    0x685,      # MSR_LAST_BRANCH_5_FROM_IP
    0x686,      # MSR_LAST_BRANCH_6_FROM_IP
    0x687,      # MSR_LAST_BRANCH_7_FROM_IP
    0x688,      # MSR_LAST_BRANCH_8_FROM_IP
    0x689,      # MSR_LAST_BRANCH_9_FROM_IP
    0x68a,      # MSR_LAST_BRANCH_A_FROM_IP
    0x68b,      # MSR_LAST_BRANCH_B_FROM_IP
    0x68c,      # MSR_LAST_BRANCH_C_FROM_IP
    0x68d,      # MSR_LAST_BRANCH_D_FROM_IP
    0x68e,      # MSR_LAST_BRANCH_E_FROM_IP
    0x68f,      # MSR_LAST_BRANCH_F_FROM_IP
    0x6c0,      # MSR_LAST_BRANCH_0_TO_LIP
    0x6c1,      # MSR_LAST_BRANCH_1_TO_LIP
    0x6c2,      # MSR_LAST_BRANCH_2_TO_LIP
    0x6c3,      # MSR_LAST_BRANCH_3_TO_LIP
    0x6c4,      # MSR_LAST_BRANCH_4_TO_LIP
    0x6c5,      # MSR_LAST_BRANCH_5_TO_LIP
    0x6c6,      # MSR_LAST_BRANCH_6_TO_LIP
    0x6c7,      # MSR_LAST_BRANCH_7_TO_LIP
    0x6c8,      # MSR_LAST_BRANCH_8_TO_LIP
    0x6c9,      # MSR_LAST_BRANCH_9_TO_LIP
    0x6ca,      # MSR_LAST_BRANCH_A_TO_LIP
    0x6cb,      # MSR_LAST_BRANCH_B_TO_LIP
    0x6cc,      # MSR_LAST_BRANCH_C_TO_LIP
    0x6cd,      # MSR_LAST_BRANCH_D_TO_LIP
    0x6ce,      # MSR_LAST_BRANCH_E_TO_LIP
    0x6cf,      # MSR_LAST_BRANCH_F_TO_LIP
```

The MSR differences with the Cougar Canyon CRB, Huron River Embedded Mobile reference Platform and VX3035 BIOS ID12171 (with SETUP modified as indicated in chapter 6.2) are the following:

MSR	Ref Platform	VX3035	Comment
MSR 0x35	0x20002	0x20004	The ref platform has hyper-threading disabled (2 threads) and VX3035 has hyper-threading enabled (4 threads) by default.
MSR 0x3a	0x1	0x5	IA32_FEATURE_CONTROL bit 2: VX3035 enable VMX
MSR 0x8b	0x900000000	0x1800000000	Microcode update signature
MSR 0xce	0x80068010e00	0x80068011600	MSR_PLATFORM_INFO Bits 15-8: Maximum Non-Turbo Ratio. (R/O) This is the ratio of the frequency that invariant TSC runs at.

MSR	Ref Platform	VX3035	Comment
MSR 0xe2	0x6000404	0x8400	MSR_PKG_CST_CONFIG_CONTROL Bit 2: Package C-State limit. (R/W) is C7 Bit 15: CFG Lock. (R/WO) When set, lock bits 15:0 of this register until next reset. Bit 24: Interrupt filtering enable. (R/W) When 0, all processor cores in a deep C-State will wake for an event message. Bit 26: C1 state auto demotion enable. (R/W)
MSR 0x194	0x10e00	0x10000	MSR_MCG_R12
MSR 0x19a	No MSR	0x0	IA32_CLOCK_MODULATION Clock Modulation Control
MSR 0x19b	No MSR	0x0	IA32_THERM_INTERRUPT Thermal Interrupt Control
MSR 0x19d	No MSR	0x0	MSR_THERM2_CTL
MSR 0x1a0	0x850089	0x4000850089	IA32_MISC_ENABLE Bit 38 reserved
MSR 0x1ad	0x17171718	0x1919191d	MSR_TURBO_POWER_CURRENT_LIMIT Bits 14-0: TDP Limit (R/W) Watt granularity Bits 30-16: TDC Limit (R/W) Amp. granularity
MSR 0x1b1	0x88350000	0x883d0100	IA32_PACKAGE_THERM_STATUS Bit 8: Pkg Thermal Threshold #2 Status (RO) Bit 19: Pkg Digital Readout (RO)
MSR 0x1b2	0x0	0xcbb700	IA32_PACKAGE_THERM_INTERRUPT Bits > 24 Reserved
MSR 0x1e1	No MSR	0x1	MSR not in Intel documentation
MSR 0x1f2	0xab000006	0x7b000006	IA32_SMRR_PHYSBASE Base address of SMM memory range.
MSR 0x1fc	0x4005f	0x40045	MSR_POWER_CTL bit 1: C1E Enable. (R/W). Set to 0 to disable Intel Speed Step bits 63-2: reserved
MSR 0x202	0x80000006	0x7c000000	IA32_MTRR_PHYSBASE1
MSR 0x203	0xfe0000800	0xffc000800	IA32_MTRR_PHYSMASK1
MSR 0x204	0xa0000006	0x7b000000	IA32_MTRR_PHYSBASE2
MSR 0x205	0xff8000800	0xfff000800	IA32_MTRR_PHYSMASK2
MSR 0x206	0xa8000006	0x100000006	IA32_MTRR_PHYSBASE3
MSR 0x207	0xffc000800	0xfff800800	IA32_MTRR_PHYSMASK3
MSR 0x208	0xab000000	0x100600000	IA32_MTRR_PHYSBASE4
MSR 0x209	0xfff000800	0xfffe00800	IA32_MTRR_PHYSMASK4
MSR 0x20a	0x100000006	0xffe00005	IA32_MTRR_PHYSBASE5
MSR 0x20b	0xfc0000800	0xfffe00800	IA32_MTRR_PHYSMASK5

MSR	Ref Platform	VX3035	Comment
MSR 0x20c	0x140000006	0x0	IA32_MTRR_PHYSBASE6
MSR 0x20d	0xff0000800	0x0	IA32_MTRR_PHYSMASK6
MSR 0x20e	0x14fe00000	0x0	IA32_MTRR_PHYSBASE7
MSR 0x20f	0xfffe00800	0x0	IA32_MTRR_PHYSMASK7
MSR 0x38f	0xff	0xf	IA32_PERF_GLOBAL_CTRL (MSR_PERF_GLOBAL_CTRL) Bits 4-7 Reserved
MSR 0x417	0x1040000086	0x5040000086	IA32_MC5_MISC (bits 63:9): Not architecturally defined
MSR 0x485	0x401e5	0x100401e5	IA32_VMX_MISC If bit 28 is read as 1, bit 2 of the IA32_SMM_MONITOR_CTL can be set to 1. VMXOFF unblocks SMIs unless IA32_SMM_MONITOR_CTL[bit 2] is 1
MSR 0x601	0x181414948000030c	0x1814149480000380	MSR not in Intel documentation 0x600 is Debug Store
MSR 0x602	0x1814149480000104	0x1814149480000118	MSR not in Intel documentation
MSR 0x603	0x804c4c4c	0x80303030	MSR not in Intel documentation
MSR 0x604	0x80747474	0x80646464	MSR not in Intel documentation
MSR 0x609	0x100	0x0	MSR not in Intel documentation
MSR 0x60a	0x8c02	0x889c	MSR_PKGC3_IRTL Bits 9-0: Interrupt response time limit. (R/W) Bits 12-10: Time Unit. (R/W)
MSR 0x60b	0x8854	0x88b5	MSR_PKGC6_IRTL Bits 9-0 Interrupt response time limit. (R/W)
MSR 0x60c	0x8854	0x88c7	MSR_PKGC7_IRTL Bits 9-0 Interrupt response time limit. (R/W)
MSR 0x610	0x80a800dc8088	0x80fa001480c8	MSR_PKG_RAPL_POWER_LIMIT bits:14:0 Package Power Limit bits 23-17: Time Window for Power Limit #1 bits 46:32: Package Power Limit#2
MSR 0x614	0x1000c000800088	0xf010000c000c8	MSR_PKG_POWER_INFO bits 14-0: Thermal Spec Power bits 30-16: Minimum Power bits 46-32: Maximum Power bits 53-48:Maximum Time Window

Note: the Cougar Canyon CRB, Huron River Embedded Mobile Platform has a Processor signature 0x206a3 while the VX3035 has Processor signature 0x206a7.

- VX3035 with BIOS ID13127

The BIOS 13127 is considered with the following SETUP modifications:

- Intel SpeedStep [Disabled]
- CState [Disabled]
- Hyperthreading [Disabled]
- CPU frequency [1600MHz]
- Internal SPD [Enabled] -> Memory Frequency [1333MHz]
- Boot device order: [EFI Shell]/[USB]/[Sata Flash]
- VPX Resets output [Enabled]

Here are the MSR values for VX3035 on BIOS ID13127 with above modified SETUP value. Values are obtained using Intel Implementation Test Suite (BITS)

```
MSR 0x6: 0x40
MSR 0x17: 0x10000000000000
MSR 0x1b: 0xfee00800
MSR 0x2a: 0x0
MSR 0x2e: 0x0
MSR 0x33: 0x0
MSR 0x35: 0x20002
MSR 0x3a: 0x5
MSR 0x3e: 0x0
MSR 0x8b: 0x1800000000
MSR 0x9b: 0x0
MSR 0xc1: 0x0
MSR 0xc2: 0x0
MSR 0xc3: 0x0
MSR 0xc4: 0x0
MSR 0xce: 0x80060011600
MSR 0xe2: 0x8400
MSR 0xe4: 0x20414
MSR 0xfe: 0xd0a
MSR 0x132: 0xffffffffffffffff
MSR 0x133: 0xffffffffffffffff
MSR 0x134: 0xffffffffffffffff
MSR 0x13c: 0x0
MSR 0x174: 0x0
MSR 0x175: 0x0
MSR 0x176: 0x0
MSR 0x179: 0xc07
MSR 0x17a: 0x0
MSR 0x186: 0x0
MSR 0x187: 0x0
MSR 0x188: 0x0
MSR 0x189: 0x0
MSR 0x194: 0x10000
MSR 0x19a: 0x0
MSR 0x19b: 0x0
MSR 0x19d: 0x0
MSR 0x1a0: 0x4000840089
MSR 0x1a2: 0x640e00
MSR 0x1a4: 0x0
MSR 0x1a6: 0x0
```

```
MSR 0x1a7: 0x0
MSR 0x1a8: 0x0
MSR 0x1aa: 0x400000
MSR 0x1ad: 0x1919191d
MSR 0x1b0: 0x0
MSR 0x1b1: 0x88430100
MSR 0x1b2: 0xcbb700
MSR 0x1c6: 0x3
MSR 0x1c8: 0x0
MSR 0x1d9: 0x0
MSR 0x1db: 0x0
MSR 0x1dc: 0x0
MSR 0x1e1: 0x1
MSR 0x1f0: 0x74
MSR 0x1f2: 0x7b000006
MSR 0x1f3: 0xff800800
MSR 0x1fc: 0x40045
MSR 0x200: 0x6
MSR 0x201: 0xf80000800
MSR 0x202: 0x7c000000
MSR 0x203: 0xffc000800
MSR 0x204: 0x7b000000
MSR 0x205: 0xfff000800
MSR 0x206: 0x100000006
MSR 0x207: 0xfff800800
MSR 0x208: 0x100600000
MSR 0x209: 0xfffe00800
MSR 0x20a: 0xffe00005
MSR 0x20b: 0xfffe00800
MSR 0x20c: 0x0
MSR 0x20d: 0x0
MSR 0x20e: 0x0
MSR 0x20f: 0x0
MSR 0x210: 0x0
MSR 0x211: 0x0
MSR 0x212: 0x0
MSR 0x213: 0x0
MSR 0x250: 0x606060606060606
MSR 0x258: 0x606060606060606
MSR 0x259: 0x0
MSR 0x268: 0x505050505050505
MSR 0x269: 0x505050505050505
MSR 0x26a: 0x0
MSR 0x26b: 0x0
MSR 0x26c: 0x0
MSR 0x26d: 0x505050505050505
MSR 0x26e: 0x505050505050505
MSR 0x26f: 0x505050505050505
MSR 0x277: 0x7040600070406
MSR 0x280: 0x0
MSR 0x281: 0x0
MSR 0x282: 0x0
MSR 0x283: 0x0
MSR 0x284: 0x0
MSR 0x285: 0x0
MSR 0x286: 0x0
```

```
MSR 0x2e0: 0x0
MSR 0x2e7: 0x1
MSR 0x2ff: 0xc00
MSR 0x305: 0x0
MSR 0x345: 0x31c3
MSR 0x38d: 0x0
MSR 0x38e: 0x8000000000000000
MSR 0x38f: 0xff
MSR 0x390: 0x0
MSR 0x391: 0x0
MSR 0x392: 0x0
MSR 0x393: 0x0
MSR 0x394: 0x0
MSR 0x395: 0x0
MSR 0x396: 0x3
MSR 0x397: 0x0
MSR 0x3b0: 0x0
MSR 0x3b1: 0x0
MSR 0x3b2: 0x0
MSR 0x3b3: 0x0
MSR 0x3f1: 0x0
MSR 0x3f6: 0xffff
MSR 0x400: 0x1f
MSR 0x401: 0x0
MSR 0x402: 0x0
MSR 0x403: 0x0
MSR 0x404: 0x3
MSR 0x405: 0x980000000000000
MSR 0x406: 0x0
MSR 0x407: 0x86
MSR 0x408: 0x3
MSR 0x409: 0x0
MSR 0x40c: 0x7
MSR 0x40d: 0x0
MSR 0x40e: 0x0
MSR 0x40f: 0x0
MSR 0x410: 0x7
MSR 0x411: 0x0
MSR 0x414: 0x3f
MSR 0x415: 0x20000000000000
MSR 0x416: 0xfef97fc0
MSR 0x417: 0x5040000086
MSR 0x418: 0x3f
MSR 0x419: 0x20000000000000
MSR 0x41a: 0xfef97f80
MSR 0x41b: 0x1040000086
MSR 0x480: 0xda040000000010
MSR 0x481: 0x7f00000016
MSR 0x482: 0xfff9fffe0401e172
MSR 0x483: 0x7fffff00036dff
MSR 0x484: 0xffff000011ff
MSR 0x485: 0x100401e5
MSR 0x486: 0x80000021
MSR 0x487: 0xffffffff
MSR 0x488: 0x2000
MSR 0x489: 0x667ff
```

```
MSR 0x48a: 0x2a
MSR 0x48b: 0xff00000000
MSR 0x48c: 0xf0106114141
MSR 0x48d: 0x7f00000016
MSR 0x48e: 0xfff9fffe04006172
MSR 0x48f: 0x7fffff00036dfb
MSR 0x490: 0xffff000011fb
MSR 0x4c1: 0x0
MSR 0x4c2: 0x0
MSR 0x4c3: 0x0
MSR 0x4c4: 0x0
MSR 0x502: 0x0
MSR 0x600: 0x0
MSR 0x601: 0x181414948000030c
MSR 0x602: 0x1814149480000104
MSR 0x603: 0x804c4c4c
MSR 0x604: 0x80646464
MSR 0x606: 0xa1003
MSR 0x609: 0x0
MSR 0x60a: 0x889c
MSR 0x60b: 0x88b5
MSR 0x60c: 0x88c7
MSR 0x610: 0x80fa00dc80c8
MSR 0x614: 0xf010000c000c8
MSR 0x638: 0x0
MSR 0x63a: 0x0
MSR 0x640: 0x0
MSR 0x642: 0x10
MSR 0x6e0: 0x0
MSR 0x700: 0x0
MSR 0x701: 0x0
MSR 0x702: 0x0
MSR 0x703: 0x0
MSR 0x704: 0x0
MSR 0x705: 0x0
MSR 0x706: 0x0
MSR 0x707: 0x0
MSR 0x708: 0x0
MSR 0x709: 0x0
MSR 0x710: 0x0
MSR 0x711: 0x0
MSR 0x712: 0x0
MSR 0x713: 0x0
MSR 0x714: 0x0
MSR 0x715: 0x0
MSR 0x716: 0x0
MSR 0x717: 0x0
MSR 0x718: 0x0
MSR 0x719: 0x0
MSR 0x720: 0x0
MSR 0x721: 0x0
MSR 0x722: 0x0
MSR 0x723: 0x0
MSR 0x724: 0x0
MSR 0x725: 0x0
MSR 0x726: 0x0
```

```
MSR 0x727: 0x0
MSR 0x728: 0x0
MSR 0x729: 0x0
MSR 0xc0000080: 0x0
MSR 0xc0000081: 0x0
MSR 0xc0000082: 0x0
MSR 0xc0000083: 0x0
MSR 0xc0000084: 0x20200
MSR 0xc0000100: 0x0
MSR 0xc0000101: 0x0
MSR 0xc0000102: 0x0
MSR 0xc0000103: 0x0
```

The MSR differences between VX3035 BIOS ID13127 (with SETUP modified as indicated above) and with VX3035 BIOS ID12171 (with SETUP modified as indicated in chapter 6.2) are the following:

MSR	VX3035 BIOS ID13127	VX3035 BIOS ID12171	Comment
MSR 0x35	0x20002	0x20004	The VX3035 BIOS13127 has hyper-threading disabled (2 threads) and VX3035 BIOS 12171 has hyper-threading enabled (4 threads) by default.
MSR 0xce	0x80060011600	0x80068011600	bit27 : reserved. Seems to correspond to « CpuIsProduction » according to BIOS source code. This is not BIOS depending.
MSR 0x1a0	0x4000840089	0x4000850089	IA32_MISC_ENABLE Bit 16: Enhanced Intel SpeedStep Technology Enable (R/W). Change due to Enhanced Intel Speed Step now disabled with BIOS13127
MSR 0x1b1	0x88440100	0x883d0100	IA32_PACKAGE_THERM_STATUS Bit 22:16 = Package Digital Readout bits => Current package temperature is different Bits 22:16 should be ignored when checking this MSR !
MSR 0x1b2	0xcbb700 0xd5c100 Etc	0xcbb700	IA32_PACKAGE_THERM_INTERRUPT Bit 14 :8 Pkg Threshold #1 Value Bit 22 :16 Pkg Threshold #2 Value Threshold values are fixed by BIOS according to the current CPU temperature. This MSR must not be checked
MSR 0x280 to 0x286	0x0 at power on or Value set by OS software.	0x0	IA32_MCi_CTL2 i = 0..6 Bits 14 :0 Corrected error count threshold Bit 30: CMCI_EN Error Reporting Register Bank i Enabled i = 0..6 Warning: in case of software reset these MSR are not reset to 0x0. So the value cannot be guaranteed.

MSR	VX3035 BIOS ID13127	VX3035 BIOS ID12171	Comment
MSR 0x38F	0xFF	0xF	IA32_PERF_GLOBAL_CTRL (MSR_PERF_GLOBAL_CTRL) Bits 4:7 are Reserved But this is BIOS configuration depending. The value change from 0xF to 0xFF when hyperthreading is disabled. This is the case for BIOS 13127 configuration. 0xFF is the new reference.
MSR 0x601	0x1814149480000030c	0x1814149480000380	MSR not in Intel documentation According to BIOS code this is called PRIMARY_PLANE_CURRENT_CONFIG Change due to Enhanced Intel Speed Step now disabled with BIOS 13127
MSR 0x602	0x1814149480000104	0x1814149480000118	MSR not in Intel documentation According to BIOS source code SECONDARY_PLANE_CURRENT_CONFIG Change due to Enhanced Intel Speed Step now disabled with BIOS 13127
MSR 0x603	0x804C4C4C	0x80303030	MSR not in Intel documentation nor BIOS source code. This is not caused by BIOS version but by VX3035 version. 0x804c4c4c is the new reference.
MSR 0x610	0x80FA00DC80C8	0x80FA001480C8	MSR_PKG_RAPL_POWER_LIMIT bits:14:0 Package Power Limit bits 23-17: Time Window for Power Limit #1 bits 46:32: Package Power Limit#2 Difference in field: “Time window Power Limit #1” This change is caused by TURBO mode. TURBO mode is not disabled with BIOS 13127 because Intel Speed Step is disabled instead, 0x80fa00dc80c8 is the new reference value

7.3 Hyper-threading

Hyperthreading mechanism is described into Intel documentation:

- Intel Document CPU_SandyBridge_EDS_Vol1_Feb 2011 #445465 (194 pages) Chapter 3.3, status NDA2.

Hyper-threading can be disabled by SETUP. Hyper-threading enabling or disabling can also be verified using MSR 0x35. MSR is a 32 bits register. The first 16 bits (MSB) indicates the number of active cores while the last 16 bits (LSB) indicates the number of active threads.

Here is a code example to read MSR 0x35 information:

