Intel® Active Management Technology

Technical Overview For Desktop Enablement

Intel Developer FORUM

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY RELATING TO SALE AND/OR USE OF INTEL PRODUCTS, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

Intel may make changes to specifications, product descriptions, and plans at any time, without notice.

The Cedar Mill, Conroe, Allendale, Presler processors, the Intel 945 Express (Lakeport), Broadwater chipsets, ICH7 or the ICH8 components may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available upon request.

All dates provided are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

Intel, the Intel logo, SpeedStep, NetBurst, SingleDriver and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Agenda

- Intel® AMT Features
- Intel® AMT Architecture
- Setup & Configuration
- Manufacturing & Validation
- Intel® AMT ISVs
- Questions

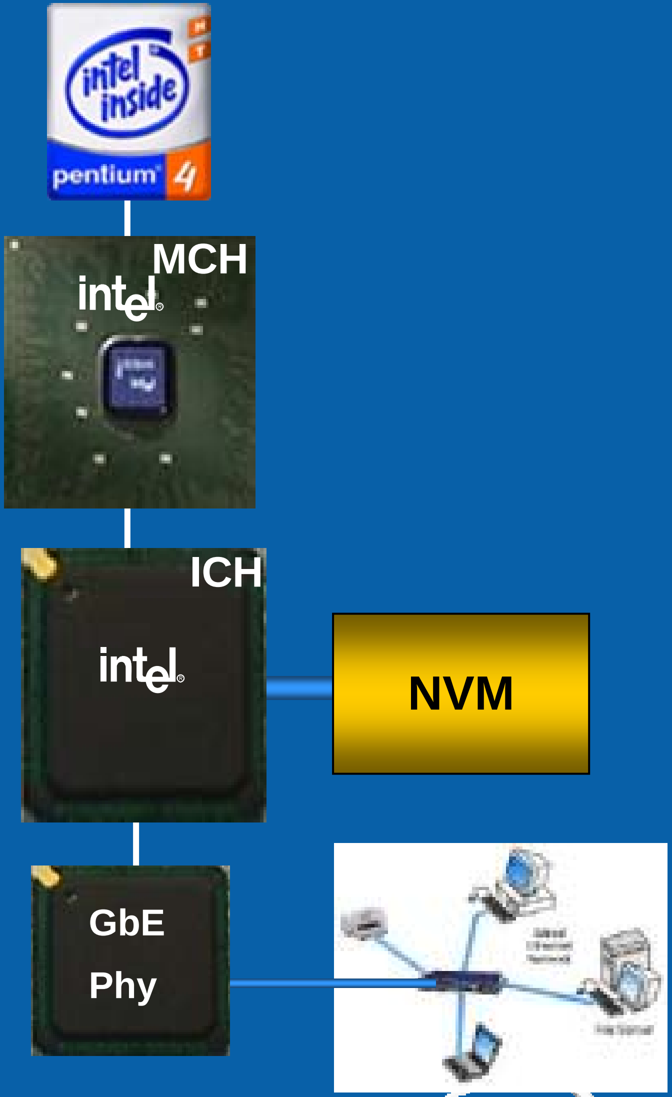
Averill Intel® AMT Overview

- Intel® Active Management Technology combines highly-available OOB remote management and network protection into an OS-independent and tamper-resistant solution to help address IT departments' top issues of network protection, asset management, and system reliability.

  Features:

  - H/W and S/W Asset Management
  - Provide OOB Diagnostics
  - *Circuit Breaker – Network Outbreak Containment (NOC) & Agent Presence (NEW)*
  - *Integrated H/W and S/W Platform Solution (NEW)*

- Intel® AMT solution is comprehensive including software support from top-tier security and management software vendors



