Definition of the TXT.ERRORCODE register for 4th_gen_i5_i7-SINIT AC Module

The tables below describe the format of the TXT.ERRORCODE register and the associated error code values generated by the 4th Generation Intel® Core™ i7 and i5 Processor Series Client TXT SINIT AC Module.

Table 1. TXT.CRASH register format for ACM initiated TXT-shutdown

Bit	Name	Description
31	Valid	Valid error when set to 1. The rest of the register contents should be ignored if '0'.
30	External	0 = induced from processor 1 = induced by external software
29:25	Reserved	Reserved
24:16	Minor Error Code	Field value depends on Class Code and / or Major Error Code. Several examples are: If Class Code = "TPM Access" and Major Error Code = "TPM retuned an error": Field value = TPM returned error code If error code is fatal, it occupies bits [23:16] and bit 24 remains clean. For non-fatal error codes lower byte is placed into bits [23:16] and bit 24 is asserted. For instance error code 0x803 will be translated into 0x103 If Class Code = "Launch Control Policy and Major Error Code = "Policy Integrity Fail": Field value = (LIST_INDEX << 6) + Specific Minor Error Code If Class Code = "Range Check Error": Field value = Index of first range in conflict with another range
15	SW source	0 = if error generated by AC module (below field definitions apply) 1 = if error generated by other software (field definitions will be software-specific)
14:10	Major Error Code	0 – 0x1F = Error code within current class code
9:4	Class Code	0 – 0x3F = Class code clusters several congeneric errors into a group.
3:0	Module Type	0000 = BIOS ACM 0001 = SINIT ACM 0010-1111 = Reserved for future use

Table 2. 4th_gen_i5_i7-SINIT ACM Error Codes

Class Code	Major Error Code	Minor Error Code	Description
0			Class ACM Progress
	0	0 … N	Progress value
1			Class ACM Entry
	1	0	Error in ACM launching: BIOS AC is launched not via ENTERACCS; BIOS AC: Reserved bits are not 0 in EDI register; SINIT is launched not via SENTER; SINIT: EDX register is not 0;
	2	0	No Eviction Mode (NEM) is enabled
	3	0	Processor-based S-CRTM is supported – detected in Client SINIT or Processor-based S-CRTM is NOT supported – detected in Server SINIT
	4	0	Not supported Device ID
	5	0	Not supported CPU ID
	6	0	MCU (micro-code update) is not loaded
	7	0	Debug MCU is not allowed
	8	0	DMI link is down
	9	0	ACM Revoked
	0xA	0	Invalid TPM AUX index (both old and new AUX indices present)
2			Class MTRR (Memory Type Range Register) Check
	1	0	MTRR Rule 1 Error
	2	0	MTRR Rule 2 Error
	3	0	MTRR Rule 3 Error
	4	0	MTRR Rule 4 Error
	5	0	MTRR Rule 5 Error
	6	0	MTRR Rule 6 Error
	7	0	Invalid MTRR mask value
	8	0	Invalid MTRR mapping
	9	0	Invalid MTRR count
3			Class Range Check
	1	Range index [1]	Basic Range Check failed: — Incorrect Range alignment; — Incorrect Range placement in container range; — Range top is less than Range base
	2	Index of first range [2]	Two ranges that must be separate are detected to be overlapping.
	3	Index of first range [2]	Two ranges that must be sequential in memory are detected to be not TANGENT_BELOW
4			Class TPM Access
	1	TPM Error	TPM returned an error. Error is reported as: Fatal error codes: — [23:16] – error code; — [24] = 0 Non-fatal error codes: — [23:16] – error code & 0xFF; — [24] = 1
	2	0	Invalid entry locality
	3	0	Invalid ACCESS register
	4	0	TPM NV is unlocked
	5	0	TPM disabled
	6	0	TPM deactivated
	7	0	Invalid TPM NV index
	8	0	Incompatible BIOS AC module
	9	0	Incompatible AUX index revision
	0xA	0	Input buffer too short to include write data
	0xB	0	Output buffer too short to include read data
	0xC	0	Secrets bit is set: Reset TPM EST bit is not allowed
	0x1B	0	Driver error: Output buffer too short for TPM response