```
Data32 = (UINT32) ReadMsr (MSR_CORE_THREAD_COUNT);
NumberOfActiveCores   = (UINT32) ((Data32 >> 16) & 0xFFFF);
NumberOfActiveThreads = (UINT32) (Data32 & 0xFFFF);
```

Also under BIOS EFI shell prompt, MSR 0x35 can be checked with cpuutil command

When hyper-threading is enabled (number of threads is 4)
VX3035> cpuutil /msr 35
MSR In: ECX = 0x35
MSR Out: EDX:EAX = 0x2000**4**

When hyper-threading is disabled (number of threads is 2)
VX3035> cpuutil /msr 35
MSR In: ECX = 0x35
MSR Out: EDX:EAX = 0x2000**2**

8 SANDY BRIDGE CPU INTEGRATED DEVICES

This chapter lists and dumps the PCI configuration register of the devices Integrated into the Sandy Bridge.

8.1 Reference documentation for Integrated Device registers

Sandy Bridge Integrated Device registers are described in the following manuals:

- Intel Document CPU_SandyBridge_EDS_Vol2_July 2011 #445465 (302 pages) Chapter 2.13 to 2.16, status NDA2. These registers are dedicated to the DRAM memory controller integrated into the CPU.

Sandy Bridge Integrated devices are

- DRAM Controller
- PCI Express Controllers
- Integrated Graphics Device

8.2 Integrated DRAM Memory Controller (IMC)

The BIOS initialize the DDR3 according to the SPD table values read from the SPD EEPROM 0xA0 (and 0xA4 if present) located on SMBUS. Kontron programs this EEPROM by means of a BIOS command then the BIOS/Intel standard DDR3 initialization is performed. The DDR3 initialization is done once and must not be changed or performed again by any Operating System. Even after a system reset the DDR3 initialization is not performed again into the BIOS.

Note that ECC functionality is enabled by default on VX3035. ECC can be disabled by SETUP. ECC error injection is possible using the error injection register described in specific documentation:

- 494178_Gladden_SNB_IVB_ECC_Injection_R2_1_1.pdf April 2012 (24 pages), status NDA2
- 2ndGen_Intel_Core_ECC_syndrome_Table(Intel Format).pdf (2 pages), status NDA2

ECC registers offset are related to MCHBAR address which is 0xFED10000 on VX3035

8.3 DRAM Controller Configuration register (B0:D0:F0)

Here are the PCI Configuration Registers after the BIOS execution (when dumped in raw mode data are Big Endian and must swapped)

```
Device pci 00 00 00
  PCI Segment 00 Bus 00 Device 00 Func 00 [EFI 0000000000]
  00000000: 86 80 04 01 06 00 90 20-09 00 00 06 00 00 00 00  *....... ........*
  00000010: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 99 19  *................*
  00000030: 00 00 00 00 E0 00 00 00-00 00 00 00 00 00 00 00  *................*

  00000040: 01 90 D1 FE 00 00 00 00-01 00 D1 FE 00 00 00 00  *................*
  00000050: 11 02 00 00 1D 00 00 00-00 00 00 00 01 00 00 7B  *................*
  00000060: 05 00 00 F8 00 00 00 00-01 80 D1 FE 00 00 00 00  *................*
```

```
  00000070: 00 00 F0 FF 7F 00 00 00-00 04 00 00 00 00 00 00  *................*
  00000080: 10 11 11 00 00 00 11 00-1A 00 00 00 00 00 00 00  *................*
  00000090: 01 00 00 00 01 00 00 00-01 00 50 00 01 00 00 00  *..........P.....*
  000000A0: 01 00 00 80 00 00 00 00-01 00 60 00 01 00 00 00  *..........`.....*
  000000B0: 01 00 A0 7B 01 00 80 7B-01 00 00 7B 01 00 A0 7F  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 09 00 0C 01 96 61 00 C0-90 00 08 16 00 00 00 00  *.....a..........*
  000000F0: 00 00 00 00 00 00 00 00-B8 0F 06 00 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 0104

Command(4): 0006
  (00)I/O space access enabled:       0  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 2090
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      1  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          1
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     09                  BIST(0F):  Incapable
Cache Line Size(C): 00                  Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Bridge Device - Host/PCI bridge -
Base Address Registers(10):
  (None)
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      1999
Capabilities Ptr(34):        E0
Interrupt Line(3C):          00      Interrupt Pin(3D):       00
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

8.4 PCI Express Controller B0:D1:F0,F1

```
Device pci 00 01 00
  PCI Segment 00 Bus 00 Device 01 Func 00 [EFI 0000010000]
  00000000: 86 80 01 01 07 00 10 00-09 00 04 06 10 00 81 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 01 01 00 F0 00 00 00  *................*
  00000020: F0 FF 00 00 F1 FF 01 00-00 00 00 00 00 00 00 00  *................*
  00000030: 00 00 00 00 88 00 00 00-00 00 00 00 0B 01 10 00  *................*

  00000040: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 0A  *................*
  00000080: 01 90 03 C8 08 00 00 00-0D 80 00 00 86 80 99 19  *................*
  00000090: 05 A0 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 10 00 42 01 00 80 00 00-00 00 00 00 82 4C 21 02  *..B..........L!.*
  000000B0: 00 00 01 10 80 25 0C 00-00 00 00 00 00 00 00 00  *.....%..........*
  000000C0: 00 00 00 00 00 08 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 42 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *B...............*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 01 00-00 00 00 00 00 00 10 00  *................*

Vendor ID(0): 8086                    Device ID(2): 0101

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     09                  BIST(0F):  Incapable
Cache Line Size(C): 10                  Latency Timer(D): 00
Header Type(0E):    81, Multi-function, P2P bridge
Class: Bridge Device - PCI/PCI bridge -
Base Address Registers(10):  (None)
No Expansion ROM(38)

(Bus Numbers)  Primary(18)     Secondary(19)   Subordinate(1A)
               ----------------------------------------------------
               00               01              01
Secondary Latency Timer(1B):       00

Secondary Status(1E):    0
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Received System Error:          0  (15)Detected Parity Error:          0

Resource Type                          Base                    Limit
```

```
------------------------------------------------------------------------
I/O(1C)                             0000F000                 00000FFF
Memory(20)                          FFF00000                 000FFFFF
Prefetchable Memory(24)    00000000FFF00000         00000000000FFFFF

Capabilities Ptr(34):   88

Bridge Control(3E)     0010
  (00)Parity Error Response:          0  (01)SERR# Enable:                  0
  (02)ISA Enable:                     0  (03)VGA Enable:                   0
  (05)Master Abort Mode:              0  (06)Secondary Bus Reset:          0
  (07)Fast Back-to-Back Enable:       0  (08)Primary Discard Timer:      2^15
  (09)Secondary Discard Timer:     2^15  (10)Discard Timer Status:         0
  (11)Discard Timer SERR# Enable:     0

Interrupt Line(3C)      0B             Interrupt Pin(3D):       01

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    00  Cap Register( 2):   0142
  Device Capabilities( 4):  00008000
  Device Control( 8):       0000       Device Status( A):    0000
  Link Capabilities( C):    02214C82
  Link Control(10):         0000       Link Status(12):      1001
  Slot Capabilities(14):    000C2580
  Slot Control(18):         0000       Slot Status(1A):      0000
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

```
Device pci 00 01 01
  PCI Segment 00 Bus 00 Device 01 Func 01 [EFI 0000010100]
  00000000: 86 80 05 01 07 00 10 00-09 00 04 06 10 00 81 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 02 02 00 F0 00 00 00  *................*
  00000020: F0 FF 00 00 F1 FF 01 00-00 00 00 00 00 00 00 00  *................*
  00000030: 00 00 00 00 88 00 00 00-00 00 00 00 0B 01 10 00  *................*

  00000040: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 0A  *................*
  00000080: 01 90 03 C8 08 00 00 00-0D 80 00 00 86 80 10 20  *............... *
  00000090: 05 A0 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 10 00 42 01 00 80 00 00-00 00 00 00 82 4C 21 03  *..B..........L!.*
  000000B0: 00 00 01 10 80 25 14 00-00 00 00 00 00 00 00 00  *.....%..........*
  000000C0: 00 00 00 00 00 08 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 42 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *B...............*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 01 00-00 00 00 00 00 00 10 00  *................*

Vendor ID(0): 8086                  Device ID(2): 0105

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0
```

```
Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                 0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:      0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:         0
  (12)Received Target Abort:          0  (13)Received Master Abort:         0
  (14)Signaled System Error:          0  (15)Detected Parity Error:         0

Revision ID(8):     09                BIST(0F):  Incapable
Cache Line Size(C): 10                Latency Timer(D): 00
Header Type(0E):    81, Multi-function, P2P bridge
Class: Bridge Device - PCI/PCI bridge -
Base Address Registers(10):  (None)
No Expansion ROM(38)

(Bus Numbers)  Primary(18)     Secondary(19)   Subordinate(1A)
               ----------------------------------------------------
               00               02               02
Secondary Latency Timer(1B):       00

Secondary Status(1E):    0
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                 0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:      0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:         0
  (12)Received Target Abort:          0  (13)Received Master Abort:         0
  (14)Received System Error:          0  (15)Detected Parity Error:         0

Resource Type                             Base                    Limit
-------------------------------------------------------------------------
I/O(1C)                             0000F000                00000FFF
Memory(20)                          FFF00000                000FFFFF
Prefetchable Memory(24)    00000000FFF00000         00000000000FFFFF

Capabilities Ptr(34):   88

Bridge Control(3E)     0010
  (00)Parity Error Response:          0  (01)SERR# Enable:                   0
  (02)ISA Enable:                     0  (03)VGA Enable:                    0
  (05)Master Abort Mode:              0  (06)Secondary Bus Reset:           0
  (07)Fast Back-to-Back Enable:       0  (08)Primary Discard Timer:       2^15
  (09)Secondary Discard Timer:     2^15  (10)Discard Timer Status:          0
  (11)Discard Timer SERR# Enable:     0

Interrupt Line(3C)      0B             Interrupt Pin(3D):       01

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    00  Cap Register( 2):   0142
  Device Capabilities( 4):  00008000
  Device Control( 8):       0000       Device Status( A):    0000
  Link Capabilities( C):    03214C82
  Link Control(10):         0000       Link Status(12):      1001
  Slot Capabilities(14):    00142580
  Slot Control(18):         0000       Slot Status(1A):      0000
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

8.5 Integrated Graphics Device (B0:D2:F0)

```
Device pci 00 02 00
  PCI Segment 00 Bus 00 Device 02 Func 00 [EFI 0000020000]
  00000000: 86 80 16 01 07 00 90 00-09 00 00 03 00 00 00 00  *................*
  00000010: 04 00 C0 F5 00 00 00 00-0C 00 00 E0 00 00 00 00  *................*
  00000020: 01 E0 00 00 00 00 00 00-00 00 00 00 86 80 10 20  *................ *
  00000030: 00 00 00 00 90 00 00 00-00 00 00 00 0B 01 00 00  *................*

  00000040: 09 00 0C 01 96 61 00 C0-90 00 08 16 00 00 00 00  *.....a..........*
  00000050: 11 02 00 00 1D 00 00 00-00 00 00 00 01 00 A0 7B  *................*
  00000060: 00 00 02 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 05 D0 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 00 00 00 00 13 00 06 03-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 01 A4 22 00 00 00 00 00-00 00 00 00 00 00 00 00  *..".............*
  000000E0: 00 00 00 00 00 00 00 00-00 80 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-00 00 06 00 18 50 F9 7A  *.............P.z*

Vendor ID(0): 8086                    Device ID(2): 0116

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0090
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      1  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     09                  BIST(0F):  Incapable
Cache Line Size(C): 00                  Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Display Controller - VGA/8514 controller - VGA compatible
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ------------------------------------------------------------------------
  00000000F5C00000  Mem   64 bits  No     0000000000400000  00000000F5FFFFFF
  00000000E0000000  Mem   64 bits  YES    0000000010000000  00000000EFFFFFFF
              E000  I/O                                0040              E03F
  ------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      2010
Capabilities Ptr(34):        90
Interrupt Line(3C):          0B      Interrupt Pin(3D):       01
Min_Gnt(3E):                 00      Max_Lat(3F):             00

VX3035>
```

8.6 Platform Timers

This chapter considers the 3 Intel Platform common timers: TSC (Time Stamp Counter), HPET (High Precision Event Timer) and Local APIC timer.

8.6.1 TSC timer

The TSC is clocked at a fixed frequency into the CPU. Here is an extract of Intel architecture document :

For Pentium 4 processors, Intel Xeon processors (family [0FH], models [03H and higher]); for Intel Core Solo and Intel Core Duo processors (family [06H], model [0EH]); for the Intel Xeon processor 5100 series and Intel Core 2 Duo processors (family [06H], model [0FH]); for Intel Core 2 and Intel Xeon processors (family[06H], DisplayModel [17H]); for Intel Atom processors (family [06H], DisplayModel [1CH]): the time-stamp counter increments at a constant rate. That rate may be set by the maximum core-clock to bus-clock ratio of the processor or may be set by the maximum resolved frequency at which the processor is booted. The maximum resolved frequency may differ from the maximum qualified frequency of the processor, see Section 18.12.5 for more detail.

17.12.1 Invariant TSC

The time stamp counter in newer processors may support an enhancement, referred to as invariant TSC. Processor's support for invariant TSC is indicated by CPUID.80000007H:EDX[8].

The invariant TSC will run at a constant rate in all ACPI P-, C-. and T-states. This is the architectural behavior moving forward. On processors with invariant TSC support, the OS may use the TSC for wall clock timer services (instead of ACPI or HPET timers). TSC reads are much more efficient and do not incur the overhead associated with a ring transition or access to a platform resource.

So on VX3035: the time stamp counter is set by the max recognized CPU frequency which is **1.6 Ghz for VX3035 on SCU Moon configuration**. This time stamp clock comes from BusCLK CPU pin entry onto the CPU and is generated into Cougar Point PCH by XTAL25 pin which is connected to a 25 Mhz quartz oscillator (reference designator Y1201).

8.6.2 HPET, APIC timers

On Cougar Point HPET counters and APCI counters work from a clock oscillator at a frequency of 14,31818 MHz. This clock of 14,31818 MHz is generated by the Cougar Point itself from entry pin clock XTAL25 25 MHz. So this is he same entry as for the TSC.

To conclude there is no derivation expected between timers TSC, HPET and APIC.

Timer Accuracy Rules

1. The timers are expected to be accurate over any 1 ms period to within 0.05% (500 ppm)of the time specified in the timer resolution fields.

2. Within any 100-microsecond period, the timer is permitted to report a time that is up to 2 ticks too early or too late. Each tick must be less than or equal to 100 ns, so this represents an error of less than 0.2% (2000 ppm).

9 PCH (PLATFORM CONTROLLER HUB) REGISTERS

9.1 Reference documentation for PCH registers

The following documents describe the PCH registers:

- PCH BIOS writer's guide: Intel C200 series chipset Platform Controller Hub, Bios Spec, March 2011, rev 1.2.0, #30051, status NDA2. This document provides details on the BIOS initialization sequence for PCH functions.
- EDS PCH (External Design Specification): Intel C200 Series Chipset External Design Specification (EDS), Revision 2.0, January 2011 (962 pages), #443554, status NDA1. This document describes the registers of the PCH including functions related to SATA, USB, Ethernet.

9.2 PCH Configurations registers

This chapter lists the PCH integrated PCIe devices configurations registers after the BIOS initialization and before giving the hand to any operating system. For each device PCIe Config registers are dumped and their interpretation is given after that.

9.2.1 PCI Express* Root Ports (B0:D28:F0)

```
Device pci 00 1C 00
  PCI Segment 00 Bus 00 Device 1C Func 00 [EFI 00001C0000]
  00000000: 86 80 10 1C 07 00 10 00-B5 00 04 06 10 00 81 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 03 03 00 D0 D0 00 20  *............... *
  00000020: 40 F7 D0 F7 41 F1 D1 F1-00 00 00 00 00 00 00 00  *@...A...........*
  00000030: 00 00 00 00 40 00 00 00-00 00 00 00 0B 01 10 00  *....@...........*

  00000040: 10 80 42 01 00 80 00 00-00 00 10 00 42 4C 12 01  *..B.........BL..*
  00000050: 00 00 01 10 00 FD 04 00-00 00 00 00 00 00 00 00  *................*
  00000060: 00 00 00 00 16 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 02 00 01 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 05 90 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 0D A0 00 00 86 80 70 72-00 00 00 00 00 00 00 00  *......pr........*
  000000A0: 01 00 02 C8 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 01 02 0B 00 00-00 80 11 81 00 00 00 00  *................*
  000000E0: 00 3F 00 00 00 00 00 00-01 00 00 00 00 00 00 00  *.?..............*
  000000F0: 00 00 00 00 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C10

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
```

```
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     B5                 BIST(0F):  Incapable
Cache Line Size(C): 10                 Latency Timer(D): 00
Header Type(0E):    81, Multi-function, P2P bridge
Class: Bridge Device - PCI/PCI bridge -
Base Address Registers(10):  (None)
No Expansion ROM(38)

(Bus Numbers)  Primary(18)     Secondary(19)   Subordinate(1A)
               ------------------------------------------------------
               00               03              03
Secondary Latency Timer(1B):       00

Secondary Status(1E): 2000
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          1
  (14)Received System Error:          0  (15)Detected Parity Error:          0

Resource Type                             Base                    Limit
-------------------------------------------------------------------------
I/O(1C)                             0000D000                0000DFFF
Memory(20)                          F7400000                F7DFFFFF
Prefetchable Memory(24)    00000000F1400000         00000000F1DFFFFF

Capabilities Ptr(34):   40

Bridge Control(3E)     0010
  (00)Parity Error Response:          0  (01)SERR# Enable:                    0
  (02)ISA Enable:                     0  (03)VGA Enable:                     0
  (05)Master Abort Mode:              0  (06)Secondary Bus Reset:            0
  (07)Fast Back-to-Back Enable:       0  (08)Primary Discard Timer:       2^15
  (09)Secondary Discard Timer:     2^15  (10)Discard Timer Status:           0
  (11)Discard Timer SERR# Enable:     0

Interrupt Line(3C)      0B             Interrupt Pin(3D):       01

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    80  Cap Register( 2):   0142
  Device Capabilities( 4):  00008000
  Device Control( 8):       0000       Device Status( A):    0010
  Link Capabilities( C):    01124C42
  Link Control(10):         0000       Link Status(12):      1001
  Slot Capabilities(14):    0004FD00
  Slot Control(18):         0000       Slot Status(1A):      0000
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

9.2.2 PCI Express* Root Ports (B0:D28:F4)

```
Device pci 00 1C 04
  PCI Segment 00 Bus 00 Device 1C Func 04 [EFI 00001C0400]
  00000000: 86 80 18 1C 07 00 10 00-B5 00 04 06 10 00 81 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 04 04 00 C0 C0 00 20  *............... *
  00000020: A0 F6 30 F7 A1 F0 31 F1-00 00 00 00 00 00 00 00  *..0...1.........*
  00000030: 00 00 00 00 40 00 00 00-00 00 00 00 0B 01 10 00  *....@...........*

  00000040: 10 80 42 01 00 80 00 00-00 00 10 00 22 3C 12 05  *..B.........."<..*
  00000050: 40 00 22 F0 00 00 24 00-00 00 40 01 00 00 00 00  *@."...$...@.....*
  00000060: 00 00 00 00 16 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 02 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 05 90 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 0D A0 00 00 86 80 70 72-00 00 00 00 00 00 00 00  *......pr........*
  000000A0: 01 00 02 C8 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 01 02 0B 00 00-80 11 81 00 00 00 00 00  *................*
  000000E0: 00 3F 00 00 00 00 00 00-01 00 00 00 00 00 00 00  *.?..............*
  000000F0: 00 00 00 00 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C18

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     B5                BIST(0F):  Incapable
Cache Line Size(C): 10                Latency Timer(D): 00
Header Type(0E):    81, Multi-function, P2P bridge
Class: Bridge Device - PCI/PCI bridge -
Base Address Registers(10):  (None)
No Expansion ROM(38)

(Bus Numbers)  Primary(18)     Secondary(19)   Subordinate(1A)
               ---------------------------------------------------
               00               04              04
Secondary Latency Timer(1B):       00

Secondary Status(1E): 2000
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          1
  (14)Received System Error:          0  (15)Detected Parity Error:          0

