DELL Technologies

Statement of Volatility – Dell EMC PowerEdge R750XA

Dell EMC PowerEdge R750XA contains both volatile and non-volatile (NV) components. Volatile components lose their data immediately upon removal of power from the component. Non-volatile components continue to retain their data even after the power has been removed from the component. Components chosen as user-definable configuration options (those not soldered to the motherboard) are not included in the Statement of Volatility. Configuration option information (pertinent to options such as microprocessors, remote access controllers, and storage controllers) is available by component separately. The following NV components are present in the PowerEdge R750XA server.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
Planer				
PCH Internal CMOS RAM	Non-Volatile	1	U_PCH1	256 Bytes
BIOS SPI Flash	Non-Volatile	1	U34	32 MB
BIOS Data SPI Flash	Non-Volatile	1	U33	4 MB
iDRAC SPI Flash	Non-Volatile	1	U94	4 MB
BMC EMMC	Non-Volatile	1	U15	8 GB
iDRAC DDR4	Volatile	1	U5	8Gb
System CPLD RAM	Volatile	1	U_CPLD1	432 Kb
System CPLD RAM	Non-Volatile	1	U_CPLD1	448 Kb
System Memory	Volatile	Up to 16 per CPU	CPU1: A1~16, CPU2: B1~B16	Up to 256GB per DIMM
System Memory-BPS	Non-Volatile	Up to 8 per CPU	CPU1: A14/A10/A16/A12/A11/A15/A9/A13 CPU2: B14/B10/B16/B12/B11/B15/B9/B13	Up to 512GB per DIMM
CPU Vcore and VSA Regulators	Non-Volatile	1 for CPU1, 1 for CPU2	U523 U532	16KB
Memory VDDQ Regulators	Non-Volatile	1 for CPU1, 1 for CPU2	U541 U548	16KB
8 x 2.5" Universal SAS/SATA/NVMe front Backplane				
SEP internal flash	Non-Volatile	1	U14	4Mbit in-chip SPI Serial Flash
Backplane External FRU	Non-Volatile	1	U14	256 Bytes
H745 fPERC (Internal Controller)				
SDRAM	Volatile	4	U1077~U1080	4GB
NV Flash	Non-volatile	1	U1100	32Gb
BMU	Non-Volatile	1	U1090	180KB

SPI Flash	Non-Volatile	1	U1086	128Mb
NVSRAM	Non-volatile	1	U1087	128KB
FRU	Non-volatile	1	U1019	2Kb
SPD	Non-volatile	1	U22	2Kb
CPLD	Non-volatile	1	U1088	64kb
MCU (Cordova)	Non-volatile	1	U1113	8KB
H755/H755N fPERC (Internal Controller)				
SDRAM	Volatile	9	U1077~U1085	8GB
NV Flash	Non-volatile	1	U1100	512Gb
BMU	Non-Volatile	1	U1126	180KB
SPI Flash	Non-Volatile	1	U1086	128Mb
NVSRAM	Non-volatile	1	U1087	128KB
FRU	Non-volatile	1	U1019	2Kb
SPD	Non-volatile	1	U22	2Kb
CPLD	Non-volatile	1	U1088	64kb
MCU (Cordova)	Non-volatile	1	U41	8KB
H345 fPERC (Internal Controller)				
SPI Flash	Non-Volatile	1	U2	256Mb
NVSRAM	Non-volatile	1	U5	128KB
CPLD	Non-volatile	1	U7	24Kb
FRU	Non-volatile	1	U8	64Kb
RMC	Non-volatile	1	U9	64Kb
MCU (Cordova)	Non-volatile	1	U41	8KB
H355 fPERC (Internal controller)				
SPI Flash	Non-Volatile	1	U2	128Mb
FRU	Non-volatile	1	U5	2Kb
CPLD	Non-volatile	1	U23	24kb
MCU	Non-volatile	1	U41	8KB
NVSRAM	Non-volatile	1	U3	128KB
HBA355i fPERC (Internal controller)				

