Jetson Orin Fuse Specification

Application Note

Document History

DA-10877-001_v1.2

Version	Date	Description of Change
1.0	March 21, 2022	Initial release
1.1	December 14, 2022	Added fuses in Table 1
1.2	January 11, 2023	• Updated some fuses with additional description • Added Section "PSC Static OEM Key Purpose"

Table of Contents

List of Tables

Introduction

This application note provides a technical overview of the considerations and issues related to the NVIDIA® Jetson™ Orin module fuse specification. This covers the following series:

- Jetson AG Orin™ series
- Jetson Orin NX series
- Jetson Orin Nano™ series

The Jetson Orin modules include customer and original device manufacturer (ODM) programmable fuses. They are used to store security keys and ODM system design configuration options.

Fuses are divided into three distinct areas:

- Manufacturing Fuses (for example, security keys, boot options, and so on)
- ODM Field Fuses (for example, defined by ODM software for rollback protection, IDs, and so on)
- Ratchet Fuses (for example, used by NVIDIA software rollback protection)

All fuses default values are Logic 0 when not programmed. After they are programmed, they represent Logic 1.

Fuses that are deemed critical to the security of the Jetson Orin have built-in redundancy and are duplicated for glitch resistance. These corresponding fuses are called shadow fuses. See Section "Shadow Fuses," for additional information on shadow fuses.

ECC

Individual fuses can fail with very low probability and the fuse logic corrects these failures by using redundancy techniques:

- An OR-ECC, where two fuses are ORed together to get the corrected value. This code is unidirectional and protects against a 1b becoming a 0b.
- A block code ECC, based on a CRC, applied to a set of fuses. The ECC can correct one error in the set of protected fuses combined with very good error detection when more than one error is present. This ECC has much less overhead than the OR-ECC but requires groups of bits to be programmed together.

The exact ECC applied to specific fuses is specified per chip option, as part of the global fuse definition table. See the *Orin Series SoC Technical Reference Manual*. The two ECC methods are transparent to software when using fuse option registers to get access to fuse information but requires some care when programming fuses.

System Requirements

Jetson Orin contains all the power and logic to program the onboard fuses. The system designer does not have to make any provision on their own system design.

Fuse Types

Jetson Orin contains three types of fuses for ODM use. Those that configure the device and should be programmed during the system manufacturing process before the product is released to the end user, and those that may be programmed during the lifetime of the product by the ODM for software to use.

An example of each of these is as follows:

1. Manufacturing Fuses:
   a). Boot keys
   b). Boot device
   c). Product serial number
2. ODM Field Programmable Fuses:
   a). OTA information
3. Ratchet Fuses:
   a). Used by NVIDIA software to prevent rollback
   b). Used by ODM software to prevent rollback

Manufacturing Programmable Fuses

Jetson Orin modules contain multiple manufacturing fuses that control different items for security and boot. These fuses should be programmed during the manufacturing process. The ODM production mode fuse (also known as "Security Mode") should always be programmed by the ODM on the manufacturing line before the product is shipped to the end user. This fuse acts as a primary lock for all the manufacturing fuses. Once programmed it locks the values of the other manufacturing fuses. They cannot be programmed once the ODM production mode fuse has been programmed.

Note: All ODM and manufacturing programmable fuses have the value of ZEROs when shipped to an ODM.

! **CAUTION**: Programming a fuse (changing the value of a fuse from 0 to 1) is non-reversible. Once a fuse bit is programmed (set to 1), you cannot change the fuse value from 1 to 0. For example: A value of 1 (0x0001) can be changed to 3 (0x0011) or 7 (0x0111). It cannot however be changed to a value of 4 (0x0100) since bit zero is already programmed to 1.

The programming of fuses should be done without a system reset between different phases.

Table 1 lists the available fuses for Jetson AGX Orin.