Resource Type                          Base                    Limit
-------------------------------------------------------------------------
```

```
I/O(1C)                            0000C000                 0000CFFF
Memory(20)                         F6A00000                 F73FFFFF
Prefetchable Memory(24)    00000000F0A00000         00000000F13FFFFF

Capabilities Ptr(34):   40

Bridge Control(3E)     0010
  (00)Parity Error Response:          0  (01)SERR# Enable:                  0
  (02)ISA Enable:                     0  (03)VGA Enable:                   0
  (05)Master Abort Mode:              0  (06)Secondary Bus Reset:          0
  (07)Fast Back-to-Back Enable:       0  (08)Primary Discard Timer:      2^15
  (09)Secondary Discard Timer:     2^15  (10)Discard Timer Status:         0
  (11)Discard Timer SERR# Enable:     0

Interrupt Line(3C)      0B             Interrupt Pin(3D):       01

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    80  Cap Register( 2):   0142
  Device Capabilities( 4):  00008000
  Device Control( 8):       0000       Device Status( A):    0010
  Link Capabilities( C):    05123C22
  Link Control(10):         0040       Link Status(12):      F022
  Slot Capabilities(14):    00240000
  Slot Control(18):         0000       Slot Status(1A):      0140
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

9.2.3 PCI Express* Root Ports (B0:D28:F7)

```
Device pci 00 1C 07
  PCI Segment 00 Bus 00 Device 1C Func 07 [EFI 00001C0700]
  00000000: 86 80 1E 1C 07 00 10 00-B5 00 04 06 10 00 81 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 05 05 00 B0 B0 00 20  *............... *
  00000020: 00 F6 90 F6 01 F0 91 F0-00 00 00 00 00 00 00 00  *................*
  00000030: 00 00 00 00 40 00 00 00-00 00 00 00 0B 04 10 00  *....@...........*

  00000040: 10 80 42 01 00 80 00 00-00 00 10 00 12 4C 12 08  *..B..........L..*
  00000050: 00 00 01 10 60 B2 3C 00-08 00 00 00 00 00 00 00  *....`.<.........*
  00000060: 00 00 00 00 16 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 02 00 01 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 05 90 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 0D A0 00 00 86 80 70 72-00 00 00 00 00 00 00 00  *......pr........*
  000000A0: 01 00 02 C8 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 01 02 0B 00 00-02 80 11 C1 00 00 00 00  *................*
  000000E0: 00 03 00 00 00 00 00 00-01 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C1E

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     B5                BIST(0F):  Incapable
Cache Line Size(C): 10                Latency Timer(D): 00
Header Type(0E):    81, Multi-function, P2P bridge
Class: Bridge Device - PCI/PCI bridge -
Base Address Registers(10):  (None)
No Expansion ROM(38)

(Bus Numbers)  Primary(18)     Secondary(19)   Subordinate(1A)
               ---------------------------------------------------
               00               05              05
Secondary Latency Timer(1B):       00

Secondary Status(1E): 2000
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          1
  (14)Received System Error:          0  (15)Detected Parity Error:          0

Resource Type                          Base                    Limit
-------------------------------------------------------------------------
```

```
I/O(1C)                             0000B000                 0000BFFF
Memory(20)                          F6000000                 F69FFFFF
Prefetchable Memory(24)    00000000F0000000         00000000F09FFFFF

Capabilities Ptr(34):   40

Bridge Control(3E)     0010
  (00)Parity Error Response:          0  (01)SERR# Enable:                  0
  (02)ISA Enable:                     0  (03)VGA Enable:                    0
  (05)Master Abort Mode:              0  (06)Secondary Bus Reset:           0
  (07)Fast Back-to-Back Enable:       0  (08)Primary Discard Timer:       2^15
  (09)Secondary Discard Timer:     2^15  (10)Discard Timer Status:          0
  (11)Discard Timer SERR# Enable:     0

Interrupt Line(3C)      0B             Interrupt Pin(3D):       04

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    80  Cap Register( 2):   0142
  Device Capabilities( 4):  00008000
  Device Control( 8):       0000       Device Status( A):    0010
  Link Capabilities( C):    08124C12
  Link Control(10):         0000       Link Status(12):      1001
  Slot Capabilities(14):    003CB260
  Slot Control(18):         0008       Slot Status(1A):      0000
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

9.2.4 Gigabit Ethernet Controller (B0:D25:F0)

```
Device pci 00 19 00
  PCI Segment 00 Bus 00 Device 19 Func 00 [EFI 0000190000]
  00000000: 86 80 02 15 07 00 10 00-05 00 00 02 00 00 00 00  *................*
  00000010: 00 00 E0 F7 00 50 E2 F7-81 E0 00 00 00 00 00 00  *.....P..........*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 00 00  *................*
  00000030: 00 00 00 00 C8 00 00 00-00 00 00 00 0A 01 00 00  *................*

  00000040: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-01 D0 22 C8 00 20 00 07  *..........".. ..*
  000000D0: 05 E0 80 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 13 00 06 03 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1502

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     05                BIST(0F):  Incapable
Cache Line Size(C): 00                Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Network Controller - Ethernet controller -
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ------------------------------------------------------------------------
          F7E00000  Mem   32 bits  No             00020000          F7E1FFFF
          F7E25000  Mem   32 bits  No             00001000          F7E25FFF
              E080  I/O                               0020             E09F
  ------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      0000
Capabilities Ptr(34):        C8
Interrupt Line(3C):          0A      Interrupt Pin(3D):       01
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

9.2.5 LPC Bridge (B0:D31:F0)

```
Device pci 00 1F 00
  PCI Segment 00 Bus 00 Device 1F Func 00 [EFI 00001F0000]
  00000000: 86 80 4F 1C 07 00 10 02-05 00 01 06 00 00 80 00  *..O.............*
  00000010: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 4F 1C  *..............O.*
  00000030: 00 00 00 00 E0 00 00 00-00 00 00 00 00 00 00 00  *................*

  00000040: 01 04 00 00 80 00 00 00-01 05 00 00 10 00 00 00  *................*
  00000050: F8 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 0B 05 05 0B D0 00 00 00-0A 80 80 0A F8 F0 00 00  *................*
  00000070: 78 F0 79 F0 7A F0 7B F0-7C F0 7D F0 7E F0 7F F0  *x.y.z...........*
  00000080: 10 00 0F 3C 81 06 7C 00-41 16 0C 00 01 08 FC 00  *...<....A.......*
  00000090: 01 0A 1C 00 00 05 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 14 0E 80 00 40 18 06 00-00 47 00 00 00 00 00 00  *....@....G......*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 33 22 11 00 67 45 00 00-C0 F0 00 00 20 00 00 00  *3"..gE...... ...*
  000000E0: 09 00 0C 10 00 00 00 00-93 02 64 0E 00 00 00 00  *..........d.....*
  000000F0: 01 C0 D1 FE 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C4F

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0210
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:             Medium  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     05                  BIST(0F):  Incapable
Cache Line Size(C): 00                  Latency Timer(D): 00
Header Type(0E):    80, Multi-function, PCI device
Class: Bridge Device - PCI/ISA bridge -
Base Address Registers(10):
  (None)
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      1C4F
Capabilities Ptr(34):        E0
Interrupt Line(3C):          00      Interrupt Pin(3D):       00
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

9.2.6 SATA Host Controller (B0:D31:F2, F5)

By default SATA controller are set in AHCI mode so only one SATA controller is visible (2 controller are visible if IDE mode is set by SETUP)

```
Device pci 00 1F 02
  PCI Segment 00 Bus 00 Device 1F Func 02 [EFI 00001F0200]
  00000000: 86 80 03 1C 07 00 B0 02-05 01 06 01 00 00 00 00  *................*
  00000010: D1 E0 00 00 C1 E0 00 00-B1 E0 00 00 A1 E0 00 00  *................*
  00000020: 61 E0 00 00 00 20 E2 F7-00 00 00 00 86 80 03 1C  *a.... ..........*
  00000030: 00 00 00 00 80 00 00 00-00 00 00 00 0B 02 00 00  *................*

  00000040: 00 80 00 80 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 01 A8 03 40 08 00 00 00-00 00 00 00 00 00 00 00  *...@............*
  00000080: 05 70 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *.p..............*
  00000090: 60 30 0F 80 83 01 00 30-08 42 5C 01 00 00 00 00  *`0.....0.B\.....*
  000000A0: E0 00 00 00 00 00 00 00-12 B0 10 00 48 00 00 00  *............H...*
  000000B0: 13 00 06 03 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C03

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0
Status(6): 02B0
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  1
  (07)Fast Back-to-Back Capable:      1  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:             Medium  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0
Revision ID(8):     05                   BIST(0F):  Incapable
Cache Line Size(C): 00                   Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Mass Storage Controller - UNDEFINED - UNDEFINED
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
             E0D0  I/O                                 0008             E0D7
             E0C0  I/O                                 0004             E0C3
             E0B0  I/O                                 0008             E0B7
             E0A0  I/O                                 0004             E0A3
             E060  I/O                                 0020             E07F
         F7E22000  Mem   32 bits  No              00000800          F7E227FF
  ---------------------------------------------------------------------------
Expansion ROM Disabled(30)
Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      1C03
Capabilities Ptr(34):        80
Interrupt Line(3C):          0B      Interrupt Pin(3D):       02
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

9.2.7 USB EHCI Host Controllers (B0:D29:F0 and D26:F0)

```
pci 00 1A 00
  PCI Segment 00 Bus 00 Device 1A Func 00 [EFI 00001A0000]
  00000000: 86 80 2D 1C 06 00 90 02-05 20 03 0C 00 00 00 00  *..-...... ......*
  00000010: 00 40 E2 F7 00 00 00 00-00 00 00 00 00 00 00 00  *.@..............*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 70 72  *..............pr*
  00000030: 00 00 00 00 50 00 00 00-00 00 00 00 0B 01 00 00  *....P...........*

  00000040: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 01 58 C2 C9 00 00 00 00-0A 98 A0 20 00 00 00 00  *.X......... ....*
  00000060: 20 20 FF 07 00 00 00 00-01 00 01 00 07 20 08 00  *  ........... ..*
  00000070: 00 00 DD 3F 00 00 00 00-00 00 00 00 00 00 00 00  *...?............*
  00000080: 00 00 80 00 11 88 0C 93-30 0D 00 24 00 00 00 00  *........0..$....*
  00000090: 00 00 00 00 00 00 00 00-13 00 06 03 00 00 00 00  *................*
  000000A0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 AA FF 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 46 20 88 23-81 22 91 31 8C C6 47 49  *....F .#."1..GI*
  000000F0: 00 00 00 00 88 85 80 00-87 0F 05 08 08 17 5B 20  *..............[ *

Vendor ID(0): 8086                    Device ID(2): 1C2D

Command(4): 0006
  (00)I/O space access enabled:       0  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0290
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      1  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:             Medium  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     05                BIST(0F):  Incapable
Cache Line Size(C): 00                Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Serial Bus Controllers - USB - UNDEFINED
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
         F7E24000  Mem   32 bits  No              00000400          F7E243FF
  ---------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      7270
Capabilities Ptr(34):        50
Interrupt Line(3C):          0B      Interrupt Pin(3D):       01
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

```
pci 00 1D 00
  PCI Segment 00 Bus 00 Device 1D Func 00 [EFI 00001D0000]
  00000000: 86 80 26 1C 06 00 90 02-05 20 03 0C 00 00 00 00  *..&...... ......*
  00000010: 00 30 E2 F7 00 00 00 00-00 00 00 00 00 00 00 00  *.0..............*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 70 72  *..............pr*
  00000030: 00 00 00 00 50 00 00 00-00 00 00 00 0A 01 00 00  *....P...........*

  00000040: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 01 58 C2 C9 00 00 00 00-0A 98 A0 20 00 00 00 00  *.X......... ....*
  00000060: 20 20 FF 07 00 00 00 00-01 00 01 00 07 20 08 00  *  ........... ..*
  00000070: 00 00 DD 3F 00 00 00 00-00 00 00 00 00 00 00 00  *...?............*
  00000080: 00 00 80 00 11 88 0C 93-30 0D 00 24 00 00 00 00  *........0..$....*
  00000090: 00 00 00 00 00 00 00 00-13 00 06 03 00 00 00 00  *................*
  000000A0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 AA FF 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 00 20 00 40-C0 40 00 01 98 87 18 35  *..... .@.@.....5*
  000000F0: 00 00 00 00 88 85 80 00-87 0F 05 08 08 17 5B 20  *..............[ *

Vendor ID(0): 8086                    Device ID(2): 1C26

Command(4): 0006
  (00)I/O space access enabled:       0  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0290
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      1  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:             Medium  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     05                BIST(0F):  Incapable
Cache Line Size(C): 00                Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Serial Bus Controllers - USB - UNDEFINED
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ------------------------------------------------------------------------
         F7E23000  Mem   32 bits  No             00000400          F7E233FF
  ------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      7270
Capabilities Ptr(34):        50
Interrupt Line(3C):          0A      Interrupt Pin(3D):       01
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

9.2.8 SMBus Controller (B0:D31:F3)

```
Device pci 00 1F 03
  PCI Segment 00 Bus 00 Device 1F Func 03 [EFI 00001F0300]
  00000000: 86 80 22 1C 03 00 80 02-05 00 05 0C 00 00 00 00  *.."............*
  00000010: 04 10 E2 F7 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 41 E0 00 00 00 00 00 00-00 00 00 00 86 80 22 1C  *A..............".*
  00000030: 00 00 00 00 00 00 00 00-00 00 00 00 05 03 00 00  *................*

  00000040: 01 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 03 04 04 00 00 00 08 08-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 04 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C22

Command(4): 0003
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           0  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0280
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      1  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:             Medium  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     05                BIST(0F):  Incapable
Cache Line Size(C): 00                Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Serial Bus Controllers - System Management Bus -
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ------------------------------------------------------------------------
  00000000F7E21000  Mem   64 bits  No     0000000000000100  00000000F7E210FF
             E040  I/O                                0020              E05F
  ------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      1C22
Capabilities Ptr(34):        00
Interrupt Line(3C):          05      Interrupt Pin(3D):       03
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

9.2.9 Thermal Sensor Registers (B0:D31:F6)

```
Device pci 00 1F 06 -i
  PCI Segment 00 Bus 00 Device 1F Func 06 [EFI 00001F0600]
  00000000: 86 80 24 1C 00 00 10 00-05 00 80 11 00 00 00 00  *..$.............*
  00000010: 04 00 E2 F7 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 24 1C  *..............$.*
  00000030: 00 00 00 00 50 00 00 00-00 00 00 00 05 03 00 00  *....P...........*

  00000040: 05 00 A0 7F 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000050: 01 00 23 00 08 00 00 00-00 00 00 00 00 00 00 00  *..#.............*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 05 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-87 0F 05 08 00 00 00 00  *................*

Vendor ID(0): 8086                    Device ID(2): 1C24

Command(4): 0000
  (00)I/O space access enabled:       0  (01)Memory space access enabled:    0
  (02)Behave as bus master:           0  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     05                BIST(0F):  Incapable
Cache Line Size(C): 00                Latency Timer(D): 00
Header Type(0E):    00, Single function, PCI device
Class: Data Acquisition & Signal Processing Controllers - Other DAQ & SP controllers -
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
  00000000F7E20000  Mem   64 bits  No     0000000000001000  00000000F7E20FFF
  ---------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      1C24
Capabilities Ptr(34):        50
Interrupt Line(3C):          05      Interrupt Pin(3D):       03
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

9.3 AMT Consideration

Intel AMT (Active Management Technology) is not activated on VX3035. This feature is removed from the BIOS compilation (as for the Management Engine) and its activation/deactivation is not available into BIOS SETUP Menu.

The AMT features are IDE-R (for Remote boot) and SOL/KVM (for Remote console). These features are associated to 2 PCI devices functions of PCH device PCI D22. These 2 functions are F2 et F3. These functions are disabled after booting by the Management Engine of the PCH. This is visible under BIOS EFI Shell when listing the PCI device. Device « bus0 device22 (0x16) func0 » corresponding to Intel Management Engine Interface #1 is present but devices D22/F2 et D22/F3 disapear after 1-2 seconds during the platform setup and are not available anymore after that.

AMT field into SMBios tables (type 82) are then not initialized at all.

```
// This is definition for SMBIOS Oem data type 0x82
 typedef struct
 {
   SMBIOS_STRUCTURE_HEADER      Header;
   UINT8                        AmtSignature[4];
   UINT8                        AmtSupported;
   UINT8                        AmtEnabled;
   UINT8                        IderEnabled;
   UINT8                        SolEnabled;
   UINT8                        NetworkEnabled;
   UINT8                        ExtendedData;
   UINT8                        OemCapabilities1;
   UINT8                        OemCapabilities2;
   UINT8                        OemCapabilities3;
   UINT8                        OemCapabilities4;
   UINT8                        KvmEnabled;
   UINT8                        Reserved;
   UINT16                        Zero;   //terminator
 } EFI_MISC_OEM_TYPE_0x82;
```

10 MEMORY MAPPING

Memory mapping is given into the following document

- 2nd Generation Intel® Core™ Processor Family Desktop 445465_CPU_SandyBridge_EDS_Vol2_July2011 (302 pages), status NDA1. Chapter 2.3 System Address Map

This gives the standard memory mapping for Intel Core processors. In particular the Legacy Address Range (Including the SMM memory), Main memory Address Range and PCI Memory Address Range are considered.

BIOS E820 table indicates the Memory mapping to Operating System. Here is the Memory mapping for the VX3035 (No PEX8609, 2G RAM)

BIOS-provided physical RAM map:

0000000000000000 - 000000000009c800	usable but I/O Legacy Address Range
000000000009c800 - 00000000000a0000	reserved
00000000000e0000 - 0000000000100000	reserved
0000000000100000 - 0000000020000000	usable
0000000020000000 - 0000000020200000	reserved
0000000020200000 - 0000000040000000	usable
0000000040000000 - 0000000040200000	reserved
0000000040200000 - 000000007ad1f000	usable
000000007ad1f000 - 000000007ad8e000	reserved Run Time Driver Services Code
000000007ad8e000 - 000000007ad9e000	usable
000000007ad9e000 - 000000007ad9f000	reserved Run Time Driver Services Data
000000007ad9f000 - 000000007ada0000	usable
000000007ada0000 - 000000007ade8000	reserved Run Time Services Data
000000007ade8000 - 000000007af42000	usable
000000007af42000 - 000000007af91000	ACPI NVS
000000007af91000 - 000000007af95000	usable
000000007af95000 - 000000007afe8000	ACPI NVS
000000007afe8000 - 000000007affd000	usable
000000007affd000 - 000000007b000000	ACPI data
000000007b000000 - 000000007fa00000	reserved
00000000f8000000 - 00000000fc000000	reserved MEM I/O
00000000fec00000 - 00000000fec01000	reserved MEM I/O
00000000fed10000 - 00000000fed14000	reserved MEM I/O
00000000fed18000 - 00000000fed1a000	reserved MEM I/O
00000000fed1c000 - 00000000fed20000	reserved MEM I/O
00000000fee00000 - 00000000fee01000	reserved MEM I/O
00000000ffa00000 - 00000000ffc00000	reserved MEM I/O
00000000ffe00000 - 0000000100000000	reserved MEM I/O
0000000100000000 - 0000000100600000	usable

10.1 Legacy Address Range specific to VX3035

The DOS Area or Legacy address range described in Intel documentation (from addresses 0x0 to 0x9FFFF) is modified to support the CPLD device I/O mapping. The only BIOS modification for I/O mapping is to replace the FIR (Function not used in SIO 1007) LPC I/O mapping address 0x7E8 by the CPLD device mapping accessed on LPC bus at **I/O address 0x800**.

10.2 Main Memory Mapping

The main memory mapping is standard and maps from 1MB to TOLUD register (Top of Low Usable physical memory) value.
The TOLUD register is set to the appropriate value by the BIOS. The remapbase/remaplimit registers remap logical accesses bound for addresses above 4 GB onto physical addresses that fall within DRAM.

For VX3035 (with modified SETUP as describded)

- TOLUD = 7FA00000H (see IMC BCh-BFh register)
- REMAPBASE = 00000001_00000000H (see IMC register 90h)
- REMAPLIMIT = 00000001_005FFFFFH (see IMC register 98h)

TOLUD register indicates the top of Usable memory below 4GB. The total amount of physical memory detected by the BIOS is indicated into the TOM register (see IMC controller device 0:0:0 PCI registers A0h-A7h).

10.3 PCI Memory Allocation

The PCI memory area is located above TOLUD. Its size depends on the PCIe device list. The BIOS determines the correct PCI memory mapping according to the PCIe devices that has been listed during the PCI discovery mechanism. Each detected devices will have a reserved PCI memory area with a size corresponding to its requirements.

