

SEMI T23-0119

SPECIFICATION FOR SINGLE DEVICE TRACEABILITY FOR THE SUPPLY CHAIN

This Standard was technically approved by the Traceability Global Technical Committee. This edition was approved for publication by the global Audits and Reviews Subcommittee on December 17, 2018. Available at www.semiviews.org and www.semi.org in January 2019.

1 Purpose

1.1 Background

1.1.1 Device-level identification (device ID), implemented in individual die/designs, has been traditionally used by the silicon designers and manufacturers to trace die through the silicon manufacturing flow to aid the enhancement of silicon fab yields. An additional benefit of this identification (ID) is to be able to trace individual die and packaged parts through their final application testing in the final product before shipping to a customer. The ID can also be used to trace parts that subsequently fail in the field.

1.1.2 The recent evolution of data analytics is now allowing, via the device ID, end to end data analysis of single dies' performances from initial wafer test to the product level test and field performance. Analysis of a device's data in its native mode compared to its initial wafer or package (final test) testing data, now allows further in-depth yield learning. Silicon device fail data from failing die during the product manufacturing test (that forms the device's defective parts per million [DPPM]), can be correlated back to the wafer and final test manufacturing test data to find new issues, for example, silicon test coverage gaps and systematic and random defects found only during product level or system level test. Adding device ID to a component provides an extended opportunity to improve product quality and reduce DPPMs. Further, if a field recall is needed, individual faulty parts can be traced, thus greatly reducing the size of a recall, where all parts may have to be recalled if no device ID were present.

1.1.3 Device designers, manufacturers and suppliers that do not implement device IDs in their devices will be missing out on this opportunity to reduce DPPM. Many applications, like networking, medical and automotive are requiring the lowest possible DPPMs (trending to zero). Device ID for end to end traceability is one way to enable this continued quest for highest quality.

1.2 This Document establishes a standardized approach for enabling traceable device ID throughout the IC manufacturing, test, and assembly processes to the point of use in the final system. Suppliers and board-level manufacturers can use this unique identifier to communicate about a specific device for the purposes of performance or failure analysis. The unique identifier will enable the ability to send manufacturing data back and forward through the supply chain to perform data analysis.

2 Scope

2.1 This Standard provides a model focusing on the minimum of key concepts, behaviors, and requirements for enabling device ID and traceability. This Standard is intended for implementation by materials suppliers, device designers, device makers, board manufacturers, and system integrators from various industry sectors such as semiconductor, automotive, and medical. This Standard applies to different device configurations ranging from single integrated circuits to multi-chip/3D structures. This Standard can be adapted for use with a range of technologies, ranging from legacy systems to the latest in electronic chip identification (ECID) and 2D code package marking. This Standard defines, at a high level, the minimum requirements for device ID and traceability for new design and manufacturing implementation as well as for backwards compatibility with existing methods.

NOTICE: SEMI Standards and Safety Guidelines do not purport to address all safety issues associated with their use. It is the responsibility of the users of the Documents to establish appropriate safety and health practices, and determine the applicability of regulatory or other limitations prior to use.

3 Limitations

3.1 This Standard does not cover specific implementations on how an ID could be read as well as how manufacturing data could be retrieved.

3.2 This Standard does not specify or place requirements on the manufacturing data linked to this ID that may be exchanged between business partners in the supply chain.

3.3 This Standard does not restrict how the device ID is marked on, or recorded in, the package.

3.4 While traceable data must be reported, this Standard does not cover what is included by the data.

3.5 This Standard does not cover the time period over which the data needs to be retained.

3.6 This Standard does not provide a solution for device security, but its execution must be compliant with current and anticipated future implementations.

4 Referenced Standards and Documents

4.1 SEMI Standards and Safety Guidelines

SEMI E142 — Specification for Substrate Mapping

SEMI T7 — Specification for Back Surface Marking of Double-Side Polished Wafers with a Two-Dimensional Matrix Code Symbol

SEMI T9 — Specification for Marking of Metal Lead-Frame Strips with a Two-Dimensional Data Matrix Code Symbol

SEMI T19 — Specification for Device Marking

4.2 IEEE Standard¹

IEEE 1149.1 — IEEE Standard for Test Access Port and Boundary-Scan Architecture

NOTICE: Unless otherwise indicated, all documents cited shall be the latest published versions.