Table 1. Fuse Names and Descriptions

Fuse Name	Fuse Description	Bit Length	Notes
FUSE_SECURITY_MODE_0	ODM Production Mode Also known as security mode. It enables security mechanisms for protecting the critical security fuses from being read and modified. This fuse must be programmed last.	1	
FUSE_SECURITY_MODE_SHADOW_0	Shadow of previous fuse	1	Notes 4, 7
FUSE_ARM_JTAG_DIS_0	Arm JTAG Disable Completely disables the external debug paths, including Arm JTAG path and USB SWD path. This field complements the Arm debug authentication field.	1	Note 3
FUSE_ARM_JTAG_DIS_SHADOW_0	Shadow of previous fuse	1	Note 7
FUSE_DEBUG_AUTHENTICATION_0	Arm Debug Authentication Provides fine control of Arm debug capabilities	5	Note 3

Fuse Name	Fuse Description	Bit Length	Notes
	Programming one of these fuses permanently disables the equivalent debug capability: • Bit [0] forces dbgen to 0 • Bit [1] forces niden to 0 • Bit [2] forces spiden to 0 • Bit [3] forces spniden to 0 • Bit [4] forces deviceen to 0		
FUSE_DEBUG_AUTHENTICATION_SHADOW_0	Shadow of secure bits of previous fuse: • Bit [0] shadows spiden (bit 2 of previous) • Bit [1] shadows spniden (bit 3 of previous)	2	Notes 4, 7
FUSE_KEYS_SBK_0_0 /../ FUSE_KEYS_SBK_0_7	Secure Boot Key (SBK), used by the PSCROM to validate boot images. This key may be programmed in encrypted form, with decryption performed by PSCROM,	256	Notes 1, 3, 6, 7
FUSE_KEYS_SBK_0_TAG_0	Tag information for the corresponding wrapped key	128	Note 6
FUSE_KEYS_FKDD_SK_0_0	Key Derivation Key input to the SE KDF function to derive OEM symmetrical keys	256	Note 6
FUSE_KEYS_FKDD_SK_0_TAG_0	CRC information protecting the corresponding key	32	Note 6
FUSE_KEYS_FKDD_AK_0_0	Key Derivation Key input to the SE KDF function to derive OEM asymmetrical type keys	256	Note 6
FUSE_KEYS_FKDD_AK_0_TAG_0	CRC information protecting the corresponding key	32	Note 6
FUSE_KEYS_OEM_FUSE_IV_0_0	Initialization vector used as part of the OEM fused keys encryption	96	Note 6
FUSE_KEYS_OEM_FUSE_IV_0_TAG_0	CRC information protecting the corresponding key (IV is technically not a key)	32	Note 6
FUSE_PUBLIC_KEY0_0 /../ FUSE_PUBLIC_KEY15_0	Public Key Hash (PKC) These registers encode a 512-bit hash of the main ODM public key. Can be revoked by field programmable fuse FUSE_REVOKE_PK_H0	512	Note 3
FUSE_PK_H1_0_0 /../ FUSE_PK_H1_15_0	Public Key Hash 1 These registers encode a 512-bit hash of the main ODM public key. Can be revoked by field programmable fuse FUSE_REVOKE_PK_H1	512	Note 3
FUSE_PK_H2_0_0 /../ FUSE_PK_H2_15_0	Public Key Hash 2 Optional key hash if public key revocation is supported; used when PCK0 and PCK1 are revoked	512	Note 3
FUSE_KEYS_OEM_EK_0_0	Endorsement Key	521	Notes 3, 6