SPI Flash	Non-Volatile	1	U2	128Mb
FRU	Non-volatile	1	U5	2Kb
CPLD	Non-volatile	1	U23	24kb
MCU	Non-volatile	1	U41	8KB
HBA355E Adapter PERC (External controller)				
SPI Flash	Non-Volatile	1	U2	128Mb
FRU	Non-volatile	1	U5	2Kb
CPLD	Non-volatile	1	U23	24kb
H840 Adapter PERC (External controller)				
SDRAM	Volatile	9	U1077~U1085	8GB
NV Flash	Non-volatile	1	U1100	64Gb
BMU	Non-Volatile	1	U1090	180KB
SPI Flash	Non-volatile	1	U1098	128Mb
NVSRAM	Non-volatile	1	U1087	128KB
FRU	Non-volatile	1	U1019	2Kb
SPD	Non-volatile	1	U22	2Kb
CPLD	Non-volatile	1	U1088	64kb
Left Status CP				
Microcontroller	Non-Volatile	1	U_TINY	8KB
Left Titan2				
Microcontroller	Non-Volatile	1	USAM7	2MB Flash in chip
TPM				
Trusted Platform Module (TPM)	Non-Volatile	1	U2	128 Bytes
Right FIO 2U Package 1				
SPI Flash	Non-Volatile	1	U2	32 Mb
IDSDM				
iDSDM (uSD1, uSD2)	Non-Volatile	2	J1, J2	16GB, 32GB, 64GB
SPI Flash	Non-Volatile	1	U2	8Mb
BOSS				
RAID controller external SPI FLASH	Non-Volatile	1	U17	8Mb
CPLD	Non-Volatile	1	U1120	256Kb

MCU (Cordova)	Non-volatile	1	U1113	8KB
FRU	Non-Volatile	1	U_BOSS_EEPROM	2Kb
LCD Bezel				
Microcontroller	Non-Volatile	1	IC1	256KB
PSU				
DELTA PSU				
MCU	Non-volatile	2	IC805, IC703	64KB
EEPROM	Non-volatile	1	IC601	2KB
ARTESYN PSU				
Primary MCU	Non-volatile	1	U317	64KB
Secondary MCU	Non-volatile	1	U315	128KB
DCDC MCU	Non-volatile	1	U301	32KB
Liteon PSU				
Primary MCU	Non-volatile	1	IC050	64K
Secondary MCU	Non-volatile	1	IC900	128K
LOM				
SPI FLASH	Non-volatile	1	U_LOM	8MB
R1-paddle				
MCU	Non-volatile	1	U1	8kB
R2A				
MCU	Non-volatile	1	U1	8kB
R3B/R3 Paddle				
MCU	Non-volatile	1	U1	8kB
R4 Paddle				
MCU	Non-volatile	1	U1	8kB
STD/LC RIO				
MCU	Non-volatile	1/1	U6	8kB

Item	**Type (e.g. Flash PROM, EEPROM)**	**Can user programs or operating system write data to it during normal operation?**	**Purpose? (e.g. boot code)**
Planer			
PCH Internal CMOS RAM	Battery-backed CMOS RAM	No	Real-time clock and BIOS configuration settings
BIOS SPI Flash	SPI Flash	Yes	Boot code, system configuration information, UEFI

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
			environment, Flash Disceptor, ME
BIOS Data ROM SPI Flash	SPI Flash	No	4MB Data SPI ROM storage BIOS setting.
iDRAC SPI Flash	SPI Flash	No	iDRAC Uboot (boot loader), server management persistent store (i.e. iDRAC boot variables), and virtual planar FRU
BMC EMMC	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware, IDRAC MAC Address, and EPPID, rac log, System Event Log, lifecycle log cache
iDRAC DDR4	RAM	Yes	iDRAC RAM
System CPLD RAM	RAM	No	Not utilized
System Memory	RAM	Yes	System OS RAM
System Memory-BPS	BPS	Yes	System OS RAM App direct
Memory VDDQ, CPU Vcore and VSA Regulators	OTP(one time programmable)	No	Operational parameters
8 x 2.5" Universal SAS/SATA/NVMe front Backplane			
SEP internal flash	Integrated Flash+EEPROM	No	Firmware + FRU
Backplane External FRU	I2C EEPROM	No	FRU
H345/H355/H745/H755/H755N fPERC (Internal controller)			
NVSRAM	NVSRAM	No	Configuration data
FRU	EEPROM	No	Card manufacturing information
SPD	EEPROM	No	Memory configuration data
NV Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
SPI Flash	SPI Flash	No	Holds cache data during power loss
SDRAM	SDRAM	No	Cache for HDD I/O
MCU (Cordova)	EEPROM	No	PCIe Bifurcation information to system iDRAC
BMU	Integrated Flash+EEPROM	No	Battery Management control
H840 Adapter PERC (External controller)			