10.3.1 PCI device list

```
 Seg  Bus  Dev  Func
  ---  ---  ---  ----
   00   00   00    00 ==> Bridge Device - Host/PCI bridge
           Vendor 8086 Device 0104 Prog Interface 0
   00   00   01    00 ==> Bridge Device - PCI/PCI bridge
           Vendor 8086 Device 0101 Prog Interface 0
   00   00   01    01 ==> Bridge Device - PCI/PCI bridge
           Vendor 8086 Device 0105 Prog Interface 0
   00   00   02    00 ==> Display Controller - VGA/8514 controller
           Vendor 8086 Device 0116 Prog Interface 0
   00   00   16    00 ==> Simple Communications Controllers - Other communicati
           Vendor 8086 Device 1C3A Prog Interface 0
   00   00   19    00 ==> Network Controller - Ethernet controller
           Vendor 8086 Device 1502 Prog Interface 0
   00   00   1A    00 ==> Serial Bus Controllers - USB
           Vendor 8086 Device 1C2D Prog Interface 20
   00   00   1C    00 ==> Bridge Device - PCI/PCI bridge
           Vendor 8086 Device 1C10 Prog Interface 0
   00   00   1C    04 ==> Bridge Device - PCI/PCI bridge
           Vendor 8086 Device 1C18 Prog Interface 0
   00   00   1C    07 ==> Bridge Device - PCI/PCI bridge
           Vendor 8086 Device 1C1E Prog Interface 0
```

```
    00   00   1D    00 ==> Serial Bus Controllers - USB
              Vendor 8086 Device 1C26 Prog Interface 20
    00   00   1F    00 ==> Bridge Device - PCI/ISA bridge
              Vendor 8086 Device 1C4F Prog Interface 0
    00   00   1F    02 ==> Mass Storage Controller - UNDEFINED
              Vendor 8086 Device 1C03 Prog Interface 1
    00   00   1F    03 ==> Serial Bus Controllers - System Management Bus
              Vendor 8086 Device 1C22 Prog Interface 0
    00   00   1F    06 ==> Data Acquisition & Signal Processing Controllers - Ot
              Vendor 8086 Device 1C24 Prog Interface 0
    00   04   00    00 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 1510 Prog Interface 0
    00   04   00    01 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 1510 Prog Interface 0
```

10.3.2 PCI device Resources mapping

```
00   00   01    00 (PCI bridge) ==>
Resource              Type                      Base                    Limit
-------------------------------------------------------------------------
I/O(1C)                                         0000F000          00000FFF
Memory(20)                                      FFF00000          000FFFFF
Prefetchable Memory(24)                         00000000FFF00000  00000000000FFFFF

00   00   02    00 (VGA) ==>
  Start_Address       Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
  00000000F5C00000    Mem   64 bits  No        0000000000400000  00000000F5FFFFFF
  00000000E0000000    Mem   64 bits  YES       0000000010000000  00000000EFFFFFFF
                      E000  I/O                0040              E03F
  ---------------------------------------------------------------------------

00   00   16    00 (ME Ctrl) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
  00000000F7E27000    Mem   64 bits  No        0000000000000010  00000000F7E2700F
  ---------------------------------------------------------------------------

00   00   19    00 (Network) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
           F7E00000    Mem   32 bits  No         00020000          F7E1FFFF
           F7E25000    Mem   32 bits  No         00001000          F7E25FFF
               E080    I/O                      0020              E09F
  ---------------------------------------------------------------------------

00   00   1A    00 (USB) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
           F7E24000    Mem   32 bits  No        00000400          F7E243FF
  ---------------------------------------------------------------------------

00   00   1C    00 (PCI Bridge) ==> Bridge
Resource              Type                      Base                     Limit
-------------------------------------------------------------------------
I/O(1C)                                         0000D000          0000DFFF
Memory(20)                                      F7400000          F7DFFFFF
Prefetchable Memory(24)                         00000000F1400000  00000000F1DFFFFF

00   00   1C    04 (PCI bridge) ==>
Resource              Type                      Base                     Limit
-------------------------------------------------------------------------
I/O(1C)                                         0000C000          0000CFFF
```

```
Memory(20)                                F6A00000          F73FFFFF
Prefetchable Memory(24)                   00000000F0A00000  00000000F13FFFFF

00   00   1C    07 (PCI bridge) ==>
Resource              Type                Base                    Limit
-------------------------------------------------------------------------
I/O(1C)                                   0000B000           0000BFFF
Memory(20)                                F6000000           F69FFFFF
Prefetchable Memory(24)                   00000000F0000000   00000000F09FFFFF


00   00   1D    00 (USB) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
           F7E23000    Mem   32 bits  No             00000400       F7E233FF
  ---------------------------------------------------------------------------

00   00   1F    02 (SATA) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
               E0D0      I/O                        0008             E0D7
               E0C0      I/O                        0004             E0C3
               E0B0      I/O                        0008             E0B7
               E0A0      I/O                        0004             E0A3
               E060      I/O                        0020             E07F
           F7E22000    Mem   32 bits      No        00000800         F7E227FF
  ---------------------------------------------------------------------------

00   00   1F    03 (SMBus) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
  00000000F7E21000    Mem   64 bits  No        0000000000000100   00000000F7E210FF
               E040    I/O                    0020               E05F
  ---------------------------------------------------------------------------

00   00   1F    06 (Thermal) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
  00000000F7E20000    Mem   64 bits  No        0000000000001000  00000000F7E20FFF
  ---------------------------------------------------------------------------


00   04   00    00 (Network) ==>
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
           F6A80000    Mem   32 bits  No             00080000          F6AFFFFF
               C020    I/O                        0020              C03F
           F6B04000    Mem   32 bits  No             00004000          F6B07FFF
  ---------------------------------------------------------------------------


00   04   00    01 (Network)
     Start_Address    Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
           F6A00000    Mem   32 bits  No             00080000          F6A7FFFF
               C000    I/O                        0020              C01F
           F6B00000    Mem   32 bits  No             00004000          F6B03FFF
  ---------------------------------------------------------------------------
```

10.4 PCI IRQ mapping

Seg Bus Dev Func	Interrupt Line(3C)	Interrupt Pin(3D)
00 00 00 00	00	00
00 00 01 00	0B	01
00 00 01 01	0B	01
00 00 02 00	0B	01
00 00 16 00	00	01
00 00 19 00	0A	01
00 00 1A 00	0B	01
00 00 1C 00	0B	01
00 00 1C 04	0B	01
00 00 1C 07	0B	04
00 00 1D 00	0A	01
00 00 1F 00	00	00
00 00 1F 02	0B	02
00 00 1F 03	05	03
00 00 1F 06	05	03
00 04 00 00	10	01
00 04 00 01	11	02

11 BARTON HILL ETHERNET CONTROLLER REGISTERS (B0:D4:F0, F1)

The Barton Hill Ethernet controller programming guide is given in documentation:

- Intel® 82580 Quad/Dual Gigabit Ethernet LAN Controller Datasheet (321027-013EN Revision: 2.41 June 2010 730 pages) NoNDA

The device must be reset and reinitialized by Operating System. Anyway the PCI configuration space Register is the following after the BIOS has boot up.

11.1 First Ethernet Controller on Barton Hill

Here are the exhaustive PCI configuration register values for First 82580 Ethernet controller.

11.1.1 PCI configuration register dump

```
 PCI Segment 00 Bus 04 Device 00 Func 00 [EFI 0004000000]
  00000000: 86 80 10 15 07 00 10 00-01 00 00 02 10 00 80 00  *................*
  00000010: 00 00 A8 F6 00 00 00 00-21 C0 00 00 00 40 B0 F6  *........!....@..*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 00 00  *................*
  00000030: 00 00 00 00 40 00 00 00-00 00 00 00 10 01 00 00  *....@...........*

  00000040: 01 50 23 48 00 20 00 00-00 00 00 00 00 00 00 00  *.P#H. ..........*
  00000050: 05 70 80 01 00 00 00 00-00 00 00 00 00 00 00 00  *.p..............*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 11 A0 09 00 03 00 00 00-03 20 00 00 00 00 00 00  *......... ......*
  00000080: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000090: 00 00 00 00 00 00 00 00-00 00 00 00 FF FF FF FF  *................*
  000000A0: 10 00 02 00 C2 8C 00 10-10 28 09 00 42 CC 01 00  *.........(..B...*
  000000B0: 40 00 22 10 00 00 00 00-00 00 00 00 00 00 00 00  *@."............*
  000000C0: 00 00 00 00 1F 18 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 02 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
```

11.1.2 PCI configuration register value interpretation

```
Vendor ID(0): 8086                    Device ID(2): 1510

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0
```

```
Revision ID(8):     01                BIST(0F):  Incapable
Cache Line Size(C): 10                Latency Timer(D): 00
Header Type(0E):    80, Multi-function, PCI device
Class: Network Controller - Ethernet controller -
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ------------------------------------------------------------------------
          F6A80000  Mem   32 bits  No             00080000          F6AFFFFF
              C020  I/O                               0020             C03F
          F6B04000  Mem   32 bits  No             00004000          F6B07FFF
  ------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      0000
Capabilities Ptr(34):        40
Interrupt Line(3C):          10      Interrupt Pin(3D):       01
Min_Gnt(3E):                 00      Max_Lat(3F):             00

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    00  Cap Register( 2):   0002
  Device Capabilities( 4):  10008CC2
  Device Control( 8):       2810       Device Status( A):    0009
  Link Capabilities( C):    0001CC42
  Link Control(10):         0040       Link Status(12):      1022
  Slot Capabilities(14):    00000000
  Slot Control(18):         0000       Slot Status(1A):      0000
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

11.2 Second Ethernet Controller on Barton Hill

Here is the exhaustive PCI configuration register value for second 82580 ethernet controller.

11.2.1 PCI configuration register dump

```
PCI Segment 00 Bus 04 Device 00 Func 01 [EFI 0004000100]
00000000: 86 80 10 15 07 00 10 00-01 00 00 02 10 00 80 00  *................*
00000010: 00 00 A0 F6 00 00 00 00-01 C0 00 00 00 00 B0 F6  *................*
00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 00 00  *................*
00000030: 00 00 00 00 40 00 00 00-00 00 00 00 11 02 00 00  *....@...........*
00000040: 01 50 23 48 00 20 00 00-00 00 00 00 00 00 00 00  *.P#H. ..........*
00000050: 05 70 80 01 00 00 00 00-00 00 00 00 00 00 00 00  *.p..............*
00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
00000070: 11 A0 09 00 03 00 00 00-03 20 00 00 00 00 00 00  *......... ......*
00000080: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
00000090: 00 00 00 00 00 00 00 00-00 00 00 00 FF FF FF FF  *................*
000000A0: 10 00 02 00 C2 8C 00 10-10 28 09 00 42 CC 01 00  *.........(..B...*
000000B0: 40 00 22 10 00 00 00 00-00 00 00 00 00 00 00 00  *@."............*
000000C0: 00 00 00 00 1F 18 00 00-00 00 00 00 00 00 00 00  *................*
000000D0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
000000F0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
```

11.2.2 PCI configuration register value interpretation

```
Vendor ID(0): 8086                    Device ID(2): 1510

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0

Revision ID(8):     01                BIST(0F):  Incapable
Cache Line Size(C): 10                Latency Timer(D): 00
Header Type(0E):    80, Multi-function, PCI device
Class: Network Controller - Ethernet controller -
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
  ---------------------------------------------------------------------------
          F6A00000  Mem   32 bits  No             00080000          F6A7FFFF
          C000         I/O                                 0020              C01F
          F6B00000  Mem   32 bits  No             00004000          F6B03FFF
  ---------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      0000
Capabilities Ptr(34):        40
Interrupt Line(3C):          11      Interrupt Pin(3D):       02
Min_Gnt(3E):                 00      Max_Lat(3F):             00