Fuse Name	Fuse Description	Bit Length	Notes
	OEM Endorsement key, 521 bits stored with unused padding bits providing alignment to 32 bits fuse macro rows		
FUSE_KEYS_OEM_EK_0_TAG_0	Tag information for the corresponding wrapped key	128	Note 6
FUSE_KEYS_KDK0_0_0	Key Decryption Key, these keys can be programmed in encrypted form	256	Note 6
FUSE_KEYS_KDK0_0_TAG_0	Tag information for the corresponding wrapped key	128	Note 6
FUSE_KEYS_OEM_K1_0_0	OEM Key 1, no specific usage allocated in advance	256	Note 6
FUSE_KEYS_OEM_K1_0_TAG_0	Tag information for the corresponding wrapped key	128	Note 6
FUSE_KEYS_OEM_K2_0_0	OEM Key 2, no specific usage allocated in advance	256	Note 6
FUSE_KEYS_OEM_K2_0_TAG_0	Tag information for the corresponding wrapped key	128	Note 6
FUSE_KEYS_PSC_STATIC_OEM_0_0_0 FUSE_KEYS_PSC_STATIC_OEM_0_1_0	Static information reserved for ODM usage: [3:0]: OEM_K1_PURPOSE, defines the exact usage for key OEM_K1 [7:4]: OEM_K2_PURPOSE, defines the exact usage for key OEM_K2 [8]: OEM_CRC_PRESENT, CRC values are present for OEM fields, OEM CRC check status flags must be interpreted [9]: OEM_CBB_DEBUG_DIS, disable the debug path inside PSC CBB Bit [11:10] 2b Endorsement Key Curve Select 00b = NIST P256 01b = NIST P384 10b = Ed25519 11b = NIST P521 All other bits are reserved	32	Note 6, 9
FUSE_RESERVED_SW_0	Reserved Bits for software (read by Boot ROM) Bits [23:0] Boot Device Select – configure the boot process Bit [1:0] Boot device select 00b = Reserved 01b = QSPI 10b = Reserved 11b = Reserved Bit [3] Skip Device Selection straps Bit [6] 3 Button RCM mode enable	24	Note 3

Fuse Name	Fuse Description	Bit Length	Notes
	Bit [7] RCM SS Mode Enable – option to enable USB RCM to use SS transfer mode Bit [10] Enable Low Batt check and stall boot if SOC_GPIO02 is pulled low Bit [21:18] disable boot from selected boot device [18] = Reserved [19] = SPI [20] = Reserved [21] = Reserved Bit [22] Disable SC7-Exit Boot mode Bit [23] Disable entry into RCM mode Bits not listed are reserved.		
FUSE_BOOT_DEVICE_INFO_0	Boot Device Configuration Identifies the OS image boot device configuration. Used in conjunction with the Boot Device Selection to provide its configuration.	24	Notes 2,3
FUSE_BOOT_SECURITY_INFO_0	Boot Security Info Bits interpreted by boot software with following mapping: Bits [2:0] mapped to Secure Boot Authentication Scheme, where: 000b: SHA2-512 Hash (not recommended) 001b: 3072-bit RSA 010b: ECDSA P-256 Curve 011b: ECDSA P-521-Curve 100b: Ed25519 101b:XMSS – no Pre Hashing Bit [3] secure boot encryption scheme (SBK) enable Bit [4] ODM FEK usage enable Bits [8:5] ODM Fuse Encryption Key Select with Numerical Selection (0-15) Bit [9] ODM Key Valid Bit [11] OEM DICE1 Feature enable Bit [13] FMC DICE Feature enable Bits not listed are reserved	32	Notes 3,4,8
FUSE_SECURE_PROVISION_INFO_0	Factory Secure Provisioning Allows the ODM to control secure provisioning features: [0] is hide bit; [1] is test_part bit.	2	Note 3

Fuse Name	Fuse Description	Bit Length	Notes
	The hide bit ([0]) should be burned *before* burning SBK fuses if the Factory Secure Provisioning feature is being used.		
FUSE_CCPLEX_DFD_ACCESS_DISABLE_0	CCPLEX Low-Level DFD Access Disable CCPLEX power management DFD Disable access (when fuse is programmed, DFD access is disabled)	1	Note 3
FUSE_CCPLEX_DFD_ACCESS_DISABLE_SHADOW_0	Shadow of pervious fuse	1	Notes 4, 7
FUSE_ODM_INFO_0	ODM Info No predefined use, free to use by ODM	16	Note 3
FUSE_ODMID0_0 FUSE_ODMID1_0	ODM ID These 2 consecutive registers encode a 64-bit ODM ID.	64	Note 3
FUSE_H2_0	Hamming Code Implement the ECC for the ODM manufacturing fuses. This fuse must be programmed just before programming ODM Production Mode.	32	Notes 3,4
FUSE_FLW2_0	Force Large Weight This bit is used as part of the ECC scheme, burn to 1 to ensure field H2 has large enough weight.	1	Note 3
FUSE_OPT_CUSTOMER_OPTIN_FUSE_0	Customer OPTIN Enable Indicates if field burning of NV ratchet fuses for MB1/CCPLEX microcode is allowed.	1	Note 3
FUSE_ZEROIZE_DIS_0	When this fuse is programmed, zeroization is not allowed, that is, the keys that are identified as zeroizable otherwise cannot be programmed in the field: FKDD_{A,S}K PSC_{KD,E}K.	1	
FUSE_FUSE_INTEGRITY_CHECK_ENABLE_0	Perform integrity check (currently restricted to control word) and act if problems are detected	1	