	0x1C	0	Driver error: Invalid input parameters
	0x1D	0	Driver error: Invalid TPM response during command reception
	0x1E	0	Driver error: Invalid TPM response during command completion
	0x1F	1	Driver error: Response timeout (ERR_WAIT_COMMAND_READY)
	0x1F	2	Driver error: Response timeout (ERR_WAIT_SELFTEST_DONE)
	0x1F	3	Driver error: Response timeout (ERR_WAIT_STATUS_VALID)
	0x1F	4	Driver error: Response timeout (ERR_WAIT_BURSTCOUNT_READY)
	0x1F	5	Driver error: Response timeout (ERR_WAIT_COMMAND_COMPLETE)
	0x1F	6	Driver error: Response timeout (ERR_WAIT_ACCESS_VALID)
	0x1F	7	Driver error: Response timeout (ERR_WAIT_ACTIVE_LOCALITY)
5			Class Chipset Configuration
	1	0	One of mandatory ranges is not enabled: — BIOS AC: HEAP and DPR ranges are required for SCHECK function — SINIT: HEAP, SINIT, and DPR ranges are required.
	2	0	Incorrect size of one of mandatory ranges: — BIOS AC: HEAP and DPR ranges are checked in SCHECK function — SINIT: HEAP, SINIT, and DPR ranges are checked.
	3	0	Invalid GFX UMA size
	4	0	Invalid GTT UMA size
	5	0	Invalid GFX memory aperture size
	6	0	CS configuration is not locked – error is generated by SINIT
	7	0	Reserved
	8	0	TXT not locked
	9	0	Invalid Remap configuration
	0xA	0	Invalid ILP SMRR configuration
	0xB	0	Invalid SINIT configuration
	0xC	0	Invalid Local APIC configuration
	0xD	0	Invalid PMR configuration
	0xE	0	Invalid DPR configuration
	0xF	0	Invalid TOLUD configuration
	0x10	0	Invalid ME UMA configuration
	0x11	0	Invalid TOM configuration
	0x12	0	Graphics configuration register is not locked
	0x13	0	Graphics UMA configuration register is not locked
	0x14	0	Graphics GTT configuration register is not locked
	0x15	0	TSEG configuration register is not locked
	0x16	0	TOUUD configuration register is not locked
	0x17	0	Invalid PCEe configuration
	0x18	0	Wake error status bit is set
	0x19	0	Invalid flash configuration or flash is not write protected and locked
	0x1A	0	Invalid MCHBAR configuration
	0x1B	0	Invalid ILP SMRR2 configuration
	0x1E	0	Protected Audio/Video Path configuration error
	0x1F	0	UMAGFX register configuration error
6			Class Launch Control Policy (LCP)
	1	0	PO is required but not defined
	2	0	SINIT module is revoked
	4	0 – 4	No match is found for Element. Element type being processed is reported via minor error code.
	7	0 – 0x12	PO integrity check failed. Minor error code contains additional details
	8	0 – 0x12	PS integrity check failed. Minor error code contains additional details
	7, 8	1	Wrong signature of policy data file
	7, 8	2	Invalid number of lists
	7, 8	3	Policy data file is not accessible (wrong base, size, or above 4GB)
	7, 8	4	Policy data file hash mismatch
	7, 8	5	Policy data file size too large to fit heap indicated range
	7, 8	6	Invalid LCP_POLICY version
	7, 8	7	Invalid LCP_POLICY hash algorithm
	7, 8	8	Invalid LCP_POLICY policy type
	7, 8	9	Pre-production module is not allowed.