Pci Express device capability structure:
  CapID( 0):          10  NextCap Ptr( 1):    00  Cap Register( 2):   0002
  Device Capabilities( 4):  10008CC2
  Device Control( 8):       2810       Device Status( A):    0009
  Link Capabilities( C):    0001CC42
  Link Control(10):         0040       Link Status(12):      1022
  Slot Capabilities(14):    00000000
  Slot Control(18):         0000       Slot Status(1A):      0000
  Root Control(1C):         0000       RsvdP(1E):            0000
  Root Status(20):          00000000
```

12 SUPER I/O REGISTERS

SIO data sheet is described into document SIO1007 DS Rev 0.11 (03-03-05).pdf from SMSC (NDA1)

At the end of BIOS boot the configuration registers and UART registers are initialized as described here after. UART should be reinitialized as whished for serial use (baud rate) under Operating System

Kontron changes SIO configuration to remove FIR configuration and add COM2/UART2 support. FIR support mode is not supported so is disabled.
UART COM 2 is accessible at **I/O address 0x2F8** and **UART COM0 at I/O address 0x3F8**. Configuration registers to select SMC1007 UART are accessible at I/O address 0x164E (index) and 0x164F (Data)

12.1 Configuration Register

To enter into configuration mode write 0x55 in Index register (at 0x164E). Then write at 0x164E the register number to access and read/write its value at 0x164F.

Here is the value of the SIO1007 configuration registers after the BIOS initialisation to have UART1 and UART2 available:

SIO1007 Config Register	Programmed value
Reg 0	0x00
Reg 1	0x80
Reg 2	0x88
Reg 3	0x00
Reg 4	0x00
Reg 5	0x00
Reg 6	0x00
Reg 7	0x00
Reg 8	0x00
Reg 9	0x00
Reg A	0x40
Reg B	0x02
Reg C	0x01
Reg D	0x20
Reg E	0x09
Reg F	0x00
Reg 10	0x00
Reg 11	0x00
Reg 12	0x4E
Reg 13	0x16
Reg 14	0x00

SIO1007 Config Register	Programmed value
Reg 20	0x00
Reg 21	0x00
Reg 22	0x00
Reg 23	0x00
Reg 24	0xFE
Reg 25	0xBE
Reg 26	0x00
Reg 27	0x00
Reg 28	0x43
Reg 29	0x80
Reg 2A	0x43
Reg 2B	0x00
Reg 2C	0x03
Reg 2D	0x03
Reg 2E	0x00
Reg 2F	0x00
Reg 30	0x68
Reg 31	0x1F
Reg 32	0x00
Reg 33	0x04
Reg 34	0x01

SIO1007 Config Register	Programmed value
Reg 15	0x01
Reg 16	0x00
Reg 17	0x00
Reg 18	0x00
Reg 19	0x00
Reg 1A	0x00
Reg 1B	0x03
Reg 1C	0x00
Reg 1D	0x00
Reg 1E	0x00
Reg 1F	0x00

SIO1007 Config Register	Programmed value
Reg 35	0xFE
Reg 36	0x0C
Reg 37	0xFE
Reg 38	0xFB
Reg 39	0x00
Reg 3A	0x0B
Reg 3B	0x06
Reg 3C	0x90

12.2 UART 1 Register (COM0)

Here the COM0 UART 1 line status read from UART COM1 for default SETUP BIOS mode (COM1 is intialized and ready to used because BIOS SETUP option “COM0 serial line redirection” is enabled)

UART Register (I/O 0x3f8)	Read Value
IER,interrupt enable register (base + 1)	0x00
IIR,interrupt identification register (base + 2)	0xC1
LCR,line control register (base + 3)	0x03
MCR,modem control register (base + 4)	0x03
LSR,line status register (base + 5)	0x00
MSR,modem status register (base + 6)	0xB0
SCR,scratch register (base + 7)	0xAA
DLL,divisor latch LSB (base + 0)	0x6D
DLM,divisor latch MSB (base + 1)	0x00

12.3 UART2 Register (COM1)

Here the COM1 UART line status read from UART COM1 for default SETUP BIOS mode (COM1 not initialized by BIOS by default)

UART Register (I/O 0x2f8)	Read Value
IER,interrupt enable register	0x00
IIR,interrupt identification register	0x01
LCR,line control register	0x03
MCR,modem control register	0x00
LSR,line status register	0x60
MSR,modem status register	0x00
SCR,scratch register	0xAA
DLL,divisor latch LSB	0x01
DLM,divisor latch MSB	0x00

13 VOLTAGE SENSORS

8 Voltages sensors are available on CougarPoint SMBus by means of Analog to Digital Converter ADS7830. See documentation from Texas Instrument ADS7830 SBAS302 December 2003 (NoNDA). ADS7830 can be reached on SMbus at **address 0x4B**

Eight voltage values can be obtained reading data from ADS7830 converter (12V0, 5V0, 2V5, 3V3, 3V3SB, 1V05S,1V05, 1V0). Source code from BIOS or Linux can be provided by KOM-SA as example.

14 RTC ON SMBUS

RTC on Smbus is not used at all by the BIOS. The internal CougarPoint RTC is used instead. However it is planned to be used in the futur to economize the battery life time.

15 SELF-LOADED SETUP EEPROM

15.1 Barton Hill Ethernet controller EEPROM

The Barton Hill or 82580EB/DB uses an EEPROM device for storing product configuration information. Several words of the EEPROM are accessed automatically by the 82580EB/DB after reset in order to provide pre-boot configuration data that must be available to the 82580EB/DB before it is accessed by host software.
The remainder of the stored information is accessed by various software modules used to report product configuration, serial number, etc.

The content of this EEPROM is programmed during the VX3035 factory process using an Intel tool (EEUPDATE). The programmed EEPROM file is 82580.EEP.MAC addresses are also updated into the EEPROM after the EEPROM programming.

The lack of EEPROM programming will cause the 82580 Ethernet interface to not work.

15.2 MAC/LewisVille Phy Ethernet controller “EEPROM” area

The MAC/LewisVille 82579 Phy ethernet device doesn’t have any EEPROM but uses the System Flash Area 0x1000 to 0x2FFF instead to load pre-boot configuration data. This area content can be found and dumped from 8M BIOS image itself. Only the MAC addresses are updated during the factory process using kmac BIOS command.

This area (0x1000-0x2FFF) must be preserved in case of System Flash updated under Operating System otherwise these these MAC addresses will be erased.

The 82579 data Sheet documentation from Intel is

- Intel 82579 Gigabit Ethernet Controller PHY v2.0 (January 2011 131 pages) (NoNDA)

15.3 System flash partition for Cougar Point PCH

Two 8 Mbytes SPI flashes are present on VX3035. One is the MAIN flash and allows the VX3035 to load the BIOS code. The second is a RESCUE SPI Flash containing a RESCUE BIOS image and used only in case of MAIN flash BIOS corruption.

The Flash content is the BIOS image delivered by Kontron updated by the GBE area configured during the board factory process.

The MAIN or RESCUE SPI flash layout for SPI Flash part SST25VF064C (8 MB) is shown in following figure:

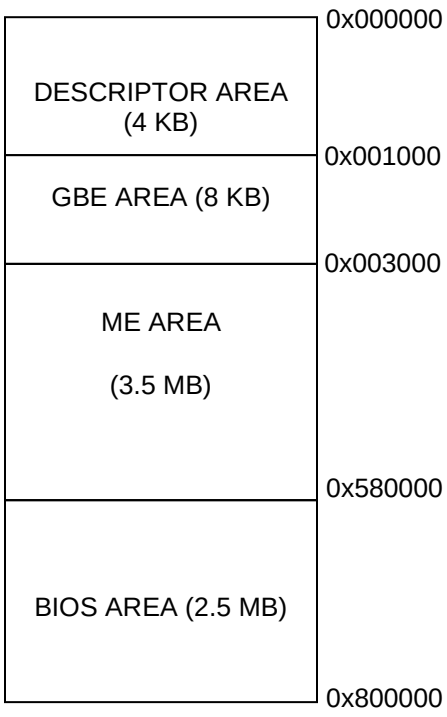


Figure 1 - SPI FLASH mapping (8 MB)

MAIN and RESCUE Flash should never by written by operating system unless to reprogram a new BIOS version. More detailed on SPI Flash mapping can be found in Intel document

- 445780_Intel_6SeriesExpressChipset_SPI_ProgGuide_Rev0_82 (NDA01)

SPI Flash datasheet is available into document

- spi64Mbits_S71392.pdf (NDA0) from SST

15.4 Intel ME module for Cougar Point PCH

The Cougar Point PCH integrates a firmware named M.E and flashed into the PCH by PCH vendor itself (Intel). The first 5M part of System Flash stores informations that are used and loaded by M.E at power on. Eventually BIOS or Operating System can communicates with M.E with a specific coded protocol by means of DMI bus (bus between Sandy Bridge and PCH). This feature is disabled into BIOS and not supported under our Operating System BSP.

15.5 Video BIOS

Video BIOS Table (VBT) is a binary image linked into the BIOS. The used VBIOS is v1973 (from AMI delivery). Kontron modifies this Image with a BMP tool (Binary Modification Program) with the following features:

- LVDS is disabled
- Display Port are configured In Integrated HDMI/Display Port Configuration
  - Device1 is Display Port B
  - Device 2 is Display Port D
  - Device 3 is Disabled

15.6 Software straps for Cougar point PCH

The PCH soft STRAPs are the one used by the Reference Platform with the following modifications:

PCH strap for VX3035	PCH strap for Intel reference platform
FLASH INFORMATION ME VSCC Device	
<WriteEraseFreq WriteEraseFreq="50MHz"	<WriteEraseFreq WriteEraseFreq="33MHz"
<MeVsccDevice MeVsccDevice="SST25VF032B">	<MeVsccDevice MeVsccDevice="AT26DF321">
<VendorId VendorId="0xBF"	<VendorId VendorId="0x1F"
<DeviceId0 DeviceId0="0x25"	<DeviceId0 DeviceId0="0x47"
<DeviceId1 DeviceId1="0x4A"	<DeviceId1 DeviceId1="0x00"
<MeVsccValue MeVsccValue="0x20092009"	<MeVsccValue MeVsccValue="0x20152015"
<MeVsccDevice MeVsccDevice="SST25VF064C">	<MeVsccDevice MeVsccDevice="W25Q64BV">
<VendorId VendorId="0xBF"	<VendorId VendorId="0xEF"
<DeviceId0 DeviceId0="0x25"	<DeviceId0 DeviceId0="0x40"
<DeviceId1 DeviceId1="0x4B"	<DeviceId1 DeviceId1="0x17"
<MeVsccValue MeVsccValue="0x200D200D"	<MeVsccValue MeVsccValue="0x20052005"
Part entirely removed	<MeVsccDevice name="MX25L6405L">
GPIO or LAN/PHY Configuration	
<LanPhyPcGp12Sel LanPhyPcGp12Sel="0 (General Purpose Output)" value_list="0 (General Purpose Output),,1 (Native mode)" edit="true" visible="true" name="LANPHYPC_GP12_SEL" help_text="0 = GPIO12 default is General Purpose (GP) output. 1 = GPIO12 is used in native mode as LANPHYPC."/>	<LanPhyPcGp12Sel LanPhyPcGp12Sel="1 (Native mode)" value_list="0 (General Purpose Output),,1 (Native mode)" edit="true" visible="true" name="LANPHYPC_GP12_SEL" help_text="0 = GPIO12 default is General Purpose (GP) output. 1 = GPIO12 is used in native mode as LANPHYPC."/>

PCH strap for VX3035	PCH strap for Intel reference platform
ME SMBUS	
<SmLink1Enable SmLink1Enable="false" edit="true" visible="true" name="SMLink1 Enable" help_text="Enables SMLink1."/>	<SmLink1Enable SmLink1Enable="true" edit="true" visible="true" name="SMLink1 Enable" help_text="Enables SMLink1."/>
PCH STRAP 9	
<PCIePortConf1 PCIePortConf1="11: 1x4 Port 1 (x4), Ports 2-4 (disabled)" value_list="00: 4x1 Ports 1-4 (x1),,01: 1x2, 2x1 Port 1 (x2), Port 2 (disabled), Ports 3, 4 (x1),,10: 2x2 Port 1 (x2), Port 3 (x2), Ports 2, 4 (disabled),,11: 1x4 Port 1 (x4), Ports 2-4 (disabled)" edit="true" visible="true" name="PCIe Port Configuration 1" help_text="These straps set the default value of PCIe Port Configuration 1 register covering PCIe ports 1-4."/>	<PCIePortConf1 PCIePortConf1="00: 4x1 Ports 1-4 (x1)" value_list="00: 4x1 Ports 1-4 (x1),,01: 1x2, 2x1 Port 1 (x2), Port 2 (disabled), Ports 3, 4 (x1),,10: 2x2 Port 1 (x2), Port 3 (x2), Ports 2, 4 (disabled),,11: 1x4 Port 1 (x4), Ports 2-4 (disabled)" edit="true" visible="true" name="PCIe Port Configuration 1" help_text="These straps set the default value of PCIe Port Configuration 1 register covering PCIe ports 1-4."/>
<PCIePortConf2 PCIePortConf2="01: 1x2, 2x1 Port 5 (x2), Port 6 (disabled), Ports 7, 8 (x1)" value_list="00: 4x1 Ports 5-8 (x1),,01: 1x2, 2x1 Port 5 (x2), Port 6 (disabled), Ports 7, 8 (x1),,10: 2x2 Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled),,11: 1x4 Port 5 (x4), Ports 6-8 (disabled)" edit="true" visible="true" name="PCIe Port Configuration 2" help_text="These straps set the default value of the PCI Express Port Configuration 2 register covering ports 5-8."/>	<PCIePortConf2 PCIePortConf2="00: 4x1 Ports 5-8 (x1)" value_list="00: 4x1 Ports 5-8 (x1),,01: 1x2, 2x1 Port 5 (x2), Port 6 (disabled), Ports 7, 8 (x1),,10: 2x2 Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled),,11: 1x4 Port 5 (x4), Ports 6-8 (disabled)" edit="true" visible="true" name="PCIe Port Configuration 2" help_text="These straps set the default value of the PCI Express Port Configuration 2 register covering ports 5-8."/>
MAC/PHY GBE Port on PCH	
<GbePciePortSelect GbePciePortSelect="110: Port 7" value_list="000: Port 1,,001: Port 2,,010: Port 3,,011: Port 4,,100: Port 5,,101: Port 6,,110: Port 7,,111: Port 8" edit="true" visible="true" name="Intel (R) PHY PCIe Port Select (PHY_PCIEPORTSEL)" help_text="Sets the default value of the PRC.GBEPCIERPSEL register which is used to determine which PCIe port to use for GBE MAC/PHY over PCI Express communication."/>	<GbePciePortSelect GbePciePortSelect="101: Port 6" value_list="000: Port 1,,001: Port 2,,010: Port 3,,011: Port 4,,100: Port 5,,101: Port 6,,110: Port 7,,111: Port 8" edit="true" visible="true" name="Intel (R) PHY PCIe Port Select (PHY_PCIEPORTSEL)" help_text="Sets the default value of the PRC.GBEPCIERPSEL register which is used to determine which PCIe port to use for GBE MAC/PHY over PCI Express communication."/>
PCH STRAP 10 ICC boot profile	
<DeepSx DeepSx="false" edit="true" visible="true"	<DeepSx DeepSx="true" edit="true" visible="true"

PCH strap for VX3035	PCH strap for Intel reference platform
name="Deep SX Enable" help_text="Deep SX refers to two low power states that are referred to Deep S4 and Deep S5."/>	name="Deep SX Enable" help_text="Deep SX refers to two low power states that are referred to Deep S4 and Deep S5."/>
PCH STRAP 11	
<SmLink1GpAddrEn SmLink1GpAddrEn="false" edit="true" visible="true" name="SMLink1 GP Target Address Enable" help_text="true: Address is enabled. false: Address is disabled."/>	<SmLink1GpAddrEn SmLink1GpAddrEn="true" edit="true" visible="true" name="SMLink1 GP Target Address Enable" help_text="true: Address is enabled. false: Address is disabled."/>
<SmLink1I2cAddrEn SmLink1I2cAddrEn="false" edit="true" visible="true" name="SMLink1 I2C Target Address Enable" help_text="true: Address is enabled. false: Address is disabled."/>	<SmLink1I2cAddrEn SmLink1I2cAddrEn="true" edit="true" visible="true" name="SMLink1 I2C Target Address Enable" help_text="true: Address is enabled. false: Address is disabled."/>
PCH STRAP 15	
<SlpLanGpio29Sel SlpLanGpio29Sel="true" edit="true" visible="true" name="SLP_LAN#/GPIO29 Select" help_text="false = GPIO29 can only used only as SLP_LAN# for Intel integrated LAN solution. true = GPIO29 is available for GPIO configuration"/>	<SlpLanGpio29Sel SlpLanGpio29Sel="false" edit="true" visible="true" name="SLP_LAN#/GPIO29 Select" help_text="false = GPIO29 can only used only as SLP_LAN# for Intel integrated LAN solution. true = GPIO29 is available for GPIO configuration"/>
LEWISVILLE	
<MinorVersion MinorVersion="13"	<MinorVersion MinorVersion="0"
<ImageId ImageId="3"	<ImageId ImageId="0"
ME REGION	
<InputFile InputFile="CPT_5M_Production.bin"	<InputFile InputFile="CPT_5M_Production.BIN"
<LanPowerWell LanPowerWell="0"	<LanPowerWell LanPowerWell="3"
<WlanPowerWell WlanPowerWell="0x80" WlanPowerWell="0x80,,0x82,,0x83,,0x84" edit="true" visible="true" name="WLAN Power Well Config" WlanPowerWell="0x80 = Disabled, 0x82 = Sus Well, 0x83 = ME Well, 0x84 = WLAN Power Controlled via SLP_M# || SPDA"/>	<WlanPowerWell WlanPowerWell="0x85" WlanPowerWell="0x80,,0x82,,0x83,,0x85" edit="true" visible="true" name="WLAN Power Well Config" WlanPowerWell="0x80 = Disabled, 0x82 = Sus Well, 0x83 = ME Well, 0x85 = WLAN Power Controlled via SLP_M# || SLP_ME_CSW_DEV#"/>
<M3PwrRailAvail M3PwrRailAvail="false" M3PwrRailAvail="true" visible="true" name="M3 Power Rails Availability" help_text="false = Not Available, true = Available"/>	<M3PwrRailAvail M3PwrRailAvail="true" M3PwrRailAvail="false" visible="true" name="M3 Power Rails Availability" help_text="false = Not Available, true = Available"/>
<PwrPkgs name="Power Packages"> <Package2 Package2="false" edit="true" visible="true" name="Power Pkg 2 Supported (Mobile: ON in S0, ME Wake in S3, S4-5 (AC	<PwrPkgs name="Power Packages"> <Package2 Package2="true" edit="true" visible="true" name="Power Pkg 2 Supported (Mobile: ON in S0, ME Wake in S3, S4-5 (AC

PCH strap for VX3035	PCH strap for Intel reference platform
only))" help_text="Power Package available or not. true = Available. false = Not available."/>	only))" help_text="Power Package available or not. true = Available. false = Not available."/>
<ManageAppPerm ManageAppPerm="Yes" value_list="No,,Yes" edit="true" visible="true" name="Manageability Application Permanently Disabled?"	<ManageAppPerm ManageAppPerm="No" value_list="No,,Yes" edit="true" visible="true" name="Manageability Application Permanently Disabled?"
POWER PACKAGE: Audio/TLS/Anti-Theft/Network Service ... DISABLED	
<KvmPerm KvmPerm="Yes" value_list="No,,Yes" KvmPerm="false" visible="true" name="KVM Permanently Disabled?" help_text="Select whether KVM is permanently disabled."/>	<KvmPerm KvmPerm="No" value_list="No,,Yes" KvmPerm="true" visible="true" name="KVM Permanently Disabled?" help_text="Select whether KVM is permanently disabled."/>
<TlsPerm TlsPerm="Yes" value_list="No,,Yes" edit="true" visible="true" name="TLS Permanently Disabled?" help_text="Select whether TLS is permanently disabled."/>	<TlsPerm TlsPerm="No" value_list="No,,Yes" edit="true" visible="true" name="TLS Permanently Disabled?" help_text="Select whether TLS is permanently disabled."/>
<ATPerm ATPerm="Yes" value_list="No,,Yes" edit="true" visible="true" name="Intel (R) Anti-Theft Technology Permanently Disabled?" help_text="Select whether Intel (R) Anti-Theft Technology is permanently disabled."/>	<ATPerm ATPerm="No" value_list="No,,Yes" edit="true" visible="true" name="Intel (R) Anti-Theft Technology Permanently Disabled?" help_text="Select whether Intel (R) Anti-Theft Technology is permanently disabled."/>
<MeNetworkService MeNetworkService="Yes" value_list="No,,Yes" edit="true" visible="true" name="Intel (R) ME Network Service Permanently Disabled?"	<MeNetworkService MeNetworkService="No" value_list="No,,Yes" edit="true" visible="true" name="Intel (R) ME Network Service Permanently Disabled?"
<ManageAppShipState ManageAppShipState="Disabled" value_list="Enabled,,Disabled" ManageAppShipState="false" visible="true" name="Manageability Application Enable/Disable"	<ManageAppShipState ManageAppShipState="Enabled" value_list="Enabled,,Disabled" ManageAppShipState="true" visible="true" name="Manageability Application Enable/Disable"
<MeDalPerm MeDalPerm="Yes" value_list="No,,Yes" edit="true" visible="true" name="Intel (R) DAL Permanently Disabled?" help_text="Select whether Intel (R) Dynamic Application Loader is permanently disabled."/>	<MeDalPerm MeDalPerm="No" value_list="No,,Yes" edit="true" visible="true" name="Intel (R) DAL Permanently Disabled?" help_text="Select whether Intel (R) Dynamic Application Loader is permanently disabled."/>
Clock Configuration	

PCH strap for VX3035	PCH strap for Intel reference platform
<SSCCTL SSCCTL="0x01010101" edit="true" visible="true" name="SSC Control" help_text="This parameter controls spread spectrum modulation capability of SSC blocks."/>	<SSCCTL SSCCTL="0x00000000" edit="true" visible="true" name="SSC Control" help_text="This parameter controls spread spectrum modulation capability of SSC blocks."/>

15.7 SPD EEPROM

Two SPD EEPROM on VX3035 contain the information for memory initialization. They are programmed during the factory process and are read by BIOS on SMbus (@ 0xA0, @0xA4) for memory initialization.

The SPD programming table is included into the BIOS source code and allows the BIOS to boot without reading the SPD (When boot is done with switch DEBUG mode ON) in minimal configuration or to program the SPD when the EEPROM are empty.

Possible RAM hardware option can be

---
1 Gb => MT41J128M8-15E 1 Gbit monolithiques 1067 MHz & 1333 MHz
2 Gb => MT41J256M8-15E 2 Gbits monolithiques 1067 MHz & 1333 MHz
4 Gb => MT41J512M8-15E 4 Gbits TwinDie 1067 MHz & 1333 MHz

SPD table to be written into EEPROM are selected automatically by BIOS command according to the CPLD RAM information and are the following:

```
/*-----------------------------------------------------------------------------*/
UINT8 SPD_1Gb_1067[MAX_SPD_ADDR] = {// SPD Table for 1 Gb monolithiques (Single-Die)
1067 MHz
0x92,               // 0
0x10,               // 1
0x0b,               // 2
0x02, // 3
0x02, // 4
0x11,               // 5
0x00,               // 6
0x01, // 7
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0f,               // 12
0x00,               // 13
0x1e,               // 14
0x00,               // 15
0x69,               // 16
0x78,               // 17
0x69,               // 18
0x3c,               // 19
0x69,               // 20
0x11,               // 21
0x2c,               // 22
0x95,               // 23
```

```
0x70,               // 24
0x03,               // 25
0x3c,               // 26
0x3c,               // 27
0x01,               // 28
0x2c,               // 29
0x82,               // 30
0x05,               // 31
0x80,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x03,               // 62
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0xf1,               // 126
0x25                // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_1Gb_1333[MAX_SPD_ADDR] = {// SPD Table for 1 Gb monolithiques (Single-Die)
1333 MHz
0x92,               // 0
0x00,               // 1
0x0b,               // 2
0x02, // 3
0x02, // 4
0x11,               // 5
0x00,               // 6
0x01, // 7
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0c,               // 12
0x00,               // 13
0x3e,               // 14
0x00,               // 15
0x6c,               // 16
0x78,               // 17
0x6c,               // 18
0x30,               // 19
0x6c,               // 20
0x11,               // 21
0x20,               // 22
0x8c,               // 23
0x70,               // 24
0x03,               // 25
0x3c,               // 26
```

```
0x3c,               // 27
0x00,               // 28
0xf0,               // 29
0x82,               // 30
0x05,               // 31
0x00,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x04,               // 62
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0xf1,               // 126
0x25                // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_2Gb_1333[MAX_SPD_ADDR] = {// SPD Table for 2 Gb monolithiques (Single-Die)
1333 MHz
0x92,               // 0
0x00,               // 1
0x0b,               // 2
0x02, // 3
0x03, // 4
0x19,               // 5
0x00,               // 6
0x01, // 7
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0c,               // 12
0x00,               // 13
0x3e,               // 14
0x00,               // 15
0x6c,               // 16
0x78,               // 17
0x6c,               // 18
0x30,               // 19
0x6c,               // 20
0x11,               // 21
0x20,               // 22
0x8c,               // 23
0x00,               // 24
0x05,               // 25
0x3c,               // 26
0x3c,               // 27
0x00,               // 28
0xf0,               // 29
```

```
0x82,               // 30
0x05,               // 31
0x00,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x04,               // 62
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0x27,               // 126
0xba                // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_2Gb_1067[MAX_SPD_ADDR] = {// SPD Table for 2 Gb monolithiques 1067 MHz
0x92,               // 0
0x10,               // 1
0x0b,               // 2
0x02, // 3
0x03, // 4
0x19,               // 5
0x00,               // 6
0x01, // 7
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0f,               // 12
0x00,               // 13
0x1e,               // 14
0x00,               // 15
0x69,               // 16
0x78,               // 17
0x69,               // 18
0x3c,               // 19
0x69,               // 20
0x11,               // 21
0x2c,               // 22
0x95,               // 23
0x00,               // 24
0x05,               // 25
0x3c,               // 26
0x3c,               // 27
0x01,               // 28
0x2c,               // 29
0x82,               // 30
0x05,               // 31
0x80,               // 32
0x00,               // 33
```

```
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x03,               // 62
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0x27,               // 126
0xba,               // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_4Gb_Dual_1333[MAX_SPD_ADDR] = {// SPD Table for 4 Gb Twin-Die 1333 MHz
0x92,               // 0
0x00,               // 1
0x0b,               // 2
0x02, // 3
0x03, // 4
0x19,               // 5
0x00,               // 6
0x09, // 7
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0c,               // 12
0x00,               // 13
0x3e,               // 14
0x00,               // 15
0x6c,               // 16
0x78,               // 17
0x6c,               // 18
0x30,               // 19
0x6c,               // 20
0x11,               // 21
0x20,               // 22
0x8c,               // 23
0x60,               // 24
0x09,               // 25
0x3c,               // 26
0x3c,               // 27
0x00,               // 28
0xf0,               // 29
0x82,               // 30
0x05,               // 31
0x00,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
```

```
0x00,               // 38
0x03,               // 62
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0x88,               // 126
0x22                // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_4Gb_Single_1333[MAX_SPD_ADDR] = {// SPD Table for 4 Gb Single Rank 1333 MHz
0x92,               // 0
0x00,               // 1
0x0b,               // 2
0x02, // 3
0x04, // 4 - 4 Gb
0x19,               // 5
0x00,               // 6
0x01, // 7 - single rank
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0c,               // 12
0x00,               // 13
0x3e,               // 14
0x00,               // 15
0x6c,               // 16
0x78,               // 17
0x6c,               // 18
0x30,               // 19
0x6c,               // 20
0x11,               // 21
0x20,               // 22
0x8c,               // 23
0x60,               // 24
0x09,               // 25
0x3c,               // 26
0x3c,               // 27
0x00,               // 28
0xf0,               // 29
0x82,               // 30
0x05,               // 31
0x00,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x04,               // 62 : UDIMM Type E
0x00,               // 63
0x00,               // 64
```

```
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0x88,               // 126
0x22                // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_4Gb_Dual_1067[MAX_SPD_ADDR] = {// SPD Table for 4 Gb Twin-Die 1067 MHz
0x92,               // 0
0x10,               // 1
0x0b,               // 2
0x02, // 3
0x03, // 4
0x19,               // 5
0x00,               // 6
0x09, // 7
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0f,               // 12
0x00,               // 13
0x1e,               // 14
0x00,               // 15
0x69,               // 16
0x78,               // 17
0x69,               // 18
0x3c,               // 19
0x69,               // 20
0x11,               // 21
0x2c,               // 22
0x95,               // 23
0x60,               // 24
0x09,               // 25
0x3c,               // 26
0x3c,               // 27
0x01,               // 28
0x2c,               // 29
0x82,               // 30
0x05,               // 31
0x80,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x03,               // 62
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
```

