Definition of the TXT.ERRORCODE register for 5th_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 5th Generation Intel® Core™ i7 and i5 vPro™ Processor Series Client TXT SINIT AC Module.

Table 1. TXT.Errorcode 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	= 1– induced by external software.
29:25	Reserved	Free for specific implementation
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 = ACM; 1 = MLE
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	0 = BIOS ACM 1 = SINIT

Table 2. 5th_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	1	Error in ACM launching: (ERR_LAUNCH_PARAM)
	1	2	Error in ACM launching: (ERR_LAUNCH_LEAF)
	1	3	Error in ACM launching: (ERR_LAUNCH_SENTER)
	1	4	Error in ACM launching: (ERR_LAUNCH_MEASUR)
	2	0	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 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)
	0xC	0	BIOS ACM return point is too close to 4GB
	0xD	0	Debug interface is not disabled/locked
2			Class MTRR 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	1	Invalid ACCESS register (ERR_ACC_INVLD_0_ON)
	3	2	Invalid ACCESS register (ERR_ACC_INVLD_0_OF)
	3	3	Invalid ACCESS register (ERR_ACC_INVLD_GEN_ON)
	3	4	Invalid ACCESS register (ERR_ACC_INVLD_GEN_OF)
	3	5	Invalid ACCESS register (ERR_ACC_INVLD_3_ON)
	3	6	Invalid ACCESS register (ERR_ACC_INVLD_3_OF)
	4	0	TPM NV is unlocked
	5	0	TPM disabled
	6	0	TPM deactivated

	7	1	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_AUX)
	7	2	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_AUX_ATTR)
	7	3	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_AUX_ALG)
	7	4	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_AUX_POL_SZ)
	7	5	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_AUX_POL_VAL)
	7	6	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_AUX_SIZE)
	7	7	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PO)
	7	8	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PO_ATTR)
	7	9	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PO_ALG)
	7	10	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PO_POL_SZ)
	7	11	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PO_POL_VAL)
	7	12	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PO_SIZE)
	7	13	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PS)
	7	14	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PS_ATTR)
	7	15	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PS_ALG)
	7	16	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PS_POL_SZ)
	7	17	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PS_POL_VAL)
	7	18	Invalid TPM NV index (ERR_TPM_NV_INDEX_INVALID_PS_SIZE)
	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
	0xD	0	TPM Interface not supported
	0xE	0	TPM Family not supported
	0xF	1	Bank Error (ERR_BANK_COUNT_EVT)
	0xF	2	Bank Error (ERR_BANK_COUNT_SEQ)
	0x10	0	Mandatory hashing algorithm not supported
	0x11	0	Read only index error
	0x12	1	Error Size Overflow (ERR_TPM_NV_DATA_SIZE_OVER_RD)
	0x12	2	Error Size Overflow (ERR_TPM_NV_DATA_SIZE_OVER_WR)
	0x12	3	Error Size Overflow (ERR_TPM_NV_DATA_SIZE_OVER_EV)
	0x13	0	TPM not present
	0x14	0	PCR Banks not supported
	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)
	0xFF	0	Time out for TPM response
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	CS configuration is locked – error is generated by BIOS AC
	8	0	LT lock (MSR 0x2E7) is not asserted
	9	1	Invalid Remap configuration (ERR_REMAP_CONFIG_EN)
	9	2	Invalid Remap configuration (ERR_REMAP_CONFIG_LEN)
	0xA	1	Invalid ILP SMRR configuration (ERR_SMRR_CONFIG_LOMSK)
	0xA	2	Invalid ILP SMRR configuration (ERR_SMRR_CONFIG_HIMSK)
	0xA	3	Invalid ILP SMRR configuration (ERR_SMRR_CONFIG_TYP)
	0xA	4	Invalid ILP SMRR configuration (ERR_SMRR_CONFIG_TSEG)
	0xB	0	Invalid SINIT configuration
	0xC	0	Invalid Local APIC configuration
	0xD	1	Invalid PMR configuration (ERR_PMR_CONFIG_EN)
	0xD	2	Invalid PMR configuration (ERR_PMR_CONFIG_RNG_L)
	0xD	3	Invalid PMR configuration (ERR_PMR_CONFIG_RNG_H)
	0xE	1	Invalid DPR configuration (ERR_DPR_CONFIG_EN)
	0xE	2	Invalid DPR configuration (ERR_DPR_CONFIG_SZ)
	0xF	0	Invalid TOLUD configuration
	0x10	1	Invalid ME UMA configuration (ERR_MEUMA_CONFIG_EN)
	0x10	2	Invalid ME UMA configuration (ERR_MEUMA_CONFIG_ALIGN)
	0x10	3	Invalid ME UMA configuration (ERR_MEUMA_CONFIG_VLD)
	0x10	4	Invalid ME UMA configuration (ERR_MEUMA_CONFIG_MATCH)
	0x10	5	Invalid ME UMA configuration (ERR_MEUMA_CONFIG_SZ)
	0x11	0	Invalid TOM configuration
	0x12	1	Invalid Graphics configuration register (ERR_GGC_CONFIG_EN)
	0x12	2	Invalid Graphics configuration register (ERR_GGC_CONFIG_LK)
	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	1	Invalid flash configuration or flash is not write protected and locked (ERR_FLASH_CONFIG_SZ)
	0x19	2	Invalid flash configuration or flash is not write protected and locked (ERR_FLASH_CONFIG_LK)
	0x1A	0	Invalid MCHBAR configuration
	0x1B	0	Invalid ILP SMRR2 configuration
	0x1C	0	Boot Guard configuration error
	0x1D	0	GFXVTBAR register configuration error
	0x1E	0	DLCK configuration error
6			Class Launch control policy
	2	1	SINIT module is revoked (ERR_SINIT_REVOKED_POL_CTR)
	2	2	SINIT module is revoked (ERR_SINIT_REVOKED_PS)
	2	3	SINIT module is revoked (ERR_SINIT_REVOKED_PO)
	3	0	Code is not used and is a placeholder for BIOS ACM revocation if implemented in future.
	4	0 – 4	No match is found for Element. Element type being processed is reported via minor error code.
	5	0	Auto-promotion failed.
	6	0	Failsafe boot failed. (FIT table not found or corrupted).
	7	0 – 0x14	PO integrity check failed. Minor error code contains additional details
	8	0 – 0x14	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	AUX Index Deletion
	7, 8	0xB	(List index#) + Invalid key size
	7, 8	0xC	(List index#) + Invalid list version
	7, 8	0xD	(List index#) + Invalid list size
	7, 8	0xE	(List index#) + Invalid signature algorithm
	7, 8	0xF	(List index#) + Invalid signature
	7, 8	0x10	(List index#) + List revoked
	7, 8	0x11	(List index#) + Invalid element hash algorithm
	7, 8	0x12	(List index#) + Invalid element size
	7, 8	0x13	(List index#) + PCR info integrity failure
	7, 8	0x14	No policy data
	7, 8	0x15	ERR_LIST_ECDSA_WRONG_KEY_SIZE
	7, 8	0x16	ERR_LIST_SM2_WRONG_KEY_SIZE
	7, 8	0x17	ERR_LIST_UNSUPPORTED_KEY_SIZE
	7, 8	0x18	ERR_LIST_UNSUPPORTED_HASH_ALG
	7, 8	0x19	ERR_POL_NO_HASH_ALG
	7, 8	0x1A	ERR_POL_UNSUPPORTED_HASH_ALG
	7, 8	0x1B	ERR_POL_NO_SIGNATURE_ALG
	7, 8	0x1C	ERR_POL_AUXHASH_INVALID_ALGMASK
	7, 8	0x1D	ERR_POL_AUXHASH_UNSUPPORTED_ALG
	7, 8	0x1E	ERR_POL_AUXHASH_INCOMPAT_PCR_ALG
	7, 8	0x1F	ERR_POL_PCONF_ENF_INCOMPAT_ELT_OVERRIDE
	9	0	NPW module: POwn is required
	0xA	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
	2	1	Config Timeout (Resources)
	3	1	Invalid Thread (Rendezvous)
	3	2	Invalid Thread (Missing)
	4	0	Internal Error
	5	x	Previous Error Detected
	6	0	Randomization error
	7	1	Copy Bounds Error (ERR_BOUNDS_PCR_EVENT)
	7	2	Copy Bounds Error (ERR_BOUNDS_PCR_EVENT_SEQ)
	7	3	Copy Bounds Error (ERR_BOUNDS_READ_PUBLIC)
	7	4	Copy Bounds Error (ERR_BOUNDS_PCR_BANKS_1)
	7	5	Copy Bounds Error (ERR_BOUNDS_PCR_BANKS_2)
	7	6	Copy Bounds Error (ERR_BOUNDS_PCR_BANKS_3)
9			Class Heap table Data
	1	0	Invalid size of one of heap data tables.
	2	1	Invalid version of heap data tables BIOS Data
	2	2	Invalid version of heap data tables OS SINIT Data
	3	0	Invalid PMRL alignment
	4	0	Invalid PMRH alignment
	5	0	Invalid MLE placement (Above 4GB)
	6	1	Invalid MLE requested capabilities - Wakeup
	6	2	Invalid MLE requested capabilities – PCR Map
	7	1	Heap region is overfilled (ERR_HEAPMEM_SIZE_OVER_ACPI_1)
	7	2	Heap region is overfilled (ERR_HEAPMEM_SIZE_OVER_ACPI_2)
	7	3	Heap region is overfilled (ERR_HEAPMEM_SIZE_OVER_ACPI_3)