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
NVSRAM	NVSRAM	No	Configuration data
FRU	EEPROM	No	Card manufacturing information
SPD	EEPROM	No	Memory configuration data
NV Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
SPI Flash	SPI Flash	No	Holds cache data during power loss
SDRAM	SDRAM	No	Cache for HDD I/O
HBA355i fPERC (Internal controller)			
FRU	EEPROM	No	Card manufacturing information
SPI Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
MCU (Cordova)	EEPROM	No	PCIe Bifurcation information to system iDRAC
HBA355E Adapter PERC (External controller)			
FRU	EEPROM	No	Card manufacturing information
SPI Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
Left Status CP			
Microcontroller	Flash	No	Driving Health and Status LED
Left Titan2			
Microcontroller	SPI Flash	No	For field maintenance. Have License, Service Tag and system information. Driving health and status LEDs
TPM			
Trusted Platform Module (TPM)	EEPROM	Yes	Storage of encryption keys
Right FIO 1U Package 1			
SPI Flash	SPI Flash	No	EasyRestore functionality contains Service Tag, Copy of SEL logs
IDSDM			
iDSDM (uSD1, uSD2)	NAND Flash	Yes	Provides mass storage
SPI Flash	SPI Flash	SPI flash is only indirectly connected to iDRAC. iDRAC can read any address in the SPI flash, but may only	Boot firmware storage, configuration and state data for IDSDM.

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
		write the primary firmware storage area as a part of a firmware update procedure.	
BOSS			
SPI FLASH	FLASH EEPROM	No	Boot code, FW
FRU	FLASH EEPROM	No	Card manufacturing information
LCD Bezel			
Microcontroller	Internal Flash	No	bootloader and s/w implementation of LCD command set
PSU			
MCU	Internal Flash	Yes	Boot code, FW
FRU	EEPROM	No	PSU information
LOM			
SPI FLASH	SPI Flash EEPROM	Yes	Firmware
R1-paddle/R2A/R3B/R3-paddle/R4-paddle			
MCU	Flash ROM	No	Riser information
STD/LC RIO			
MCU	Flash ROM	No	Rear IO information

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
Planer			
PCH Internal CMOS RAM	BIOS	N/A – BIOS only control	1) Set NVRAM_CLR jumper to clear BIOS configuration settings at boot and reboot system. 2) Power off the system, remove coin cell battery for 30 seconds, replace battery and then power back on. 3) Restore default configuration in F2 system setup menu.
BIOS SPI Flash	SPI interface via PCH	Software write protected	Not possible with any utilities or applications and system is not functional if corrupted or removed.

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
BIOS Data SPI Flash	SPI interface via PCH	Software write protected	Not possible with any utilities or applications and the system is not functional if BIOS SPI is corrupted or removed.
iDRAC SPI Flash	SPI interface via iDRAC	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.	The user cannot clear memory completely. However, user data, lifecycle log and archive, SEL, and fw image repository can be cleared using Delete Configuration and Retire System, which can be accessed through the Lifecycle Controller interface.
BMC EMMC	NAND Flash interface via iDRAC	Embedded FW write protected	The user cannot clear memory completely. However, user data, lifecycle log and archive, SEL, and fw image repository can be cleared using Delete Configuration and Retire System, which can be accessed through the Lifecycle Controller interface.
Memory VDDQ, CPU Vcore and VSA Regulators	Once values are loaded into register space a cmd writes to nvm.	There are passwords for different sections of the register space	The user cannot clear memory.
System CPLD RAM	Not utilized	Not accessible	Not accessible
System Memory	System OS	OS Control	Reboot or power down system
System Memory-BPS	System OS	OS Control	OS Control/System BIOS
System Memory-NVDIMM	System OS	OS Control	OS Control/System BIOS
Internal USB Key	USB interface via PCH. Accessed via system OS	No write protected	Can be cleared in the system OS
Trusted Platform Module (TPM, TPM 2.0 only)	Using TPM Enabled operating systems	SW write protected	F2 Setup option
8 x 2.5" Universal SAS/SATA/NVMe Backplane			
SEP internal flash	I2C interface via iDRAC	Program write protect bit	The user cannot clear memory.
Backplane External FRU	Programmed at ICT during production.	No write protected	The user cannot clear memory.
H345/H355/H745/H755/H755N fPERC (Internal Controller) and H840 Adapter PERC (External Controller)			
NVSRAM	ROC writes configuration data to NVSRAM	no write protected. Not visible to Host Processor	User cannot clear the memory.