Notes

1. SBK will be used to decrypt the bootloader and Boot Config Table if encryption is enabled through boot_security_info fuse.
2. See the boot options fuse configuration table (Table 4) for the correct Boot settings for your platform.
3. Fuse programming of ODM manufacturing programmable fuses is disabled when ODM Production Mode fuse = 1.
4. Further details will be made available in the *NVIDIA Orin Security Guidelines*. NVIDIA provides fuse programming software depending on the type of fuse and version of the supported OS software.
5. Check the secure boot software for the fuse programming operation.
6. This fuse is part of the PSC fuse. Refer to the “Platform Security Controller Fuses” section for additional information.
7. This fuse is part of the shadow fuses that provide redundancy. See Section “Shadow Fuses” for additional information.
8. Fuse encryption feature is not supported.
9. Refer to the “Platform Security Controller Fuses” section.

Platform Security Controller Fuses

The Platform Security Controller (PSC) fuses are special fuses that are implemented with special attention to security. They have specific burn requirements, as they cannot be read back in and become fully invisible to the software once they are programmed.

Some PSC fuses also include CRC/TAG fuse in addition to the fuse itself to provide CRC/TAG information for the corresponding fuses.

Note: Refer to the *NVIDIA Orin Security Guidelines* for any additional security-related information.

Debug Disable

There are two fuses that enable the ability to debug NVIDIA Jetson Orin SoC Arm-based processors.

ARM_JTAG_DISABLE

When programmed, this fuse permanently prevents any JTAG access to the debug access port that occurs through the JTAG pins on Orin SoC. This prevents any JTAG access by external Arm debuggers during normal product lifetime. This also disables the USB SWD debug path.

Note: ARM_JTAG_DISABLE only applied to Jetson AGX Orin. Jetson Orin NX, and Jetson Orin Nano do not have JTAG access.

Arm Debug Authentication Signals

These fuses control the standard Arm debug authentication signals. Each fuse forces the corresponding signal to 0 (disabled). Table 2 describes the Arm debug authentication signals.

Table 2. Arm Debug Authentication Signals

Signal Name	Description	Definition	Common Use Case
DBGEN	**Debug Enable** When asserted, enables invasive and non-invasive debug of non-secure state. Note that when DBGEN is not asserted access to debug components is generally still permitted, but those components are disabled.	NonSecure Invasive Debug Enable	CPUs to halt AXIAP to make system accesses ETR to stream trace to DRAM

Signal Name	Description	Definition	Common Use Case
NIDEN	Non-Invasive Debug Enable When asserted, enables non-invasive debug operations, such as trace, of non-secure state. NIDEN can be asserted independently of DBGEN.	NonSecure Non-Invasive Debug Enable	PTM trace from CPUs
SPIDEN	Secure Privileged Invasive Debug Enable When asserted along with DBGEN, enables invasive and non-invasive debug of Secure state.	Secure Invasive Debug Enable	AXI_AP to make secure accesses into the system ETR to write to Secure DRAM
SPNIDEN	Secure Privileged Non-Invasive Debug Enable When asserted along with NIDEN, enables non-invasive debug of Secure state.	Secure Non-Invasive Debug Enable	Accessing Secure registers in PMU and CPUs over the debug APB
DEVICEEN	Device Debug Enabled Enables the external debug tools connection to the device. This signal also drives the DBGSWENABLE, which is an enable input signal of the CoreSight Components and Cortex-A series processor.	Device Enable	Accessing any registers on mapped over the debug APB

Secure Boot Key

These fuses should be programmed with the Secure Boot key if SBK is being used. The SBK values are hidden once the ODM production mode fuse has been programmed.

