# Certificate of Volatility

| | | | |
|---|---|---|---|
| **Nomenclature : DSP BOARD** | | **Model/Part Number :** [redacted] | **Manufacturer :** [redacted] |
| | | | **Street Address:** [redacted] |
| **Date: 3/4/2015** | | | **City :** [redacted] **State:** [redacted] **Zip:** [redacted] |

**Volatile memory**

**Does the item contain volatile memory (i.e. memory whose contents are lost when power is removed)? Yes**

**If the answer is "Yes", please provide the following information for each type (Use additional sheets if required):**

| Type (SRAM, DRAM, etc.) | Size | User Modifiable | User/System Data Access | Function. | Write Protection | Process to clear |
|---|---|---|---|---|---|---|
| SDRAM | 8Gbytes /CPU | Yes | Yes | Main SDRAM for the processors. | None | Remove Power |
| SRAM | 2,888Mbits | Yes | Yes | SRAM within CF FPGA | None | Remove Power |
| SDRAM | 16MBytes | Yes | Yes | SDRAM attached to CF FPGA | None | Remove Power |
| SRAM | 64KBytes | No | No | SRAM within IPMC FPGA | None | Remove Power |
| SRAM | 256KBytes | No | No | SRAM attached to IPMC FPGA | None | Remove Power |
| SRAM | Unknown, invisible to user | No | No | TPM internal SRAM | None | Remove Power |

**Non-Volatile memory**

**Does the item contain non-volatile memory (i.e. memory whose contents are retained when power is removed)? Yes**

**If the answer is "Yes", please provide the following information for each type (Use additional sheets is required):**

| Type (SRAM, DRAM, etc.) | Size | User Modifiable | User/System Data Access | Function. | Write Protection | Process to clear |
|---|---|---|---|---|---|---|
| NVRAM | 256KBytes | Yes. | Yes | For user application use. | The memory is protected if jumper (or wire-wrap) JB9 is installed. It is also protected if the chassis-level NVMRO signal is high. | See procedure at the end of this document |

| | | | | | | |
|---|---|---|---|---|---|---|
| PABS NOR Flash | 16Mbytes /CPU | No | Yes | Backup copy of the Main NOR Flash. | The memory is protected if jumper (or wire-wrap) JB7 is NOT installed. User modifications are limited to predetermined manufacturer BIOS option settings. No publicly available or vendor provided mechanism is provided to write to this memory when JB7 is not installed. | None |
| Main NOR Flash | 16Mbytes /CPU | Yes. | Yes | Contains 1st level boot loading code and BIOS code. | The memory is protected if jumper (or wire-wrap) JB10 is installed. User modifications are limited to predetermined manufacturer BIOS option settings. No publicly available or vendor provided mechanism is provided to write to this memory when JB10 is installed. | See procedure at the end of this document |
| NAND Flash | 16Gbytes /CPU | Yes. | Yes | Solid State Disc (SSD) used to store OS and application code | This memory is protected if jumper (or wire wrap) JB3 is installed, or if the chassis-level NVMRO signal is high. | See procedure at the end of this document |

| | | | | | | |
|---|---|---|---|---|---|---|
| CPLD internal flash | 8Kbits | No | No | Programmable logic device. This is programmed during manufacture. It is only accessible via special purpose hardware. Note that once the CPLD is cleared, the board will not power up. | None | None |
| TPM | Stated to be 2066 bytes, but not observable | Via TCG TPM commands only | Via TCG TPM commands only | Trusted Platform Module, conforming to Trusted Computing Group (TCG) TPM version 1.2. Contains endorsement key pairs and TPM data structures. | Can only be written using the commands described in the TCG TPM document. | Can only be cleared using the commands described in the TCG TPM document. |
| Power supply regulator internal non-volatile memories | 103kbits total (approx.) | No | No | Contains settings for power supply regulators. This can only be written with external special purpose hardware. Note that once the power supply non-volatile memories are cleared, the board could be damaged if powered up. | None | None |
| CF FPGA Flash | 64MBytes | No | No | Contains the bit-stream for the CF FPGA | These memories are protected if jumper (or wire-wrap) JB8 is un-installed. | None |
| SPI flash - 4 devices | 2Mbytes per device | No | Yes | Stores firmware and data (MAC address) for the four Ethernet interfaces. | | None |