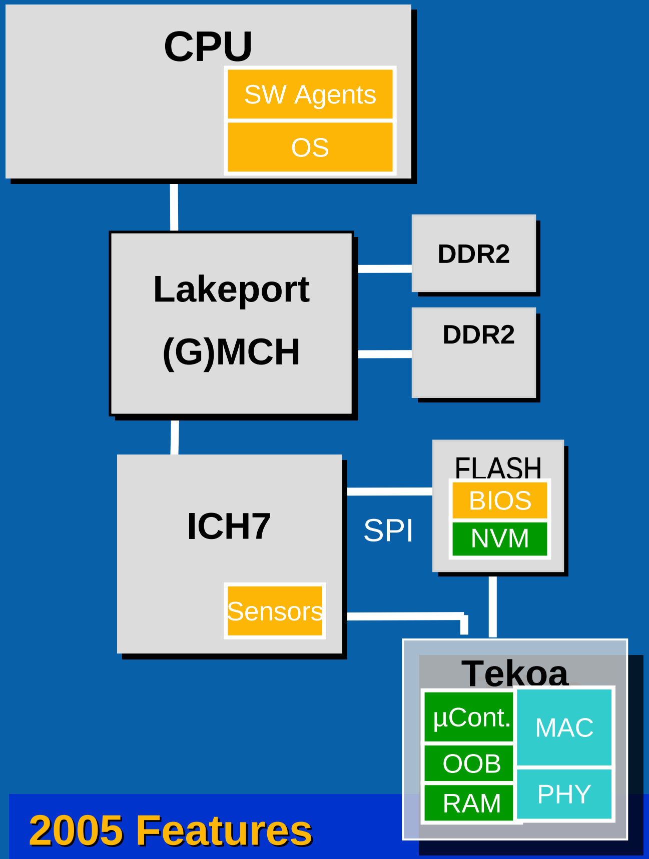
Features at a Glance

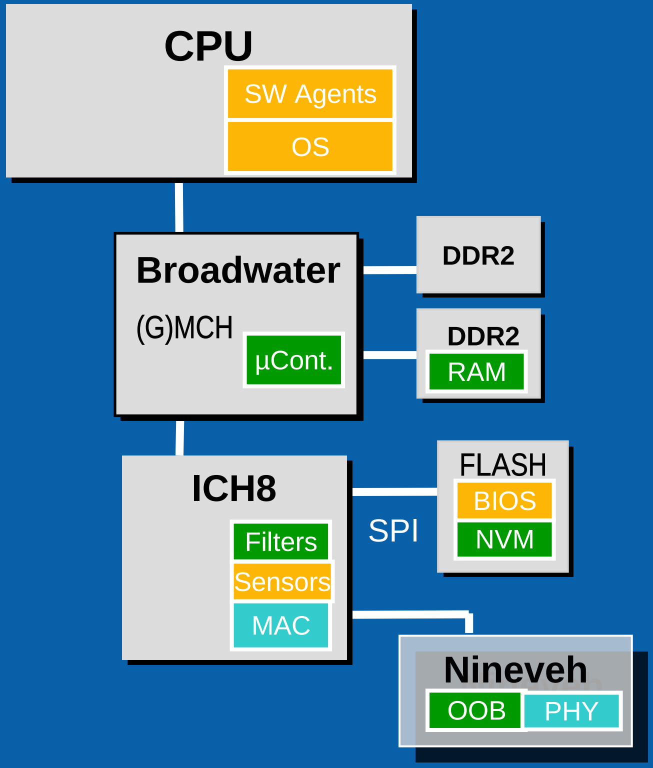
- Discover - OOB
  - Hardware Inventory
  - Software Inventory
- Heal - OOB
  - IDE-R
  - Serial Over LAN
  - Event Management
- Protect - OOB
  - Circuit Breaker
    - Network Outbreak Containment (inbound and outbound filters on ME)
    - Agent Presence
- Infrastructure - OOB
  - Network Admin
  - Security Admin
  - Mutual Authentication

Agenda

- Intel® AMT Features
- Intel® AMT Architecture
- Setup & Configuration
- Manufacturing & Validation
- Intel® AMT ISVs
- Questions