Public Key Hash

These fuses should be programmed with the hash of the ODM public key. Orin SoCs have three sets of public keys for the ODM to use, and two revocation fuses that will revoke the first two sets of the public key.

Skip Boot Device Selection Straps

This fuse determines if the boot device selection is determined by the straps or by the fuse settings. For production devices, it is recommended that the fuses are used to select the boot device. When programmed the fuses in the following tables are used to determine the boot device.

Boot Device Selection

Table 3 describes the boot selection register: FUSE_RESERVED_SW_0.

Table 3. Boot Selection Register

Register	Description	Values
FUSE_RESERVED_SW_0	Boot Device Select	0x0 = Reserved
		0x1 = QSPI
		0x2 = Reserved
		0x3 = Reserved
		0x4 = Reserved
		0x5 = Reserved
		0x6 = Reserved
		0x7 = Reserved

Boot Device Information

The fuses listed in Table 4 determine parameters for the boot device configuration register: FUSE_BOOT_DEVICE_INFO_0.

Table 4. Boot Device Configuration Register

Fuse Bits	Device	Description	Values (Default = 0x0)
7:0	QSPI	Mode: DMA Data Bus Width: DDR x4 Clk: 68 MHz Read Command: QUAD_READ	0x00
		Mode: DMA Data Bus Width: SDR x4 Clk: 81.6 MHz Read Command: QUAD_READ	0x01
		Mode: PIO Data Bus Width: SDR x1 Clk: 51 MHz Read Command: NORMAL_READ	0x02
		Mode: PIO Data Bus Width: SDR x1 Clk: 25 MHz Read Command: NORMAL_READ	0x03
		PCIe: x4 UPHY: 4/5/6/7 Mode: Boot Partition 0	0x03

Shadow Fuses

Several security sensitive fuses have an associated shadow to provide enhanced security through redundancy. For all of these, the shadow and the main fuse must always have the same value. To do so, the shadow fuse and the main fuse must be programmed in the same burn session. In other words, without a reset between the two burn operations, and with the shadow being programmed first.

PSC Static OEM Key Purpose

Table 5 describes the OEM Key Purpose for OEM_K1_PURPOSE and OEM_K2_PURPOSE.

Table 5. OEM Key Purpose for OEM_K1_PURPOSE and OEM_K2_PURPOSE

Register	Description	Values
OEM_Kn_PURPOSE	Key Purpose	0x0 = ENC
		0x1 = CMAC
		0x2 = HMAC
		0x3 = KW
		0x4 = KUW
		0x5 = KWUW
		0x6 = KDK
		0x7 = KDD
		0x8 = KDD_KUW
		0x9 = XTS
		0x10 = GCM
		0x11 = Reserved

ODM Field Programmable Fuses

The fuses in Table 6 are available for the system designer to use for programming during the product lifetime.

The **RESERVED_ODM** fuses are split into eight banks of 32 bits. The first four of these banks (0-3) can be locked out by setting the corresponding bit in the ODM Lock fuse. For example, to lock **RESERVED_ODM** Bank 1, then ODM LOCK Bit [1] should be set. This will prevent any unintentional programming of other bits in this bank.

RESERVED_ODM Banks 4-7 do not have this lock feature.

RESERVED_ODM Banks 4-7 are ratchet fuses.