5 Terminology

5.1 Abbreviations and Acronyms

5.1.1 *CM* — contract manufacturer

5.1.2 *DPPM* — defective parts per million

5.1.3 *ECID* — electronic chip identification

5.1.4 *ID* — identification

5.1.5 *IDM* — integrated device manufacturer

5.1.6 *ODM* — original design manufacturer

5.1.7 *OEM* — original equipment manufacturer

5.2 Definitions

5.2.1 *board manufacturer* — organization that integrates various devices into a functional assembly.

5.2.2 *device consumer* — a party that purchases devices from a device manufacturer or supplier.

5.2.3 *device manufacturer or supplier* — a party that provides devices to, and directly communicates with, the device consumer.

5.2.4 *designer* — the person or group of people who create the design and have the opportunity to include a readable unique ID.

5.2.5 *device* — The unit identified by the Unique ID including, but not limited to the following:

- *chip or die* — a single integrated circuit manufactured on a wafer

¹ Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, NY 10016-5997, USA; Telephone: +1.212.419.7900, Fax: +1.212.752.4929, <http://www.ieee.org>

- *device or package* — a packaged device
- *multi-chip module* — a packaged group of devices integrated in a multi-chip or 3D structure

NOTE 1: See also SEMI E142 device definition.

5.2.6 *device ID* — Unique identifier of a device including, but not limited to the following:

- *electronic ID (ECID)* — an identifier programmed into the device
- *Joint Test Access Group (JTAG)* — ECID that conforms to the Test Access Port as defined in the IEEE 1149.1 standard by the JTAG
- *physical ID* — any physical marking on a device to identify it (e.g., one dimensional and two-dimensional bar codes)

5.2.7 *fabless* — a company that designs, markets, and sells devices, but contracts out their production rather than owning its own factory.

5.2.8 *foundry* — independent subcontract wafer manufacturer.

6 Requirements

6.1 General Infrastructure

6.1.1 This Specification defines, at a high-level, the minimum requirements that must be in place for compliance. Essentially, these minimum requirements are that device designers and/or manufacturers must provide, for each device being sent to the next step in the supply chain, a unique identifier that can be externally read and used by the supplier to trace all relevant manufacturing data experienced in the manufacture of that device by them. The unique ID is accessible by the customer, but will not necessarily give access to the manufacturing data. The actual manufacturing data may be confidential in nature and its sharing between the parties will be negotiated by them on an individual basis, most likely under nondisclosure agreement (NDA). This unique identifier must be made available throughout the supply chain and may be in addition to other proprietary data.

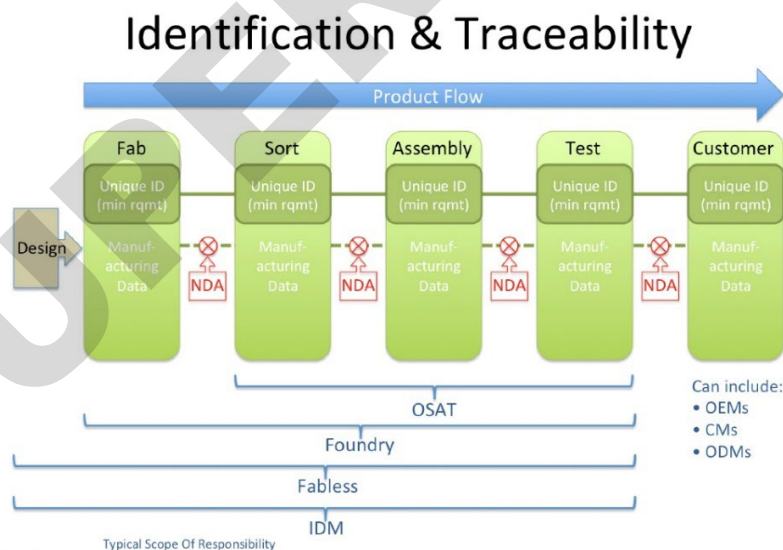


Figure 1
Device-Level Identification and Traceability Model

6.2 Device ID Requirements

- 6.2.1 The device ID must be unique to each individual device.
- 6.2.2 The device ID must be readable by external systems.