```
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
0x00,               // 125
0x88,               // 126
0x22,               // 127
};
/*-------------------------------------------------------------------------------*/
UINT8 SPD_4Gb_Single_1067[MAX_SPD_ADDR] = {// SPD Table for 4 Gb Single Rank 1067 MHz
0x92,               // 0
0x10,               // 1
0x0b,               // 2
0x02, // 3
0x04, // 4 - 4 Gb
0x19,               // 5
0x00,               // 6
0x01, // 7 - single rank
0x0b,               // 8
0x52,               // 9
0x01,               // 10
0x08, // 11
0x0f,               // 12
0x00,               // 13
0x1e,               // 14
0x00,               // 15
0x69,               // 16
0x78,               // 17
0x69,               // 18
0x3c,               // 19
0x69,               // 20
0x11,               // 21
0x2c,               // 22
0x95,               // 23
0x60,               // 24
0x09,               // 25
0x3c,               // 26
0x3c,               // 27
0x01,               // 28
0x2c,               // 29
0x82,               // 30
0x05,               // 31
0x80,               // 32
0x00,               // 33
0x00,               // 34
0x00,               // 35
0x00,               // 36
0x00,               // 37
0x00,               // 38
0x04,               // 62 : UDIMM Type E
0x00,               // 63
0x00,               // 64
0x80,               // 117
0x2c,               // 118
0x00,               // 119
0x00,               // 120
0x00,               // 121
0x00,               // 122
0x00,               // 123
0x00,               // 124
```