Intel® AMT Evolution





2005 Features

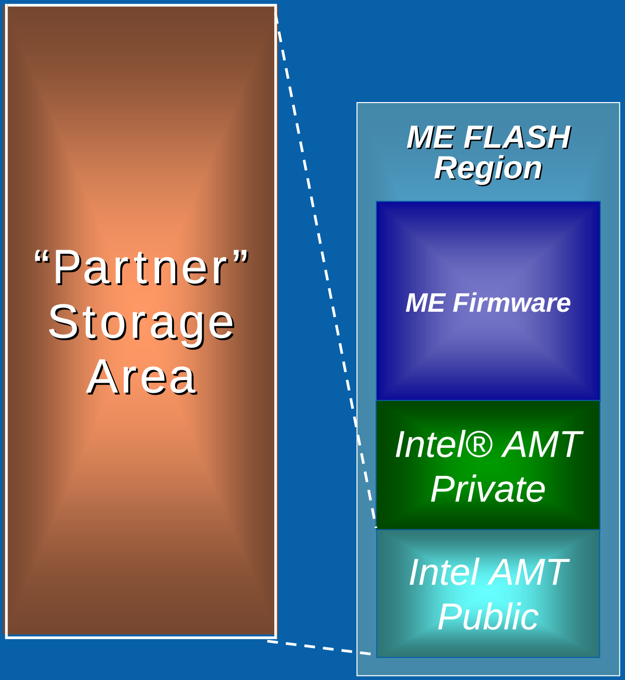
- OOB Diagnostics & Recovery
- Proactive Alerting
- Remote Asset Management
- IDE-R remote boot & SOL remote ctrl
- 3rd Party Non-Volatile Storage

2006 Features

- 2005 Features Plus…
- Uses system memory to reduce cost
- Circuit Breaker network isolation
- Agent Presence
- Increased 3rd Party Non-Volatile Storage

3rd Party Data Storage (3PDS)

Intel® AMT provides ISV applications a general purpose non-volatile data store



Intel® AMT will provide this capability through a Storage Manager implemented in the Intel® Management Engine (Intel® ME) firmware

- Accepts storage commands over local host and network interfaces
- Applications are uniquely identified using a concatenation of ISV and platform owner selected text strings plus a UUID
- Protects the space allocated by one application from other applications unless owning application grants permission
- Applications are responsible for any security mechanisms necessary to protect their stored data (e.g., encryption of sensitive data or keys)

NVM Flash Device

- Minimum Flash Size: 2MB (16Mb)
  - ~700KB reserved for BIOS & MEBx
  - The FW supports flash devices that have 4KB sector erase size.
  - Note: 64KB+ sector erase sizes not supported.
    - FW architecture uses block redundancy during data writes to ensure no data-loss in the event of a failure/corruption during the write.

Intel® ME External Memory

- A small amount of main memory is dedicated to execute ME code and store ME run-time data
  - Similar in concept to UMA for Intel® Extreme Graphics 2
  - Intel® ME code is stored compressed in Flash (no HDD access required) and loaded into UMA at bringup
- Memory used is ~.4% to .8% of a typical mainstream client memory configuration
- Utilizes channel 0 DIMM
  - MUST populate channel 0 DIMM for Intel® AMT to run
  - Host will continue to run if no channel 0 DIMM
- Chipset protects this range from access by the main CPU
  - No ability for malicious software to access this space
- Intel® ME can access its dedicated memory space in any S-state
  - GMCH can dynamically switch memory power state to allow Intel® ME access
  - Allows for low average power – since memory only "on" when needed

Agenda

- Intel® AMT Features
- Intel® AMT Architecture
- Setup & Configuration
- Manufacturing & Validation
- Intel® AMT ISVs
- Questions

Setup & Configuration

- What is Intel® AMT Setup?
  - When an Intel® AMT system is first delivered from the factory Intel® AMT is present, but "turned off"
    - Meets power regulatory guidelines
  - Intel® AMT Setup involves the steps necessary to "turn on" Intel® AMT
  - Setup is generally performed once

Setup & Configuration

- Types of Intel® AMT Setup
  - Small Business Mode
    - Can be accomplished completely using BIOS Extension interface and Web GUI interface
    - Supports HTTP Digest only (No TLS)
    - Used when enterprise infrastructure is not present
  - Enterprise Mode
    - Setup MUST be completed using a separate application running on the network (e.g. provisioning server)
    - Supports HTTP Digest and TLS security

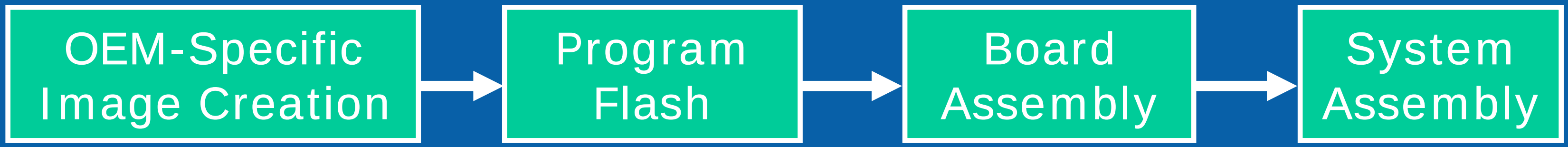
Setup & Configuration

- What is Intel® AMT Configuration?
  - Configuration involves supplying Intel® AMT with additional information to enable various features (e.g. User ACLs, Realms)
  - Configuration happens after Setup and can performed as needed