Table 6. Field Programmable Fuses

Fuse Name	Fuse Description	Bit Length
Reserved_ODM (FUSE_RESERVED_ODM0_0) /../ (FUSE_RESERVED_ODM7_0)	The consecutive registers are reserved for the customer use, including ODM/software versioning. These fuses are field programmable, Reserved_ODM{0:3} can be individually locked against further programming using corresponding bits in ODM_Lock, bit [b] locks Reserved_ODM{b}.	256
ODM_lock (FUSE_ODM_LOCK_0)	ODM_lock[i] disables further changes to the i-th 32 bits subset of the reserved ODM field. Applicable to the first four subsets only. FUSE_ODM_LOCK [0] = Reserved_ODM[0] FUSE_ODM_LOCK [1] = Reserved_ODM[1] FUSE_ODM_LOCK [2] = Reserved_ODM[2] FUSE_ODM_LOCK [3] = Reserved_ODM[3]	4
FUSE_SYSTEM_FW_FIELD_RATCHET0_0 /../ FUSE_SYSTEM_FW_FIELD_RATCHET3_0	Ratchet fuses for system FW	128
FUSE_BCT_FIELD_RATCHET_0	Similar to other ratchet fuses, but to qualify the BCT (that is, not a software image).	16
FUSE_OPT_NVJTAG_PROTECTION_ENABLE_0	NVJTAG Protection Enable This bit is used to permanently disable the access to restricted registers controlling the Design for Test functions. Setting this bit to 1b will disable the ability to put a production chip into the Failure Analysis (FA) lifecycle state for deeper level debugging and analysis. Refer to Section "Design for Test" in the latest version of *NVIDIA Orin Security Guidelines* for additional information.	1
FUSE_REVOKE_PK_H0_0	Revoke PK_H0	1
FUSE_REVOKE_PK_H1_0	Revoke PK_H1	1

Ratchet Fuses

This section describes the ratchet fuses for the Orin SoCs.

Ratchet Fuses for NVIDIA Software Rollback Protection

Ratchet fusing is a mechanism which NVIDIA uses to prevent insecure release of firmware from being used in the future.

There are two components to this mechanism. For each piece of firmware, there is a revision version that is set in the factory before delivery to the ODM. There is also a set of ratchet fuses that have a thermometer encoding and can be incremented in the field (**xxx_FIELD_RATCHET**).

Each piece of firmware has a notion of the number of security releases, which have occurred since it was created. This can be expressed as a sum of the revision fuse and the **FIELD_RATCHET** fuse (decoded from the thermometer) on the part. If firmware finds that it is running on a chip, which was created or updated with a security release newer than the firmware, then it will refuse to run. If the firmware is newer than the chip, then it will continue to boot but express a value in a secure scratch register. This is a desired value to update the **FIELD_RATCHET** fuse to.

Table 7. Field Programmable Ratchet Fuses

Fuse Name	Fuse Description	Bit Length
FUSE_CCPLEX_UCODE_FIELD_RATCHET_0 [31:0] FUSE_CCPLEX_UCODE_FIELD_RATCHET0_0	Thermometer encoded values	32
FUSE_MB1_FIELD_RATCHET_0 [31:0] FUSE_MB1_FIELD_RATCHET_0		32

Note: ODM can implement its own software components that are protected by their own ratchets using ODM field programmable fuses.

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

Unless specifically agreed to in writing by NVIDIA, NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA, the NVIDIA logo, Jetson, Jetson AGX Orin, Jetson Orin Nano, and NVIDIA Orin are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Arm

Arm, AMBA, and Arm Powered are registered trademarks of Arm Limited. Cortex, MPCore, and Mali are trademarks of Arm Limited. All other brands or product names are the property of their respective holders. "Arm" is used to represent Arm Holdings plc; its operating company Arm Limited; and the regional subsidiaries Arm Inc.; Arm KK; Arm Korea Limited.; Arm Taiwan Limited; Arm France SAS; Arm Consulting (Shanghai) Co. Ltd.; Arm Germany GmbH; Arm Embedded Technologies Pvt. Ltd.; Arm Norway, AS, and Arm Sweden AB.

Copyright

NVIDIA Corporation | 2788 San Tomas Expressway, Santa Clara, CA 95051
http://www.nvidia.com