```
0x00,               // 125
0x88,               // 126
0x22                // 127
};
```

16 I2C DEVICES

16.1 EEPROMs

EEPROMs are accessible on I2C bus 2 at addresses 0xA0 and 0xA2. The VPD EEPROM I2C @A0 is reserved for Board Information (VPD) and PBIT result and configuration.

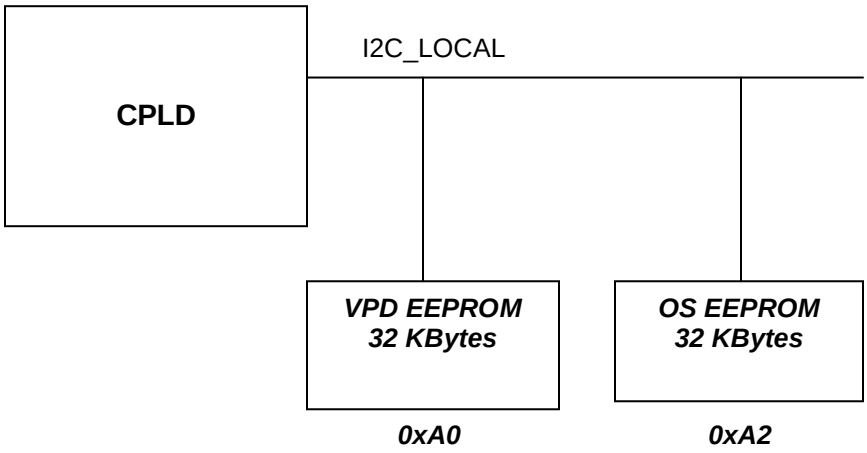


Figure 2 - VX3035 EEPROMs on CPLD i2C bus

16.1.1 VPD EEPROM @I2C 0xA0

Figure 3 - gives the mapping content of the VPD EEPROM I2C @A0

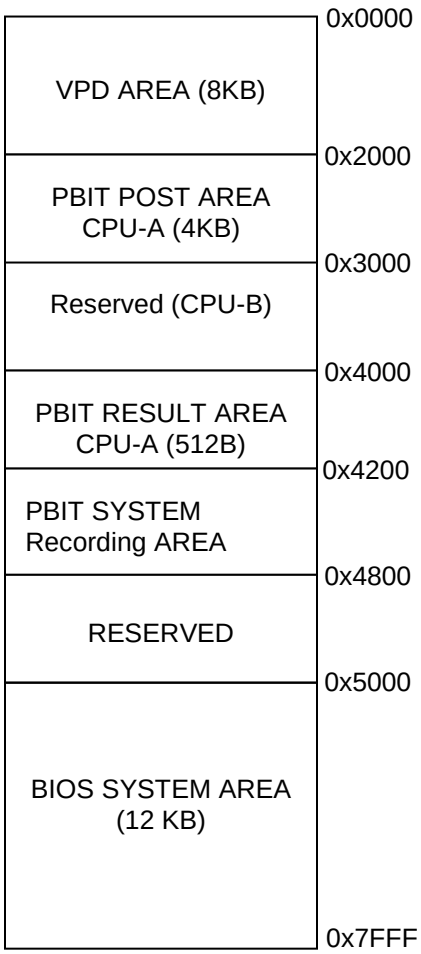


Figure 3 - VPD EEPROM mapping

Figure 4 - gives a detailed description for VPD area itself into VPD EEPROM

Offset		Contents
0x0	HEADER (32 Bytes)	"KONTRON MODULAR COMPUTERS SAS"
0x20	ORDER CODE (32 Bytes)	Order Code
0x40	EC LEVEL (8 Bytes)	EC Level
0x48	SERIAL NUMBER (32 Bytes)	Serial Number
0x68	VARIANT (20 Bytes)	Variant
0x7C	CRC (4 bytes)	CRC
0x80	PADDING (112 Bytes)	
0xF0	MAGIC (16 Bytes)	"CPLD AREA"
0x100	Reg 0x05 CPLD	Reg 0x05 CPLD
0x101	Reg 0x06 CPLD	Reg 0x06 CPLD
0x102	BOARD CONFIG 1	Reg 0x0C CPLD
0x103	BOARD CONFIG 2	Reg 0x0D & 0x70 CPLD
0x104	0x00	
0x11C	CRC (4 Bytes)	CRC

Figure 4 - VPD EEPROM Layout

If VPD or PBIT information need to be accessed from any Operating System then source code example with pre-defined used C structures must be asked to Kontron. These structures and access code example will guarantee the correct VPD or PBIT EEPROM information decoding.

16.1.2 OS EEPROM @I2C 0xA2

This EEPROM is free for OS and is not used by BIOS or PBIT. It must be accessed by CPLD I2C driver. Just note that if with a VxWorks Kontron VX3035 BSP then the first 256 bytes are used for storing VxWorks bootrom parameters.
Both previous EEPROMs data sheet are available on Internet looking at 24FC256 datasheet.

16.2 F-RAM @I2C 0xA4

A Ferro-electric RAM, F-RAM, 64 Ko size is also available on I2C bus 2 at address 0xA4. It must be accessed by CPLD I2C driver as for EEPROM device. This F-RAM is free for OS and is not used by BIOS or PBIT.

F-RAM and EEPROM will use the same I2C protocol driver. Anyways for information, F-RAM data-sheet from RAMTRON can be found in **FM24V05ds_r1.1[1].pdf**

16.3 LM73

One LM73 thermal sensors is also available on CPLD I2C bus number 2. Bus speed is 100 kHz when LM73 is accessed instead of 1Mz for EEPROMs and F-RAM. LM73 I2C address is 0x90.

LM73 datasheet from National Semiconductor is available on Web.

17 CPLD REGISTERS

CPLD registers are described in this chapter (NDA0). CPLD is accessible by PCH LPC bus from I/O address 0x800.

Sources code example on how to program CPLD I2C or other CPLD features can be provided by KOM-SAS when asked (BIOS, Linux, vxWorks sources).

CPLD registers describing is based on internal Kontron document FT.SF.212-14e.

17.1 Overview

Offset	Name	Access	Reference
0x00	CPLD ID	R	Board Implementation
0x01	PCB ID	R	Board Implementation
0x02	Firmware POST Result	RW	Power Management
0x03	Debug POST	RW	Power Management
0x04	Power/Reset Configuration	RW	Power Management
0x05	VPD BC1	R	Memory & Secure
0x06	VPD BC2	R	Memory & Secure
0x07	Serial Lines	RW	Serial Lines Configuration N/A for VX3035
0x08	PCI Mode	RW	PCI Mode Configuration
0x09	Write Protect Control / Flash Configuration	RW	Memory & Secure
0x0A	COM TX	RW	Communication
0x0B	COM RX	RW	Communication
0x0C	Board Configuration	RW	Board Ports/DIP
0x0D	PCI mode / DRAM config	RW	Board Ports/DIP Control
0x0E	Board DIP switch Control	R	Board Ports/DIP Control
0x0F	SERIRQ Control and Status	RO/RW	Serial IRQ
0x10	I2C0_PreScaleLow	RW	I2C Master/Slave
0x11	I2C0_PreScaleHigh	RW	I2C Master/Slave
0x12	I2C0_Ctrl	RW	I2C Master/Slave
0x13	I2C0_Receive	R	I2C Master/Slave
	I2C0_Transmit	W	I2C Master/Slave
0x14	I2C0_Status	R	I2C Master/Slave

Offset	Name	Access	Reference
	I2C0_Cmd	W	I2C Master/Slave
0x15	I2C0_Interrupt	RW	I2C Master/Slave
0x16-0x1F	Reserved		
0x20	I2C1_PreScaleLow	RW	I2C Master Only
0x21	I2C1_PreScaleHigh	RW	I2C Master Only
0x22	I2C1_Ctrl	RW	I2C Master Only
0x23	I2C1_Receive	R	I2C Master Only
	I2C1_Transmit	W	I2C Master Only
0x24	I2C1_Status	R	I2C Master Only
	I2C1_Cmd	W	I2C Master Only
0x25	I2C1_Interrupt	RW	I2C Master Only
0x26-0x2F	Reserved		
0x30	I2C2_PreScaleLow	RW	I2C Master Only
0x31	I2C2_PreScaleHigh	RW	I2C Master Only
0x32	I2C2_Ctrl	RW	I2C Master Only
0x33	I2C2_Receive	R	I2C Master Only
	I2C2_Transmit	W	I2C Master Only
0x34	I2C2_Status	R	I2C Master Only
	I2C2_Cmd	W	I2C Master Only
0x35	I2C2_Interrupt	RW	I2C Master Only
0x36-0x4F	Reserved		
0x50	Timer Byte0	R	Timers
0x51	Timer Byte1	R	Timers
0x52	Timer Byte2	R	Timers
0x53	Timer Byte3	R	Timers
0x54	Timer Control	RW	Timers
0x55	Watchdog Value	RW	Watchdog
0x56	Watchdog Control	RW	Watchdog
0x57-0x5A	Reserved		
0x5B	Alert Control & Status	RW	Alert

Offset	Name	Access	Reference
0x5C-0x5F	Reserved		
0x60	GPIO_Control	RW	
0x61	GPIO_DataOut	RW	
0x62	GPIO_In	RW	
0x63	GPIO_IntMask	RW	
0x64	GPIO_IntPolarity	RW	
0x65	GPIO_IntMode	RW	
0x66	GPIO_IntToggle	RW	
0x67	GPIO_IntStatus	RW	
0x68-0x69	Reserved		
0x6A	GA / SYSCON	R	Geographical Address
0x6B	GAGPIO	RW	Geographical Address
0x6C-0x6F	Reserved		
0x70	VPX/VME Control	RW	VPX/VME Registers facilities
0x71	PCIe Switch VPX (VPX Only)	RW	VPX/VME Registers facilities
0x72	I2C_BOARD_STATUS	RW	VPX/VME Registers facilities
0x73	I2C_BOARD_CONTROL	RW	VPX/VME Registers facilities
0x74	I2C_ERROR_STATUS	RW	VPX/VME Registers facilities
0x75	I2C_PORT80	RW	VPX/VME Registers facilities
0x76	I2C_FAILCODE	RW	VPX/VME Registers facilities
0x77	I2C_SCRATCHPAD	RW	VPX/VME Registers facilities
0x78-0x7F	Reserved		
0x80	LEDs User Configuration	RW	LEDs Control
0x81	LEDs User Control	RW	LEDs Control
0x82-0x8F	Reserved		
0x9A-0x9F	Reserved		
0xA6-0xFF	Reserved		

17.2 Detailed description

17.2.1 Identification

CPLD_ID @ 0x00				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*CPLD_ID*	**CPLD Identification** 0 CPLD A 1 CPLD B (for CPLD B of double sided boards such as VX6060) (This information is issue from 3Ux_PLD_CFG0_NUM input)	N.A	RO
6	*CPLD_Debug*	**Debug version** 0 official CPLD version 1 debug version	N.A	RO
5-0	*CPLD_Version*	**Version Number**	N.A	RO

This version value starts with 0x01 and will be incremented with each change in the CPLD as development continues.

PCB_ID @ 0x01				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*Board_ID*	**Board Identification** 0x60 = VX6060 (6U Board) 0x30 = VX3030 (3U Board) 0x35 = VX3035 (3U Board) 0x50 = VM6050 (6U Board) 0x42 = VX3042 0x44 = VX3044	N.A	RO

17.2.2 POST

FIRM_POST @ 0x02 This Register is initialized only on PWRG_P3V3SB low level				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-1	*PBIT_FAIL*	**ID number of first failing test (updated by PBIT)** 0 No test failed. Any other value indicates ID number of the first failing test	0x00	RW
0	*PBIT_RUN*	**PBIT run (updated by PBIT)** 0 PBIT has not run 1 PBIT has run	0	RW

Examples:

0x00 means Test NOT RUN
0x03 means ALL TESTS RUN and TEST 1 FAIL
0x61 means ALL TESTS RUN and Test 48 FAIL (48 = 0x30, 0x30 << 1 => 0x60)
0x01 means All Test PASSED

PWON_STATUS @ 0x03				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-4	*DPOST*	**Debug Power-On Status** Currently unused	0x00	RW
3	*NMODE_REFRESH_TIME*	**NMODE refresh time for DDR3 (updated by BIOS)** 0 : x2 (64 mS on SA boards) 1 : x1 (32 mS on WA/RA/RC boards)	0	RW
2	*LS_EEPROM*	**EEPROMs on high speed I2C2 clock (updated by BIOS)** 0 : EEPROMs at 0x50 (VPD) and 0x51 (user) (7bit addresses) are connected to the high speed I2C2 clock 1 : EEPROMs are connected to the low speed I2C2 clock	0	RW
1	*EXT_RTC*	**External RTC** 0 : only PCH internal RTC is used 1 : an additional external RTC is used	0	RW
0	*POST_RTC*	**RTC POST status (updated by BIOS)** 0 POST OK 1 POST FAILED (weak or missing battery)	0	RW

17.2.3 Power Management

PWR_RST_CONFIG @ 0x04				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*PWRON_MODE*	**Power Mode** 0 Power-on when VPX power present 1 Not power-on when VPX power present If this bit is 0, the board is automatically powered-on when VPX power is applied If this bit is 1 : the board remain in standby mode while not powered-on by reg 0x73 bit 0, and then can be switched on/off by the same bit. Value read from POWER_MODE DIP switch (SW2[2], using 3UA_PLD_PWRON_MODE inverted signal State). 0 when switch off; 1 when on. See reg 0x73 bit 0 for power on/off management.	N.A	RO
6	*PLTRST_To_PERST3u_Disable*	**PLTRST Propagation To 3U** 0 Enable PLTRST# propagation to PERST3u# output 1 Disable PLTRST# propagation to PERST3u# output **On VX3035 Rev >= 4** : this bit also controls the propagation of PEX reset from bit 1	0	RW
5	*Alarm_Inhib*	**Alarm Inhibition** 0 Power off in case of Alert 1 No power off in case of Alert Alerts are : THERM_PROT#, THRMTRIP# , or CATERR#; see register 0x5B for their current status.	1	RW

PWR_RST_CONFIG @ 0x04				
4	*PLTRST_To_PERST6u_Disable*	**PLTRST Propagation To 6U (Only for VX6060)** 0 Enable PLTRST# propagation to PERST6u# output 1 Disable PLTRST# propagation to PERST6u# output	0	RW
3	*PEXNT_RST*	**PEX non transparent reset #0 (Only for VX3040)** 0 Reset 1 Unreset if bit 1 is set to 1 This bit is reset when backplane power is applied and at each board reset ((PLD_PLTRST_n)	0	RW
2	*PEXNT1_RST* *or* *XMC_RESET*	**PEX non transparent reset #1 (Only for VX3040)** **OR** **XMC reset (Only for VX3030 Rev >= 0x10)** **-- PEX non transparent reset #1 (Only for VX3040) :** 0 Reset (default) 1 Unreset if bit 1 is set to 1 This bit is reset when backplane power is applied and at each board reset ((PLD_PLTRST_n) **-- XMC reset (Only for VX3030 Rev >= 0x10)** 0 : XMC_RST# asserted if PLTRST# is asserted 1 : XMC_RST# asserted (default)	0 or 1	RW
1	*PERSTb Control*	**PERST_3U# Control (and PERST_6U# on VX6060)** 0 Assert PERST_3U# (and PERST_6U#). See also bit 6. 1 Assert PERST_3U# when PLTRST# is asserted if bit 6 is 0 (also PERST_6U# when PLTRST# is asserted if bit 4 is 0) **On VX3035 Rev>=4** : this bit is reset when backplane power is applied and at each board reset (PLD_PLTRST_n). **On VX3035 Rev < 4** : this bit is reset only when backplane power is applied	0	RW
0	*Software Cross Reset*	**Reset to the other side: CPLD_A(B) resets 3UB(A) (Only for VX6060)** 0 Reset asserted 1 Reset deasserted State of this bit is propagated to other CPLD via COM17 (A to B) or COM07 (B to A) to generate an equivalent of RST_BP# input signal. This bit is automatically set to 1 after it has been written to 0	1	RW

This register controls the power-on and reset modes.

17.2.4 Configuration VPDs

VPD_BC1 @ 0x05				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*BC1*	BC1 VPD board configuration word loaded from VPD EEPROM	N.A	RO

This has a copy of the VPD EEPROM at offset @0x0100
If FACTORY_MODE is enable this register is not loaded with EEPROM value

VPD_BC2 @ 0x06				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*BC2*	BC2 VPD board configuration word loaded from VPD EEPROM	N.A	RO

This has a copy of the VPD EEPROM at offset @0x0101
If FACTORY_MODE is enable this register is not loaded with EEPROM value

17.2.5 Memory & Secure

MEM_PROTECT @ 0x09 This Register is initialized only on PWRG_P3V3SB low level				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*Boot flash CS swap DIP*	**Boot flash chip select configuration** (from switch) 0 Normal configuration (CS0 is the boot device) (switch off) 1 Rescue configuration (CS1 becomes the boot device)	N/A	RO
6	*Boot flash CS swap Valid#*	**Operator Boot flash chip select configuration** IN USER MODE: This bit is hidden and set a 0 IN OPERATOR MODE: This bit is accessible 0 Boot flash CS swap DIP (bi7) has valid value 1 Invert value of boot flash CS swap DIP (bi7)	0	WR hidden
5	*Both boot flash*	**Operator Boot double flash configuration** IN USER MODE : This bit is hidden and set a 0 IN OPERATOR MODE : This bit is accessible 0 Boot flash 0 only 1 Boot flash 0 and 1	0	WR hidden
4	*SSD_WP*	**N/A for VX3035: Onboard SSD WriteProtect hardware protection** Default value is read from the SW1[5] switch. This bit is **NOT** forced to 1 when bit 0 = 1. 0 No protection (switch off) 1 Protected (PLD_SSD_WP_n from switch SW1[5] and PLD_SATA_WP_n to SSD)	N/A	WR
3	*USER WP*	**User level WriteProtect hardware protection** default value is read from a switch. This bit is forced to 1 when	N/A	RW

MEM_PROTECT @ 0x09 **This Register is initialized only on PWRG_P3V3SB low level**				
		bit 0 = 1. 0 No user level protection (switch off) 1 User level WriteProtect active Protection of OS FRAM at SMB addr 0xA4/A5, Geth switch EEPROM, PCIe switch EEPROM memories). (3AB_PLD_USER_WP open drain and 3xx_PLD_SPI_WP signals)		
2	*SYS WP*	**System level WriteProtect hardware protection** **This bit is forced to 1 when bit 0 = 1** read from a switch 0 No system level protection (switch off) 1 System Level protection active Protection of EEPROM at SMB addr 0xA2/A3, and SPI boot flash memories. (3AB_PLD_SYS_WP open drain and 3Ux_PLD_SPI0_WP, 3Ux_PLD_SPI1_WP)	N/A	RW
1	*VPD WP*	**VPD level WriteProtect hardware protection** **This bit is forced to 1 when bit 0 = 1** read from a switch 0 No VPD level protection (switch off) 1 VPD level protection active Protection of VPD EEPROM at SMB addr 0xA0/A1 (3AB_PLD_VPD_WP open drain signal)	N/A	RW
0	*NVMRO*	**VPX NVMRO** 0 non-volatile memories are write enable 1 non-volatile memories are write protected	(1)	RW (1)

(1) :
Write 1 to this bit to force write protection on local memory devices overridden by this bit if VPX NVMRO is inactive (devices not yet protected).
But writing 0 if VPX NVMRO is active has no effect (devices remain protected).
When reading, the current VPX NVMRO value is returned, or 1 if the last value written to this bit was 1.
NOTE : SSD_WP, USER_WP, SYS_WP, VPD_WP can only protect a device that is not already protected by switch or NVMRO, but can not unprotect a device that is already protected.

17.2.6 Communication facilities

These registers are only needed on VX6060, but kept on VX3030, VX3035, and VM6050 for software compatibility (software can still get the semaphore even if not needed because only one CPLD).
Do not use these registers for new VX3030, VX3035, VM6050 designs.
On VX3035 Rev >= 4 : all unused cross cPLD communication code from VX6060 has been removed to save some space. However a dummy semaphore has been implemented so that software still using these registers should work as-is.

COM_TX @ 0x0A				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*Semaphore*	**Semaphore status** 0 Shared Semaphore is free 1 Shared Semaphore is Busy	0	RW
6-0	*Data*	**Data or Task Identifier**	0	RW

COM_RX @ 0x0B				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*Data*	**Data** Read : value of register @A of the other PLD Write: unconditional write on register @A of this PLD	0	RW

17.2.7 Configuration

BOARD Configuration @ 0x0C				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*Port D mode*	**Ibex Port D Display mode** 0 Display port mode selected 1 HDMI port mode selected Directly Set 3Ux_PLD_DPD_AUX_OE# output signal state	0	RW
6	*Port B mode*	**Ibex Port B Display mode** 0 Display port mode selected 1 HDMI port mode selected Directly Set 3Ux_PLD_DPB_AUX_OE# signal state	0	RW
5	*ESW LAN CON*	**ETH-SW LAN connector configuration (VX6060 ONLY)** 0 Front panel : 1 VPX rear panel (ESW_SEL_FRONT_N ouput)	0	RW
4	*HANK LAN CON*	**ETH-A LAN connector configuration** 0 Front panel : 1 Not-front panel (on central on-board switch) (HANK_SEL_FRONT# ouput)	0	RW

BOARD Configuration @ 0x0C				
3	*USBSW_SEL*	**USB switch configuration (VX6060 ONLY)** 0 USB B side front panel connector connected to CPU B. It should be set on both CPLD-A & B to be active at 0. 1 USB B side front panel connector connected to CPU A. Set in one CPLD (A or B) is enough to be active at 1. (3AB_PLD_USBSW_SEL signal is set to "1" or "HiZ" with external pulldown) Read displays the state of 3AB_PLD_USBSW_SEL Board signal	1	RW
2	*SERIAL1 Mode*	**SERIAL1 mode** 0 RS232 1 RS422/485 (3UA_PLD_MN2403_MODE signal)	0	RW
1	*SERIAL2 Mode*	**SERIAL2 mode** 0 RS232 1 RS422/485 (3UA_PLD_MN2404_MODE signal)	0	RW
0	*SERIAL2 cfg*	**SERIAL2 configuration (VX6060 ONLY)** 0 CPU Serial2 links not connected 1 CPU Serial2 links connected	0	RW

At the Power ON this register is loaded with **VPD EEPROM byte offset @0x0102**
If FACTORY_MODE is enable this register is not loaded with EEPROM value

PCI Mode @ 0x0D This Register is initialized only on PWRG_P3V3SB low level				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*DRAM_CHANNEL*	**DRAM CHANNEL** From 3Ux_PLD_CFG4 0 = Single CHANNEL (bank) 1 = Dual CHANNEL (bank)	N/A	RO
6	*DRAM_RANK*	**DRAM RANK** From 3Ux_PLD_CFG3 0 = Dual RANK 1 = Single RANK	N/A	RO
5-4	*DRAM_SIZE*	**DRAM SIZE** From [3Ux_PLD_CFG2, 3Ux_PLD_CFG1] 00 = reserved 01 = 4 GB 10 = 2 GB 11 = 1 GB	N/A	RO
3	*PCI BUSMODE*	**PMC BUSMODE1:** 0 = PMCB board is connected 1 = PMCB board is not present	N/A	RO
2	*PCI M66EN*	**PMC M66EN:** 0 = PCI freq forced to 33Mhz 1 = PCI freq not forced to 33Mhz (1= HZ signal) **At the PowerOn, this register is loaded with EEPROM value (Byte at offset @0x0103 – bit 5)** **If FACTORY_MODE is enable this register is not loaded with EEPROM value an its value is 0x01**	1	RW
1	*PCIXCAP*	**PCIXCAP configuration mode:** 0 = PCI forced to conventional mode 1 = PCI mode depends on PCIXCAP status Note: This bit is not a status bit. **At the PowerOn, this register is loaded with EEPROM value (Byte at offset @0x0103– bit 4)** **If FACTORY_MODE is enable this register is not loaded with EEPROM value an its value is 0x01**	1	RW
0	*PCISEL100*	**PCIX frequency:** 0 = PCI frequency for 33/66/133 MHz 1 = PCI frequency for 25/50/100 MHz (1= HZ signal) **At the PowerOn, this register is loaded with EEPROM value (Byte at offset @0x0103 – bit 3)** **If FACTORY_MODE is enable this register is not loaded with EEPROM value an its value is 0x01**	0	RW

DIP Switch State @ 0x0E				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-4	*USER_DIP*	3AB_PLD_USER[4:1] signal status	N/A	RO
3	*Res.*	Reserved	0	RO
2	*SP2*	3Ux_PLD_SP2 signal status (SW2)	N/A	RO
1	*SP1*	3Ux_PLD_SP1 signal status (SW2)	N/A	RO
0	*FACTORY_MODE*	FACTORY_MODE: 0: normal operation 1: Factory mode	N/A	RO

17.2.8 Serial IRQ

Serial IRQ register

SERIRQ_Control @ 0x0F				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*Smb_Msk*	**SMB_ALERT Mask** 1 = interrupt is masked 0 = Interrupt not masked Interrupt from backplane SMB_ALERT_n (Gdiscrete signal on VPX boards). The current status of the alert can be read from reg 0x70 (Smb_Alert_Status bit)	1	RW
6	*Alert_Msk*	**ALERT Mask** 1 = interrupt is masked 0 = Interrupt not masked This bit when set to 1 forces Alert_Int to 0 (interrupt released), however this does not clear the interrupt source that remains active as long as the alert condition is still present, so if this bit is set back to 0 another interrupt is generated. See reg 0x5B bit 3 for current alert status. **On VX3035**: alert is from SMBTEMP_ALERTb, or PLD_PECI_ALERT_n **On other boards** : alert is from SMBTEMP_ALERTb	1	RW
5	*Tip_Msk*	**TIP_1Second Mask** 1 = interrupt is masked 0 = Interrupt not masked	1	RW
4	*Gpios_Int*	**GPIOs Interrupt Status** 1 = GPIO interrupt occurred 0 = No interrupt occurred This interrupt status can be cleared through GPIOs registers	0	RO
3	*Smb_Int*	**SMB_ALERT Interrupt Status** 1 = SMB_ALERT occurred 0 = No interrupt occurred **Write 0 to clear**	0	RW
2	*Alert_ Int*	**ALERT Interrupt Status** 1 = ALERT interrupt occurred 0 = No interrupt occurred See Alert_Msk bit 6 above. Cleared when alert disappears or is masked-out by bit 6	0	RO
1	*Tip_ Int*	**TIP 1s Interrupt Status** 1 = TIP interrupt occurred 0 = No interrupt occurred **Write 0 to clear**	0	RW
0	*Wdg_ Int*	**Watchdog Interrupt Status** 1 = Watchdog interrupt occurred 0 = No interrupt occurred This interrupt status can be cleared through register 0x56	0	RO

Serial IRQ routing

Pin	Usage
IRQ0	Reserved
IRQ1	Reserved
IRQ2	Reserved
IRQ3	Reserved
IRQ4	Reserved
IRQ5	**Watchdog Alert**
IRQ6	**I2C Interrupt**
IRQ7	Reserved
IRQ8	Reserved
IRQ9	Reserved
IRQ10	**TIP_1second**
IRQ11	**SMB ALERT or SMBTemp ALERT**
IRQ12	**GPIOs Interrupt**
IRQ13	Reserved
IRQ14	Reserved
IRQ15	Reserved
IRQ16	Reserved
IRQ17	Reserved
IRQ18	Reserved
IRQ19	Reserved

17.2.9 Low speed I2C buses

I2C0 is for backplane bus routed to all boards; also called IPMB bus
I2C1 if for backplane bus routed to the chassis; also called SMB bus

I2C0_PreScaleLow @ 0x10 **I2C1_PreScaleLow @ 0x20**				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*I2C_PresScale_Low*	This register is used for programming the SCL low-speed frequency. The frequency will be 33 MHz clock divided by **4** and by this register value. **VX3035 Rev >= 4**: this register is read/write to be able to modify the clock frequency used for these backplane buses **Other versions** : read-only	'h60	RO RW

I2C0_PreScaleHigh @ 0x11 **I2C1_PreScaleHigh @ 0x21**				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*I2C_PresScale_High*	This register is used for programming the SCL High-speed frequency. The frequency will be 33 MHz clock divided by **4** and by this register value. **THIS REGISTER IS UNUSED** (only for high speed buses)	'h0A	RO

When implemented for write access, these registers are used to prescale the SCL clock line, capable for two SCL speeds to quickly swap between them.

I2C0_Control @ 0x12 I2C1_Control @ 0x22				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C_Enable*	**I2C Interface enable bit** This bit must be set before any other control bit has any effect If this bit is set then all state machines will go into reset state. 1 I2C is enabled. 0 I2C is disabled.	0	RW
6	*Reserved*	*Reserved*	0	RW
6	~~*I2C_IntEnb*~~	~~**I2C Interface interrupt enable bit.**~~ ~~1 interrupt is enabled.~~ ~~0 interrupt is disabled.~~	~~0~~	~~RW~~
5	*Reserved*	*Reserved*	0	RW
5	~~*I2C_HighSpeed*~~	~~**I2C clock Selection for Low or High Speed**~~ ~~1 High-Speed SCL defined by *I2C_PreScaleHigh* Register~~ ~~0 Low-Speed SCL defined by *I2C_PreScaleLOWh* Register~~	~~0~~	~~RW~~
4	*Reserved*	*Reserved*	0	RW
4	~~*I2C_Slave*~~	~~**I2C configuration as slave or master.**~~ ~~When run as slave, its slave address is done by the Geographical Address signals: slave address = {0,0,GA[4:0]}~~	~~0~~	~~RW~~
3-0	*Reserved*	*Reserved*	0	RW

I2C0_Transmit @ 0x13 I2C1_Transmit @ 0x23				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-1	*I2C_Data[7:1]*	This represents the 7 MSB for a data transaction	N.A	W
0	*I2C_Data[0]*	This bit represents the data's LSB. This bit represents the RW bit during slave address transfer "1" Reading from slave "0" Writing to Slave	N.A	W

I2C0_Receive @ 0x13 I2C1_Receive @ 0x23				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*I2C_Data[7:0]*	I2c Data byte	N.A	R

The **Transmit Register** and the **Receive Register** share the same address depending on the direction of data transfer. The data to be transmitted via I2C will be stored in the transmit Register, while the byte received via I2C is available in the Receive Register.

I2C0_Status@ 0x14 I2C1_Status @ 0x24				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C_RxAckb*	**Received acknowledge from slave.** This flag represents acknowledge from the addressed slave. "1" No acknowledge received "0" Acknowledge received	1	R
6	*I2C_Busy*	This bit indicates the bus is involved in transaction. This will be set at start condition and cleared at stop.	0	R
5	*I2C_ArbLost*	This bit will go high if master has lost its arbitration. Arbitration is lost when : A stop signal is detected, but not requested. The master drives SDA high, but SDA is low This bit is cleared at the next start	0	R
4-2	*Reserved*	*Reserved*	0	R
1	*I2C_TIP*	This bit indicates that one byte of data is being transferred. This bit will be set at rising edge of acknowledge cycle. "0" Byte transfer completed. "1" Byte transfer in progress.	0	R
0	*Reserved*	*Reserved*	0	R

I2C0_Command @ 0x14 I2C1_ Command @ 0x24				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C_STA*	Generate (repeated) START condition and first Addressing cycle	N.A	W
6	*I2C_STO*	Generate stop condition (this bit must be activated alone)	N.A	W
5	*I2C_RD*	Read from slave	N.A	W
4	*I2C_WR*	Write to slave	N.A	W
3	*I2C_ACK*	When a receiver, sent ACK (ACK = '0') or NACK (ACK = '1')	N.A	W
2-1	*Reserved*	*Reserved*	N.A	W
0	*I2C_IACK*	Interrupt acknowledge. When set, clears a pending interrupt.	N.A	W

The **Status Register** and the **Command Register** share the same address.