Agenda

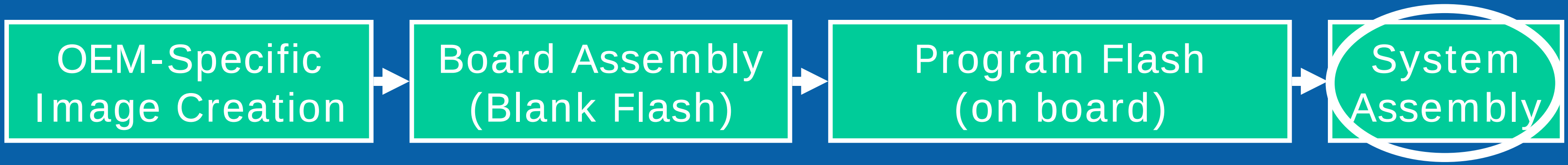
- Intel® AMT Features
- Intel® AMT Architecture
- Setup & Configuration
- Manufacturing & Validation
- Intel® AMT ISVs
- Questions

Manufacturing Flow

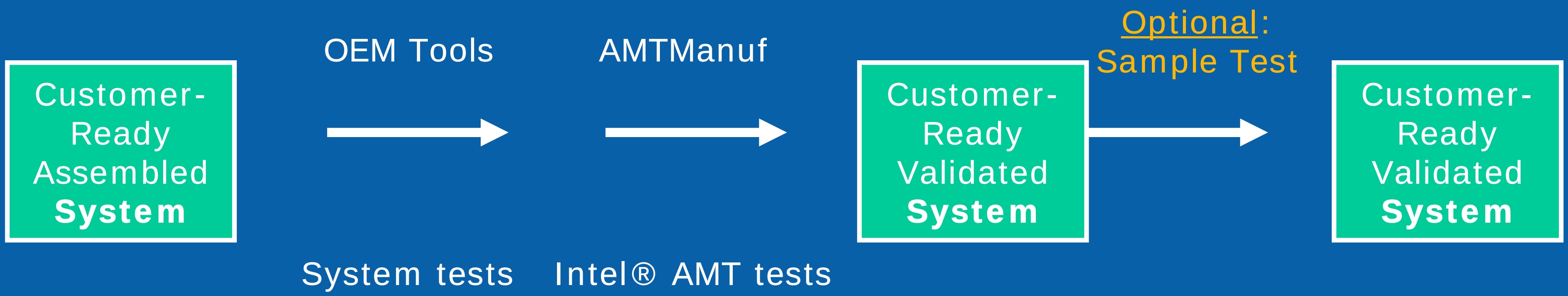


Detailed Flow in Backup

Validation



OEM-Specific Image Creation → Board Assembly (Blank Flash) → Program Flash (on board) → System Assembly



Customer-Ready Assembled **System**

OEM Tools

System tests

AMTManuf

Intel® AMT tests

Customer-Ready Validated **System**

Optional: Sample Test

Customer-Ready Validated **System**

Agenda

- Intel® AMT Features
- Intel® AMT Architecture
- Configuration and Setup
- Manufacturing & Validation
- Intel® AMT ISVs
- Questions