	7	4	Heap region is overfilled (ERR_HEAPMEM_SIZE_OVER_HEAP_1)
	7	5	Heap region is overfilled (ERR_HEAPMEM_SIZE_OVER_HEAP_2)
	7	6	Heap region is overfilled (ERR_HEAPMEM_SIZE_OVER_HEAP_3)
	8	0	Incorrect extended element type
	9	0	Incorrect extended element size
	0xA	0	Heap table is not terminated by END element
	0xB	1	Wrong event log pointer (ERR_BAD_LOG_POINTER_PTR)
	0xB	2	Wrong event log pointer (ERR_BAD_LOG_POINTER_BASE)
	0xB	3	Wrong event log pointer (ERR_BAD_LOG_POINTER_PTR2)
	0xB	4	Wrong event log pointer (ERR_BAD_LOG_POINTER_PTR2_REQ)
	0xB	5	Wrong event log pointer (ERR_BAD_LOG_POINTER_PTR2_MATCH)
	0xB	6	Wrong event log pointer (ERR_BAD_LOG_POINTER_PTR2_ALG)
	0xB	7	Wrong event log pointer (ERR_BAD_LOG_POINTER_DUP_DSCR)
	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.
	2	0	VTD sanity check failure
	3	0	DMAR sanity check failure
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
0x12			Class UNCORE Patch Check.
	1	0	Incorrect thread data.
	2	0	Hash 256 mismatch.
0x13			Class PCR Integrity Check
	1	0	Wrong PCR17 value
	2	0	Wrong PCR18 value
	3	0	PCR format is not supported.
	4	0	PCR 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
0x15			Class Heap Table build

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.

§