| | | | | | | |
|---|---|---|---|---|---|---|
| $I^2C$ EEPROM 4 devices | 1Kbits per device | No | Yes | Contains DDR3 configuration settings | These memories are protected if jumper (or wire-wrap) JB8 is un-installed, or if the chassis-level NVMRO signal is high. | None |
| SPI EEPROM | 32KBytes | No | Yes | Configuration settings for PCIe switch | | See procedure at the end of this document |
| $I^2C$ EEPROM 2 devices | 1Kbits per device | No | Yes | Contains vital product data, serial number, product ID, revision level | | |
| SPI flash - 2 devices | 4Mbytes per device | No | Yes | Stores firmware and data (MAC address) for the two Data plane interfaces. | None. This memory can only be written with the utility software provided by the Data plane interface manufacturer . This utility software is limited to installing firmware updates. | None |
| IPMC FPGA on-chip flash | 256KBytes | No | No | Stores FPGA bitstream and processor firmware for the IPMC FPGA. This can only be written with external special purpose hardware. | None | None |
| IPMC EEPROM | 16KBytes | No | No | Stores housekeeping data for the IPMC FPGA. This can only be written with external special purpose hardware. | None | None |

| Media | | | | | | |
|---|---|---|---|---|---|---|
| **Does the item contain media storage (i.e. Disk drives, memory cards, etc.)? No** | | | | | | |
| **If the answer is "Yes", please provide the following information for each type (Use additional sheets is required):** | | | | | | |
| **Type (Disk, Tape, etc.)** | **Size** | **User Modifiable** | **User/System Data Access** | **Function.** | **Write Protection** | **Process to clear** |
| - | N/A | N/A | N/A | N/A | N/A | N/A |
| | | | | | | |

| Wireless Capabilities | | | | | | |
|---|---|---|---|---|---|---|
| **Does the item have wireless capabilities installed (i.e. Bluetooth, Infrared, etc.)? No** | | | | | | |
| **If the answer is "Yes", please provide the following information for each type (Use additional sheets is required):** | | | | | | |
| **Type (Wireless)** | **Process to Deactivate** | | | | | |
| | | | | | | |
| | | | | | | |

| Procedure to clear non-volatile memory | |
|---|---|
| 1. | Power off the chassis. |
| 2. | Disconnect all portable USB Flash drives and hard drives from the CHAMP-AV9. |
| 3. | Insert a jumper on JB8 to write enable PROMs, and if there are jumpers on JB3 and JB10, remove them, to write enable the MAIN BIOS Flash and the NAND Flash (On-Board SSD). Alternatively, if you have an RTM (Rear Transition Module), the jumpers can be applied via switches on the RTM. |
| 4. | Ensure that the chassis NVMRO signal is low. The method of ensuring this is specific to the chassis; refer to the chassis documentation. Alternatively, if you have an RTM, turn switch SW13 on to drive the NVMRO signal low for the chassis. |
| 5. | Insert the [redacted] in the chassis. If you are using an RTM, install it in the same slot. |
| 6. | Apply power to the chassis. |
| 7. | For both processor nodes, perform the following steps:<br>a. Press the Esc key to enter the setup utility. |

| | |
|---|---|
| | b. In the setup utility, choose Internal EFI Shell then press Enter.<br><br>c. At the `Shell>` prompt, enter the following:<br>`nvmem -s`<br><br>d. This will begin the Scrub process. |
| 8. | The Scrub process can take over an hour. It will clear the Main BIOS flash, the PCIe switch SPI EEPROM, the NVRAM, and the NAND flash SSD. Once the Scrub is complete, the board will reset.<br><br>Please note that the [redacted] will not be capable of booting from Main flash after this procedure. To boot from PABS flash, install JB11. |