Intel® AMT Software

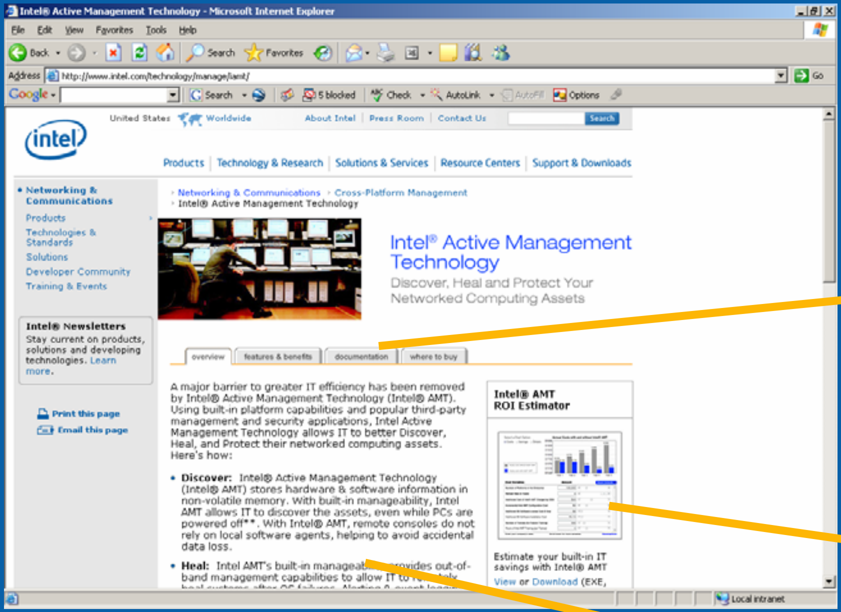
ISV	Application
Microsoft	System Management Server*
altiris intuitive > manageability	Notification Server*
bmc software	Marimba*
ca	Unicenter NSM* r11
Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.	Integrity*
Cisco Systems	Network Access Control
LANDesk SOFTWARE	LANDesk Mgmnt Suite* 8.6 LANDesk System Mgr* 8.6
Novell	Zenworks* 7
StarSoftComm	StarCenter* 2.0 StarNet*
symantec.	LiveUpdate*
TREND MICRO	OfficeScan*

Agenda

- Intel® AMT Features
- Intel® AMT Architecture
- Setup & Configuration
- Manufacturing & Validation
- Intel® AMT ISVs
- Questions

BACKUP

Where To Get More Info



Intel® Active Management Technology - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.intel.com/technology/manage/iamt/
Go
Google Search 5 blocked Check AutoLink AutoFill Options
United States Worldwide About Intel Press Room Contact Us Search
intel
Products Technology & Research Solutions & Services Resource Centers Support & Downloads
Networking & Communications
Products
Technologies & Standards
Solutions
Developer Community
Training & Events
Networking & Communications › Cross-Platform Management › Intel® Active Management Technology
overview features & benefits documentation where to buy
Print this page
Email this page
Local intranet

Intel® Newsletters
Stay current on products, solutions and developing technologies. Learn more.

Intel® Active Management Technology
Discover, Heal and Protect Your Networked Computing Assets

A major barrier to greater IT efficiency has been removed by Intel® Active Management Technology (Intel® AMT). Using built-in platform capabilities and popular third-party management and security applications, Intel Active Management Technology allows IT to better Discover, Heal, and Protect their networked computing assets. Here's how:

- **Discover:** Intel® Active Management Technology (Intel® AMT) stores hardware & software information in non-volatile memory. With built-in manageability, Intel AMT allows IT to discover the assets, even while PCs are powered off**. With Intel® AMT, remote consoles do not rely on local software agents, helping to avoid accidental data loss.
- **Heal:** Intel AMT's built-in manageab[illegible] provides out-of-band management capabilities to allow IT to re[illegible]tely

Intel® AMT ROI Estimator
Estimate your built-in IT savings with Intel® AMT
View or Download (EXE,

Documentation

CD Demo

Technology @ Intel Articles

Intel® AMT Technology Overview

Intel® AMT Whitepaper

Intel® AMT ROI Estimator

Intel® AMT ISV Solutions Briefs

Worldwide Intel® AMT Web Sites:

Taiwan: resource.intel.com/technology/manage/iamt/tc
Korea: resource.intel.com/technology/manage/iamt/kr
PRC: www.intel.com/technology/manage/iamt/sc
France: www.intel.com/cd/network/communications/emea/fra
Germany: www.intel.com/cd/network/communications/emea/deu
Italy: www.intel.com/cd/network/communications/emea/ita
Spain: www.intel.com/cd/network/communications/emea/spa
Russia: www.intel.com/cd/network/communications/emea/rus
United Kingdom: www.intel.com/cd/network/communications/emea/eng