The Status Register allows the monitoring of the I2C operations, while the Command Register stores the next command for the next I2C operation. Unlike the rest of the registers, the bits in the Command Register are cleared automatically after each operation. Therefore this register has to be written for each start, write, read, or stop of the I2C operation.

I2C0_Interrupt @ 0x15 **I2C1_ Interrupt @ 0x25** **Only on VX3035 Rev >= 4**				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C0_Int_Status*	Interrupt status for I2C0	0	RO
6	*I2C1_Int_Status*	Interrupt status for I2C1	0	RO
5	*I2C2_Int_Status*	Interrupt status for I2C2	0	RO
4				
3				
2				
1	*Int_Mask*	Interrupt mask 1 : interrupt is masked for this interface 0 : interrupt is not masked	1	RW
0	*Int_Status*	Interrupt status 1 : interrupt occurred on this interface : I2C_TIP bit transition to 0 0 : no interrupt Write 0 to clear the status	0	RW

NOTE: I2Cn_Int_Status bits have been added to know which interface has set the SERIRQ (common to all I2C interfaces) using a single read, without the need to read registers 0x15,0x25 and 0x35 to get the Int_Status bit. However the interrupt status still has to be cleared by writing 0 to interface specific Int_Status bit (can write 0 to all register without reading it before as Int_Mask should already be at 0).
NOTE : To know if this register is implemented, just read it. If default value is 0x02, it is implemented

17.2.10 Dual speed I2C bus

I2C2 bus is to access onboard I2C devices (local devices)

I2C2_PreScaleLow @ 0x30				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*I2C_PresScale_Low*	This register is used for programming the SCL low-speed frequency. The frequency will be 33 MHz clock divided by **4** and by this register value.	'h60	RO

I2C2_PreScaleHigh @ 0x31				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*I2C_PresScale_High*	This register is used for programming the SCL High-speed frequency. The frequency will be 33 MHz clock divided by **4** and by this register value.	'h0A	RO

When implemented for write access, these registers are used to prescale the SCL clock line, capable for two SCL speeds to quickly swap between them.

I2C2_Control @ 0x32				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C_Enable*	**I2C Interface enable bit** This bit must be set before any other control bit has any effect If this bit is set then all state machines will go into reset state. 1 I2C is enabled. 0 I2C is disabled.	0	RW
6	*Reserved*	Reserved	0	RW
5	*I2C_HighSpeed*	**I2C clock Selection for Low or High Speed** 1 High-Speed SCL defined by *I2C_PreScaleHigh* Register 0 Low-Speed SCL defined by *I2C_PreScaleLOWh* Register	0	RW
4	*Reserved*	Reserved	0	RW
3-0	*Reserved*	Reserved	0	RW

I2C2_Transmit @ 0x33				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-1	*I2C_Data[7:1]*	This represents the 7 MSB for a data transaction	N.A	W
0	*I2C_Data[0]*	This bit represents the data's LSB. This bit represents the RW bit during slave address transfer "1" Reading from slave "0" Writing to Slave	N.A	W

I2C2_Receive @ 0x33				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*I2C_Data[7:0]*	I2c Data byte	N.A	R

The **Transmit Register** and the **Receive Register** share the same address depending on the direction of data transfer. The data to be transmitted via I2C will be stored in the transmit Register, while the byte received via I2C is available in the Receive Register.

I2C2_Status @ 0x34				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C_RxAckb*	**Received acknowledge from slave.** This flag represents acknowledge from the addressed slave. 1 No acknowledge received 0 Acknowledge received	1	R
6	*I2C_Busy*	**NOT FOR VX3035 Rev >= 5 (not needed + saves cPLD space)** This bit indicates the bus is involved in transaction. This will be set at start condition and cleared at stop.	0	R
5	*I2C_ArbLost*	**NOT FOR VX3035 Rev >= 5 (not needed + saves cPLD space)** This bit will go high if master has lost its arbitration. Arbitration is lost when : A stop signal is detected, but not requested. The master drives SDA high, but SDA is low This bit is cleared at the next start	0	R
4-2	*Reserved*	*Reserved*	0	R
1	*I2C_TIP*	This bit indicates that one byte of data is being transferred. This bit will be set at rising edge of acknowledge cycle. “0” Byte transfer completed. “1” Byte transfer in progress.	0	R
0	*WR_FIFO_FULL*	**VX3035 Rev >= 5 ONLY** For I2C write bursts, this bit indicates when at level 1 that the transmit FIFO is full and then no more data can be written to the transmit register.	0	R

I2C2_Command @ 0x34				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C_STA*	Generate (repeated) START condition and first Addressing cycle	N.A	W
6	*I2C_STO*	Generate stop condition (this bit must be activated alone)	N.A	W
5	*I2C_RD*	Read from slave	N.A	W
4	*I2C_WR*	Write to slave	N.A	W
3	*I2C_ACK*	When a receiver, sent ACK (ACK = ‘0’) or NACK (ACK = ‘1’)	N.A	W
2-1	*Reserved*	Reserved	N.A	W
0	*Reserved*	Reserved	N.A	W

The Status Register and the Command Register share the same address.
The Status Register allows the monitoring of the I2C operations, while the Command Register stores the next command for the next I2C operation. Unlike the rest of the registers, the bits in the Command Register are cleared automatically after each operation. Therefore this register has to be written for each start, write, read, or stop of the I2C operation.

I2C2_Interrupt @ 0x35 **Only on VX3035 Rev >= 4**				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*I2C0_Int_Status*	Interrupt status for I2C0	0	RO
6	*I2C1_Int_Status*	Interrupt status for I2C1	0	RO
5	*I2C2_Int_Status*	Interrupt status for I2C2	0	RO
4				
3				
2				
1	*Int_Mask*	Interrupt mask 1 : interrupt is masked for this interface 0 : interrupt is not masked	1	RW
0	*Int_Status*	Interrupt status 1 : interrupt occurred on this interface : I2C_TIP bit transition to 0 0 : no interrupt Write 0 to clear the status	0	RW

NOTE: I2Cn_Int_Status bits have been added to know which interface has set the SERIRQ (common to all I2C interfaces) using a single read, without the need to read registers 0x15, 0x25 and 0x35 to get the Int_Status bit. However the interrupt status still has to be cleared by writing 0 to interface specific Int_Status bit (can write 0 to all register without reading it before as Int_Mask should already be at 0).

17.2.11 Serial Management interface (SMI)

Removed since not used

17.2.12 Timers

Reserved

17.2.13 Watchdog

WDG_Value @ 0x55				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*WDG_Value*	**Watchdog Timeout Value in watchdog clock periods** **Periods = WDG_Value * 2 + 1** 0x00 **DO NOT USE** (leads to immediate timeout or not timeout) 0x01 3 periods 0x02 5 periods … … 0xFD 507 periods 0xFE 509 periods 0xFF 511 periods **An additional uncertainty of –0 period / +1 period also applies to the timeout**:	0xFF	RW

WDG_Control @ 0x56				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*WDG_Timeout*	**Watchdog Timer expired status bit** Write '1' to clear from software. This bit is cleared on reset NOTE : this bit also drives a LED on front panel to report the timeout (the LED driven is board specific)	0	RW
6	*WDG_Clk_Period*	**Watchdog clock period** 0 Period is 1 Second (freq = 1Hz) 1 Period is 1.037598 mS (freq = 32.768kHz/34) **Only supported on VX3035 Rev >= 2** ; cleared on board reset **On other boards / versions** : not implemented, set to 0	0	RW
5-4	*Reserved*	Not used – always read as 0's, writes ignored		
3	*WDG_Lock*	**Watchdog Lock** 0 Watchdog timer not locked 1 Watchdog timer locked : When Locked WDG_Value and WDG_Control registers cannot be changed This bit can only be cleared when a reset occurs	0	RW
2-1	*WDG_Mode*	**Watchdog Mode** 00 Timer Only Mode 01 Reset Mode 10 Interrupt Mode 11 Power-cycle Mode (reserved) The default value at reset is 00	00	RW

WDG_Control @ 0x56				
0	*WDG_Enb*	**Watchdog Enable** 0 = Watchdog timer not enabled 1 = Watchdog timer enabled / Watchdog Trigger The default value is 0 at reset	0	RW

17.2.14 Alert

ALERT_Status @ 0x5B				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*CATERR*	**CPU CATERR pending** 0 No error 1 CPU CATERR error pending => Power off if bit 5 of register *PWR_RST_CONFIG@04* **is not set to 1** (3Ux_PLD_CATERR# signal)	N.A	RO
6	*THERMTRIP*	**CPU THERMTRIP pending** 0 No error 1 THERMTRIP error pending => Power off if bit 5 of register *PWR_RST_CONFIG@04* **is not set to 1** (3Ux_PLD_THRMTRIP# signal)	N.A	RO
5	*THERM_PROT*	**CPU THERM_PROT pending** 0 No error 1 THERM_PROT error pending => Power off if bit 5 of register *PWR_RST_CONFIG@04* **is not set to 1** (3Ux_PLD_THERM_PROT# signal)	N.A	RO
4	*PROCHOT*	**CPU PROCHOT pending** 0 No error 1 PROCHOT error pending (3Ux_PLD_PROCHOT# signal)	N.A	RO
3	*ALERT*	**Board alert** 0 No alert 1 Board alert is pending This alert comes from 3Ux_PLD_SMBTEMP_ALERT# signal **On VX3035**: also comes from PLD_PECI_ALERT_n. See reg 0xF bit 6 and 2 for interrupt mask and status	N.A	RO
2	*6U PCIe ERR*	**PCIe Error - 3UA CPLD only –** 0 No error 1 6U PCIe FATAL Error (3A6_PLD_SW_FATAL_ERR signal)	N.A	RO
1	*6U PCIe ERR*	**PCIe Error –** 0 No error 1 3U PCIe FATAL Error (3AB_PLD_SW_FATAL_ERR signal)	N.A	RO
0	*DDR throttling*	**Forces memory throttling to start** 0 Memory throttling 1 No memory throttling (3Ux_PM_EXTTS0# signal, must be open drain output!)	1	RW

17.2.15 GPIO

GPIO_Control @ 0x60 - R/W - Reset Value = 0x00		
Bit#	**Name**	**Description**
7-5	*GPIO_Control[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_Control[4]*	Control for **GPIO[4]** 1 : GPIO is configured as output 0 : GPIO is configured as input
…	…	**…**
n	*GPIO_Control[n]*	Control for GPIO[n] 1 : GPIO is configured as output 0 : GPIO is configured as input
…	…	**…**
0	*GPIO_Control[0]*	Control for GPIO[0] 1 : GPIO is configured as output 0 : GPIO is configured as input

The control register enables or disables the output and bi-directional modes of operation for each GPIO of the selected Channel (Size parameter depending of the channel)

GPIO_DataOut @ 0x61 - R/W - Reset Value = 0x00		
Bit#	**Name**	**Description**
7-5	*GPIO_DataOut[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_DataOut[4]*	Data to drive to GPIO[Size-1] of the selected Channel
…	…	**…**
n	*GPIO_ DataOut [n]*	Data to drive to GPIO[n] of the selected Channel
…	…	**…**
0	*GPIO_ DataOut [0]*	Data to drive to GPIO[0] of the selected Channel

This register specifies the Data driven by each GPIO of the selected Channel

GPIO_In @ 0x62 – Read Only - Reset Value = N.A		
Bit#	**Name**	**Description**
7-5	*GPIO_In[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_In[4]*	**Data from** GPIO[4]
…	…	**…**
n	*GPIO_In [n]*	**Data from** GPIO[n]
…	…	**…**
0	*GPIO_in [0]*	**Data from** GPIO[0]

Access to this register reads Data from the GPIOs of the selected Channel

GPIO_IntMask @ 0x63 R/W - Reset Value = FF		
Bit#	**Name**	**Description**
7-5	*GPIO_IntMaskl[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_IntMaskl[4]*	**Interrupt Mask** for GPIO[4] 1 : GPIO can not generate an interrupt 0 : GPIO can generate an interrupt
…	…	**…**
n	*GPIO_IntMaskl[n]*	**Interrupt Mask** for GPIO[n] 1 : GPIO can not generate an interrupt 0 : GPIO can generate an interrupt
…	…	**…**
0	*GPIO_IntMaskl[0]*	**Interrupt Mask** for GPIO[0] 1 : GPIO can not generate an interrupt 0 : GPIO can generate an interrupt

The interrupt mask register defines which GPIO **input** of the selected Channel can generate an interrupt to the PCIe interface.

GPIO_IntPolarity @ 0x64 - R/W - Reset Value = 0x00		
Bit#	**Name**	**Description**
7-5	*GPIO_IntPolarity[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_IntPolarity[4]*	**Interrupt Polarity** for GPIO[4] 1 : Level 1 or Rising edge on GPIO generates an interrupt 0 : Level 0 or Falling edge on GPIO generates an interrupt
…	…	**…**
n	*GPIO_IntPolarity[n]*	**Interrupt Polarity** for GPIO[n] 1 : Level 1 or Rising edge on GPIO generates an interrupt 0 : Level 0 or Falling edge on GPIO generates an interrupt
…	…	**…**
0	*GPIO_IntPolarity[0]*	**Interrupt Polarity** for GPIO[0] 1 : Level 1 or Rising edge on GPIO generates an interrupt 0 : Level 0 or Falling edge on GPIO generates an interrupt

The Interrupt Polarity Register defines the active level of a GPIO input which can generate an interrupt

GPIO_IntMode @ 0x65 - Reset Value = 0x00		
Bit#	**Name**	**Description**
7-5	*GPIO_IntMode[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_IntMode[4]*	**Interrupt Mode** for GPIO[4] 1 : Interrupt generation on GPIO is **Edge** Sensitive 0 : Interrupt generation on GPIO is **Level** Sensitive
…	…	**…**
n	*GPIO_IntMode[n]*	**Interrupt Mode** for GPIO[n] 1 : Interrupt generation on GPIO is **Edge** Sensitive 0 : Interrupt generation on GPIO is **Level** Sensitive
…	…	**…**
0	*GPIO_IntMode[0]*	**Interrupt Mode** for GPIO[0] 1 : Interrupt generation on GPIO is **Edge** Sensitive 0 : Interrupt generation on GPIO is **Level** Sensitive

The Interrupt Mode Register defines if interrupt is generated on edge or level as defined in GPIO_IntPolarity.

GPIO_IntToggle @ 0x66 - R/W - Reset Value = 0x00		
Bit#	**Name**	**Description**
7-5	*GPIO_IntToggle[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_IntToggle[4]*	**Interrupt ToggleMode** for GPIO[4] 1 : Interrupt is generated on GPIO Toggle 0 : No interrupt generated
…	…	…
n	*GPIO_ IntToggle [n]*	**Interrupt Toggle Mode** for GPIO[n] 1 : Interrupt is generated on GPIO Toggle 0 : No interrupt generated
…	…	…
0	*GPIO_ IntToggle [0]*	**Interrupt Toggle Mode**for GPIO[0] 1 : Interrupt is generated on GPIO Toggle 0 : No interrupt generated

When a GPIO is selected in Toggle Mode by this register GPIO_IntMode and GPIO_Int_polarity are not taken in consideration and interruption will be generated if GPIO changes of state and it is not masked

GPIO_IntStatus @ 0x67 - R/W - Reset Value = 0x00		
Bit#	**Name**	**Description**
7-5	*GPIO_IntStatus[7-5]*	These 3 GPIOs are **not available on VX3035**
4	*GPIO_IntStatus[4]*	**Interrupt Status** for GPIO[4] 1 : GPIO has generated an interrupt 0 : GPIO has not generated an interrupt
…	…	…
n	*GPIO_IntStatusl[n]*	**Interrupt Status** for GPIO[n 1 : GPIO has generated an interrupt 0 : GPIO has not generated an interrupt
…	…	…
0	*GPIO_IntStatusl[0]*	**Interrupt Status** for GPIO[0] 1 : GPIO has generated an interrupt 0 : GPIO has not generated an interrupt

For each channel the interrupt Status register defines which GPIO **has generated an Interrupt.**
Write 0 to Reset Status bits.

17.2.16 Geographical address

GEO_ADD @ 0x6A				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*SYSCON*	**VPX or VME System Controller** 0 System Controller 1 Not System Controller	N/A	RO
6	*Error*	**Parity Error** 0 Parity is valid 1 Parity is invalid	N/A	RO
5	*GAP*	Geographical Address Parity	N/A	RO
4-0	*GA*	Geographical Address	N/A	RO

NOTE:
- **On VX3035 Rev >= 4** : the GA/GAP and SYSCON signals are latched from backplane when standby power is applied and reported to register 0x6A.
- **On other versions** : they are latched at each LPC reset

GAGPIO @ 0x6B Only on VX3035 Rev >= 4				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*CUR_SYSCON*	Current value of SYSCON# signal from backplane	N/A	RO
6	*Cur_Error*	Current value of parity error	N/A	RO
5	*GAPGPIO*	**GPIO on GAP signal** - read : returns the current value on the signal - write 0 : forces the signal to low state - write 1 : signal not forced to low state (default) NOTE : If GAPGPIO is read at 0 and GAP (reg 0x6A bit 5) is read at 1, this means the signal has been forced low by a previous GAPGPIO write to 1 or by an external logic.	N/A	RW
4-0	*GAGPIO*	**GPIOs on GA[4:0] signals** These bits behave like GAPGPIO but for GA0 to GA4 signals	N/A	RW

NOTE : GA[4:0] and GAP signals must contain a valid Geographical ID data until latched in register 0x6A, so do not drive them with any external GPIO user logic before.

17.2.17 VPX/VME registers

VPX_Control @ 0x70				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*Gdiscrete_Ctl*	**GDISCRETE# Control** 0 : Drive 0 to VPX GDISCRETE# Signal 1 : Do not drive VPX GDISCRETE# Signal (open collector) default value is 1	*	RW
6	*Gdiscrete_Status*	**GDISCRETE1# Status** 0 : GDISCRETE# Signal is currently low 1 : GDISCRETE# Signal is currently high NOTE : GDISCRETE# signal is also called SMB_ALERT# in this document because it could be used to report an SMB alert. See reg 0x0F, SMB_ALERT# for interrupt on this signal	N.A	RO
5	*SW_FORCE_TRSP*	**PCIe Switch Force Transparent** 0 Not forced 1 Forced transparent mode See also bit 3 **VX3035 Rev >= 0x4 : supported** **Other boards or versions : NOT SUPPORTED**	0	RW
4	*MSKR2LOC P1G15/GPIO2*	**Propagation of VPX Maskable Reset to the local reset** 0 Reset not propagated 1 Reset propagated **The default value of this register is loaded with EEPROM value (Byte at offset @0x0103 – bit 2)** **If FACTORY_MODE is enable this register is not loaded from non-volatile memory and its value is 1**	1	RW
3	*SW_FORCE_NTRSP*	**PCIe Switch Force Non-Transparent** 0 Forced non-transparent mode 1 Not forced. Transparent port mode is set according to SYSCON# (if SYSCON# = 0 -> system controller -> transparent) Setting both bit 3 = 0 and bit 5 = 1 leads to a forced transparent mode	1	RW
2	*VPX_RST*	**VPX SYSRESET_OUT# Software activation** 0 Reset asserted (Side A only on VX6060) 1 Reset deasserted This bit is cleared by software and set automatically	1	RW

VPX_Control @ 0x70				
1	*VPX2LOC*	**Propagation of VPX reset** (SYSRESET_IN#) **to local reset** 1 Reset not propagated 0 Reset propagated (Side A only on VX6060)	0	RW
0	*LOC2VPX*	**Propagation of all local resets** to VPX (SYSRESET_OUT#) 1 Reset not propagated 0 Reset propagated	SYSCON#	RW

PCIe_Switch_VPX @ 0x71 This Register is initialized only on PWRG_P3V3SB low level				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*VPX_REFCLK*	**VPX 25Mhz REFCLK Generation** 1 Board generates VPX REF clock 0 Board receives VPX REF clock (This bit controls 3UA_PLD_VPX_CLK_DE signal)	0	RW
6	*VPX_AUXCLK*	**VPX 1s REFCLK Generation** 1 = Board generates VPX AUX clock 0 = Board receives VPX AUX clock (This bit controls 3UA_PLD_VPX_CLK_DE signal)	0	RW
5	*ENSW3U*	**PLD_ENSW_SPI_CS** 0 = Force access to 3U PCIE switch SPI flash 1 = 3U PCIE switch SPI flash by SYSCON#	1	RW
4	*FREQ*	**Maximum Link Speed (Gen1/Gen2)** 0 = 2.5GT/s 1 = 5GT/S (3Ux_PLD_SW_RESERVED17# signal)	USER2 = 0 : 1 USER2 = 1 : 0	RW
3	*ENSW6U*	**PLD_ENSW_SPI_CS** 0 Access to 6U PCIE switch SPI flash authorized 1 6U PCIE switch SPI flash inhibited	0	RW
21	*CFG[1:0]*	**Port Configuration** 00 = Reserved 01 = x4, x1, x1, x1, x1 10 = x4, x4 11 = Reserved (3Ux_PLD_SW_PORTCFG[1:0] signals)	USER1 = 0 : 01 USER1 = 1 : 10	RW
0-1	*CFC clock*	**VPX PCIe Clocking Operation** 0 CFC clock from Local CK505 1 CFC clock from backplane (3Ux_PLD_SW_SSC_ISO_ENABLE#, 3A6_PLD_BUFF_VPX_CLK_SEL and 3UA_PLD_P0_VPX_CLK_SEL signals)	0	RW

17.2.18 VPX/VME backplane I2C bus registers

I2C_BOARD_STATUS : This Register can be accessed from I2C0 Slave interface :
- I2C_SLAVE_ADDR = 7'b0010_111 + GA
- Register offset (1 byte) = 0

Bits meaning during read access is controlled by bit 3 of register @73.

I2C_BOARD_STATUS @ 0x72 – When bit 3 of Register @73 is set to 0 **This Register is initialized only on PWRG_P3V3SB low level**				
Bit#	**Name**	**Description**	**Reset**	**Type**
7	*Power Status*	**Power Status** 0 Power Stand By 1 Power ON	0	RO
6-5	*Reset Source*	**Last Reset Source** 0x00 Internal PSUs power-on 0x01 Watchdog expired 0x10 SYSRESET (from VPX or VME) 0x11 Local reset : GPIO2 (maskable reset), reset switch, reset from I2C (reg 0x73), or reset by software asserting PLD_PLTRST_n (see bugzilla 6505)	0	RO
4	*Reset Status*	**Reset Status Side A** 0 No PWOK or reset asserted 1 PWOK and reset unasserted	0	RO
3-0	*Boot Status*	**Boot Status** 0x00 : RESET : default hardware value 0x01 : BIOS-BOOT : written by BIOS 0x02 : BIOS : written by BIOS 0x03 : PBIT : written by BIOS 0x04 : OS-BOOT : written by BIOS 0x05 : OS-RUNNING : to be written by OS at the end of boot 0x06 : COMPLETED : to be written by the final application when running 0x07 : SHUTDOWN : to be written by OS when issuing a halt/shutdown 0x08 : REBOOT : to be written by OS when rebooting 0x09 - 0x0B : Reserved 0x0C - 0x0F : Customer defined These bits are Read Only through I2C Slave Interface and R/W through LPC Interface	0	RW

I2C_BOARD_STATUS @ 0x72 – when bit 3 register @73 is set to 1				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-0	*Power Debug 1*	**This register indicates State of Powers when a power error occurs (falling of one of the PWRGDG_XX signals).** Bit 7 : PWRGD_DDR Bit 6 : PWRGD_GFXCORE	0	RO

I2C_BOARD_STATUS @ 0x72 – when bit 3 register @73 is set to 1				
		Bit 5 : PWRGD_P1V0 Bit 4 : PWRGD_P1V0_6U Bit 3 : PWRGD_P1V05IBEX Bit 2 : PWRGD_P1V05S Bit 1 : PWRGD_P1V2_6U Bit 0 : PWRGD_P1V5_6U		

I2C_BOARD_CONTROL: This Register can be accessed from I2C0 Slave interface
- I2C_SLAVE_ADDR = 7'b0010_111 + GA
- Register offset (1 byte) = 1

I2C_BOARD_CONTROL @ 0x73 – when Bit 3 of this register is set to 0				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-4	*Board Id*	**Board Identification** 0011 VX3030 0101 VM6050 0110 VX6060 0111 VX3035 1000 VX3040 family	0	RO
3	*Check_Errors*	**Error Status Selection** 0 Default meaning for register @ 72 and register @73 1 Select Error Status for register @ 72 and register @73	0	RW
2	*Reset_3UB*	**Reset Side B – (Only for VX6060)** 0 No Reset 1 Reset Assert	0	RW
1	*Reset_3UA*	**Reset Side A** 0 No Reset 1 Reset Assert	0	RW
0	*Power_OnOff*	**Power On/Off Control** 0 = Power Off (StandBy) 1 = Power On **On VX3035 rev >=4** : this bit can always be used to set power on or off, and its default value is set according to POWER_MODE Dip Switch (SW2[2]); 1 if switch is off; 0 if on. **On other boards / versions** : this bit is only valid if reg 0x4 bit 7 is high and in this case its default value is 0. NOTE : can not power on/off the board if reg 0x4 bit 7 is low (power is always on)	N.A	RW

I2C_BOARD_CONTROL @ 0x73 - when Bit 3 of this register is set to 1 **This Register is initialized only on PWRG_P3V3SB low level**

I2C_BOARD_CONTROL @ 0x73 - when Bit 3 of this register is set to 1 **This Register is initialized only on PWRG_P3V3SB low level**				
Bit#	**Name**	**Description**	**Reset**	**Type**
7-4	*Error Status*	**Error Status** Bit 7 : Cross Power Error (always 0 for non VX6060 boards) Bit 6 : Power Error Bit 5 : Fatal Alert Bit 4 : Power Timeout	0	RO
3	*Check_Errors*	**Error Status Selection** 0 Select Board Identification for bits 7-4 of this register 1 Select Error Status for bits 7-4 of this register	0	RW
2-0	*Power Debug 2*	**This register indicates State of Powers when a power error occurs (falling of one of the PWRGDG_XX signals).** Bit 2 : PWRGD_P1V8S, Bit 1: PWRGD_P2V5 Bit 0 : PWRGD_P3V3_6U	0	RW

17.2.19 LEDs

Register Name		**LED Mode**		
Address (Offset)		**0x80**		
Bits	**Name**	**Description**	**Reset Value**	**Access**
7 – 4	*Res.*	Reserved	0000	R
3-0	*ULCON [3:0]*	User-Specific LED Configuration: 0000 Reserved 0001 Nominal Mode 0010 User Mode 0011 - 1111 reserved	0001	RW

In nominal mode, all LEDs have a specific meaning that is board dependant.
In user mode, some LEDs are controlled by software

Register Name		**User-Specific LED Control**		
Address		**0x81**		
Bits	**Name**	**Description**	**Reset Value**	**Access**
7-4	*ULCMD [3:0]*	User-Specific LED command : 0000 get LED 1 0001 get LED 2 0010 get LED 3 1000 set LED 1 (Not supported) 1001 set LED 2 1010 set LED 3 Other : Reserved	0000	RW
3-0	*ULCOL [3:0]*	User-Specific LED color: 0000 off 0001 green 0010 red 0011 amber *1000 reserved* 0101 green slow blinking 0110 red slow blinking 0111 amber slow blinking *1000 reserved* 1001 green fast blinking 1010 red fast blinking 1011 amber fast blinking	0000	RW

The User-Specific LED control register enables the user to control some front panel LEDs (user mode). Only LED 1 does not support user mode
Once set to user mode (reg 0x80), a single write to this register sets both ULCMD (LED number +get/set operation) and ULCOL (color and blinking attributes). With this approach a complex lock mechanism implemented in software can be avoided in case of different LEDs dedicated to different tasks; but only one LED can be set by a single write.
In normal or user mode, the current LED state can be read back. For this, write ULCMD for a get command using any value for ULCOL (don't care), then do a subsequent read to get ULCOL.
In user mode, ULCOL returns the color + blinking configuration.
In normal mode, ULCOL only returns the current color (no blinking info); several read must be done to check if blinking or not.

End of the document