	7, 8	0xA	(List index#) + Invalid key size
	7, 8	0xB	(List index#) + Invalid list version
	7, 8	0xC	(List index#) + Invalid list size
	7, 8	0xD	(List index#) + Invalid signature algorithm
	7, 8	0xE	(List index#) + Invalid signature
	7, 8	0xF	(List index#) + List revoked
	7, 8	0x10	(List index#) + Invalid element hash algorithm
	7, 8	0x11	(List index#) + Invalid element size
	7, 8	0x12	(List index#) + PCR info integrity failure
	7, 8	0x13	No policy data
	9	0	NPW module: PO is required
	0x1E	0	PS index not defined
7			Class ACM exit
	1	0	RLP Join timeout
	2	0	RLP MCU is not loaded or debug MCU is loaded on production platform
	3	0	Invalid RLP SMRR configuration
	4	0	Invalid RLP SMRR2 configuration
8			Class Miscellaneous Checks
	1	0	Interrupt occurred
9			Class Heap table Data
	1	0	Invalid size of one of heap data tables.
	2	0	Invalid version of one of heap data tables
	3	0	Invalid PMRL alignment
	4	0	Invalid PMRH alignment
	5	0	Invalid MLE placement (Above 4GB)
	6	0	Invalid MLE requested capabilities
	7	0	Heap region is overfilled
	8	0	Incorrect extended element type
	9	0	Incorrect extended element size
	0xA	0	Heap table is not terminated by END element
	0xB	0	Wrong event log pointer
	0xC	0	Bad ACPI pointer
0xA			Class MC configuration sanity check
	1	0 - N	Memory controller sanity check failure. Minor error code contains sequential test number and is specific for chipset.
0xB			Class Alias Check
	1	0	64-bit interrupt detected
	2	0	Invalid SINIT code page mapping
	3	0	Memory alias detected
	4	0	GTT-based mapping failed
0xC			Class ACPI Check
	1	0	Invalid RSDP checksum
	2	0	RSDT not found
	3	0	Invalid RSDT checksum
	4	0	DMAR not found
	5	0	Invalid DMAR checksum
	6	0	MADT not found
	7	0	Invalid MADT checksum
	8	0	Invalid RSDP
	9	0	Invalid XSDT
0xD			Class DMAR Check
	1	0	Invalid DRHD BAR address
	2	0	INCLUDE_ALL bit is not set
	3	0	Invalid RMRR placement
	4	0	Invalid remapping structure type
	5	0	Invalid DMAR length
	6	0	One of IR or QI bits is not set extended capability register of one of VT-d engines or IR bit is not set in Flags field of DMAR table
	7	0	Host Address Width indicated in DMAR table is more than one supported by CPU
	8	0	Invalid DRHD device scope
0xE			Class PMR Configuration

	1	0	DMA remapping is enabled
	2	0	Invalid PMRL configuration
	3	0	Invalid PMRH configuration
0xF			Class MLE Header Check
	1	0	MLE Header linear address conversion error
	2	0	Invalid MLE GUID
	3	0	Invalid MLE version
	4	0	Invalid first page address
	5	0	Invalid MLE size
	6	0	Invalid MLE entry point address
	7	0	Incompatible RLP wake-up method
0x10			Class MLE Page Tables Check
	1	0	Basic Range Check failed: — Incorrect Range alignment; — Incorrect Range placement in container range; Ranges checked are: — PDPT page — PDT page; — PT page; — MLE page
	2	0	Page Table rule failure – new MLE page is not above previous one.
	3	0	Discovered big page (2MB)
	4	0	Page Table rule failure – PDPT, PDT, PT, MLE page are not in ascending order.
	5	0	Invalid MLE hashed size
	6	0	Invalid RLP entry point address
0x11			Class STM Check
	1	0	Basic Range Check failed: — Incorrect Range alignment; — Incorrect Range placement in container range; Ranges checked are: — MSEG — STM;
	2	0	Invalid MSEG base
	3	0	SMBASE not found
	4	0	Invalid IED base
	5	0	Illegal request to enable STM while either SINIT or MLE don't support STM
	6	0	STM is required but not present or cannot be enforced.
	7	0	Invalid MSEG size
	8	0	Invalid STM header ID
	9	0	Invalid STM header features
	0xA	0	Inconsistent CPU capabilities
	0xB	0	Blank STM header fields detected
	0xC	0	Invalid GDTR, EIP or ESP offset
	0xD	0	Invalid value in header.
	0xE	0	Incorrect STM SMM revision ID
0x13			Class PCR Integrity Check
	1	0	Wrong PCR17 value
	2	0	Wrong PCR18 value
	3	0	PCR format is not supported.
0x14			Class Event Log
	1	0	Incorrect Log Header GUID
	2	0	Incorrect Log Header version
	3	0	Inconsistent values of header fields
	4	0	Insufficient log size
	5	0	Incorrect Log Record version

1. Range index is reported according to project-specific common range table.
2. Despite that two ranges are in conflict, field width constrain allows to report only index of first conflicting range. Index is reported according to project-specific common range table.