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
FRU	Programmed at ICT during production.	no write protected	User cannot clear the memory.
SPD	Pre-programmed before assembly	no write protected. Not visible to Host Processor	User cannot clear the memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	no write protected. Not visible to Host Processor	User cannot clear the memory.
Backup Flash	FPGA backs up DDR data to this device in case of a power failure	no write protected. Not visible to Host Processor	Flash can be cleared by powering up the card and allowing the controller to flush the contents to VDs. If the VDs are no longer available, cache can be cleared by going into controller BIOS and selecting Discard Preserved Cache.
SDRAM	ROC writes to this memory - using it as cache for data IO to HDDs	no write protected. Not visible to Host Processor	Cache can be cleared by powering off the card
HBA355i fPERC (Internal Controller) and HBA355E Adapter PERC (External Controller)			
NVSRAM	ROC writes configuration data to NVSRAM	no write protected. Not visible to Host Processor	User cannot clear the memory.
FRU	Programmed at ICT during production.	no write protected	User cannot clear the memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	no write protected. Not visible to Host Processor	User cannot clear the memory.
Left Status CP			
Microcontroller	I2C via iDRAC	Hardware strapping	User cannot clear the memory.
Left Titan2			
Microcontroller	SPI interface via iDRAC	Hardware strapping	User cannot clear the memory.
TPM			
Trusted Platform Module (TPM)	Using TPM Enabled operating systems	SW write protected	F2 Setup option
Right FIO 1U Package 1			
SPI Flash	SPI interface from iDRAC to Right Cntl Panel	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.	The user cannot clear memory.
IDSDM			

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
iDSDM (uSD1, uSD2)	device resides in host domain; they are exposed to the user via an internally connected, non-removable USB mass storage device	physical write protect switch on ACE card	(1) card may be physically removed and destroyed or cleared via standard means on a separate computer OR (2)User has access to the card in the host domain and may clear it manually
SPI Flash	User can initiate a firmware update of the IDSDM device.	There is no mechanism provided to iDRAC to write any SPI NOR area outside of the primary IDSDM firmware region.	iDRAC may issue a clear command to erase all contents of the SPI NOR, but doing this will leave the IDSDM non-functional.
BOSS			
SPI FLASH	By programming the image via firmware update process	N/A	Use Flash tool, type “go.nsh w y”
TFRU	During Manufacturing, by programming the image via firmware update process. During runtime, by I2C Proprietary Command Protocol	N/A	By writing to Flash
LCD Bezel			
Microcontroller	Updated as part of secure iDRAC software update. Configuration parameters can change only as part of iDRAC update	Writes are only allowed as part of secure iDRAC update	not user clearable.
PSU			
MCU	The data is flash via Dell Update Package(DUP)	SW write protected	Before firmware update, the memory will be clear.
FRU	During Manufacturing, by programming the image via firmware update process	SW write protected	User cannot clear the memory.
LOM			
SPI FLASH	The data is flash via Dell Update Package(DUP)	Reserving write protection function for HW design.	User cannot clear the memory.
R1-paddle/R2A/R3B/R3-paddle/R4-paddle			
MCU	The data is flash via iDRAC auto update	No write protected. Not visible to Host Processor	User cannot clear the memory.
STD/LC RIO			
MCU	The data is flash via iDRAC auto update	No write protected. Not visible to Host Processor	User cannot clear the memory.

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?

NOTE: For any information that you may need, direct your questions to your Dell Marketing contact.

_____

12 - 2021