AA-64 architecture system management mode

SMM state save map				
offset	contents		size	notes
FE00h	ES	sel	word	
FE02h		ar	word	
FE04h		lim	dword	
FE08h		bas	qword	
FE10h	CS	sel	word	
FE12h		ar	word	
FE14h		lim	dword	
FE18h		bas	qword	
FE20h	SS	sel	word	
FE22h		ar	word	
FE24h		lim	dword	
FE28h		bas	qword	
FE30h	DS	sel	word	
FE32h		ar	word	
FE34h		lim	dword	
FE38h		bas	qword	
FE40h	FS	sel	word	
FE42h		ar	word	
FE44h		lim	dword	
FE48h		bas	qword	
FE50h	GS	sel	word	
FE52h		ar	word	
FE54h		lim	dword	
FE58h		bas	qword	
FE60h		sel	word	reserved
FE62h		ar	word	

FE64h	GDTR	lim	dword	upper 16 bits are reserved
FE68h		bas	qword	
FE70h	LDTR	sel	word	
FE72h		ar	word	
FE74h		lim	dword	
FE78h		bas	qword	
FE80h	IDTR	sel	word	reserved
FE82h		ar	word	
FE84h		lim	dword	upper 16 bits are reserved
FE88h		bas	qword	
FE90h	TR	sel	word	
FE92h		ar	word	
FE94h		lim	dword	
FE98h		bas	qword	
FEA0h	IO_RESTART_RIP		qword	
FEA8h	IO_RESTART_RCX		qword	
FEB0h	IO_RESTART_RSI		qword	
FEB8h	IO_RESTART_RDI		qword	
FEC0h	IO_RESTART_INFO		dword	
FEC4..FEC7h	reserved		4 bytes	
FEC8h	IO_RESTART		byte	00h=no, 01h=yes
FEC9h	HLT_RESTART		byte	00h=no, FFh=yes
FECAh	BLOCK_NMI		byte	00h=no, 01h=yes
FECBh	reserved		byte	
FECCh	reserved		byte	
FECDh	reserved		byte	
FECEh	reserved		byte	
FECFh	reserved		byte	
FED0h	EFER		qword	
FED8h	reserved		qword	PDPTR0?
FEE0h	reserved		qword	PDPTR1?
FEE8h	reserved		qword	PDPTR2?
FEF0h	reserved		qword	PDPTR3?
FEF8..FEFBh	reserved		4 bytes	TEMP_DR6?
FEFCh	REVISION		dword	0003_xx64h, is at same offset as in IA-32 SSM
FF00h	SMBASE		dword	
FF04..FF47h	reserved		68 bytes	

FF48h	CR4	qword
FF50h	CR3	qword
FF58h	CR0	qword
FF60h	DR7	qword
FF68h	DR6	qword
FF70h	RFLAGS	qword
FF78h	RIP	qword
FF80h	R15	qword
FF88h	R14	qword
FF90h	R13	qword
FF98h	R12	qword
FFA0h	R11	qword
FFA8h	R10	qword
FFB0h	R9	qword
FFB8h	R8	qword
FFC0h	RDI or R7	qword
FFC8h	RSI or R6	qword
FFD0h	RBP or R5	qword
FFD8h	RSP or R4	qword
FFE0h	RBX or R3	qword
FFE8h	RDX or R2	qword
FFF0h	RCX or R1	qword
FFF8h	RAX or R0	qword

processor state after SMM entry

register	contents			
	selector	base	limit	access rights
CS	SMBASE SHR 4	SMBASE	(FFF) F_FFFFh	8093h #1
SS	0000h	0000_0000h	(FFF) F_FFFFh	8093h
DS	0000h	0000_0000h	(FFF) F_FFFFh	8093h
ES	0000h	0000_0000h	(FFF) F_FFFFh	8093h
FS	0000h	0000_0000_0000_0000h	(FFF) F_FFFFh	8093h

GS	0000h	0000_0000_0000_0000h	(FFF) F_FFFFh	8093h
RFLAGS	0000_0000_0000_0002h			
RIP	0000_0000_0000_8000h			
CR0	bits 0 (PE), 2 (EM), 3 (TS), and 31 (PG) cleared, rest unmodified			
CR4	0000_0000_0000_0000h			
DR7	0000_0000_0000_0400h			
EFER	0000_0000h			
TEMP_DR6	0000_0000_0000_0000h			
IN_REP	false			
IN_SMM	true			
IN_HLT	false			
IN_SHUTDOWN	false			
IN_FP_FREEZE	false			
SUPPRESS_INTERRUPTS	false (both bits)			
BLOCK_INIT	true			
BLOCK_SMI	true			
BLOCK_NMI	true			
LATCH_INIT	true if INIT recognized together with SMI, else false			
LATCH_SMI	false			
LATCH_NMI	true if NMI recognized together with SMI, else false			
FERR#	unmodified			
A20M#	processor-specific			
notes	description			
#1	Like the data segments, CS is writeable too.