http://www.intel.com/technology/manage/iamt/

ASF & AMT Feature Comparison

Capabilities	ASF	Intel® AMT
OOB Mgt (Any OS/power state)	No	Yes
Remote Control	Remote Reboot only	Serial Over LAN, Win EMS
Event Alerting	Yes (preset)	Yes (policy based)
Non-Volatile Storage	No	Yes
Event Logging	No	Yes
Remote Reboot	Yes (PXE)	Yes (PXE or IDE-R)
Asset Information	No	Yes
Remote BIOS Update	No	Yes
Secure Communications	Simple authentication	SSL 3.1/TLS encryption, HTTP authentication
Connection Protocol	RMCP	HTTP (web browser access)
Layer 4 Stack	UDP (often blocked by routers)	TCP (preferred routing protocol)
Broad Enterprise ISV Support	No	Yes

IT Survey Results: Top 5 Problems

2006

2005

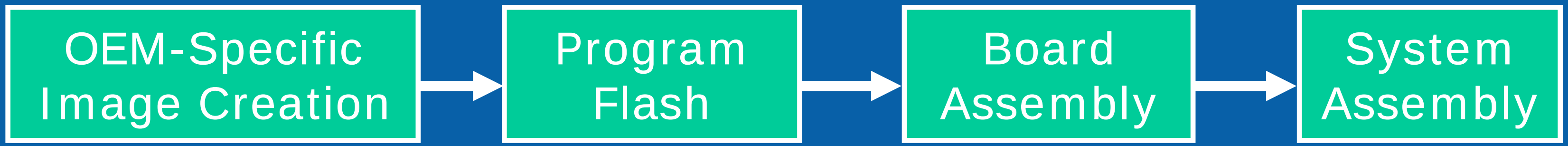
Pri	Problem	Wish list
1	**Protecting from inside:** e.g., systems bringing in many viruses	Route unknown systems to the *not ok* corral, isolate and fumigate. Need non-removable agents, to stop anomalies.
2	**Asset management:** e.g., Hard to locate systems, query basic information	Active location ID, Asset list available in any state, Non-removable agents persistent across installation of new OS images.
3	**OOB mgmt & online diagnostics:** e.g., Users remove agents. No automated FW/OS update. Can't probe a hung system. Time to repair is large	OOB mgmt, detect anomalies. Online diagnostic when the system fails Below the O/S Agent (available when system hangs, accepts updates)
4	**Application integration complexity:** e.g., Lack of standards to Integrate apps	XML Standards, self-describing objects, policies.
5	**Dynamic Resource Allocation:** e.g., Memory/CPU, etc "hard-allocated" to single apps	Support for dis-aggregation of resources.

Glossary

- ASF: *Alert Standard Format* – PC NIC-based platform instrumentation
- BMC: Baseboard Management Controller – a microcontroller embedded on the main system board to provide out-of-band access to platform instrumentation, sensors and effectors
- DTW: *Down-the-wire* – network-based remote access to systems for monitoring, managing, provisioning and troubleshooting them
- DMTF: *Distributed Management Task Force* – a standards body devoted to manageability
- EFI: *Extensible Firmware Interface* – software technology from Intel that improves on traditional BIOS firmware
- IPMI: *Intelligent Platform Management Interface* – server platform instrumentation firmware
- Intel® AMT: *Active Management Technology* – implementations arising from the Intel® Cross Platform Manageability Program
- Intel® CPMP: *Cross Platform Manageability Program* – industry-wide Intel effort to develop and market interoperable management solutions with scalable capabilities, interfaces and protocols supporting all Intel platforms
- NIC: *Network Interface Chip (or card)* – hardware that enables a system to connect to a local area network (LAN)
- OOB: *Out-of-Band* – remote access to a connected system regardless of the state of the OS or power
- PXE: *Pre-boot eXecution Environment* – enables a system to boot from the network
- SIPP: *Stable Image Platform Program* – Intel® OEMs assure that desktop & notebook chipsets & drivers remain consistent for 12 months
- SMASH: *System Management Architecture for Server Hardware* – the new name for DMTF's SMWG spec
- SMWG: *Server Management Working Group* – the DMTF group developing a spec to standardize platform management consoles and related software technology
- SOA: *Service Oriented Architecture* – event-driven solutions of loosely-coupled software components often based on XML Web services
- SOAP: *Simple Object Access Protocol* -- call-response mechanism for XML documents which operates in a client-server paradigm
- SOI: *Service Oriented Infrastructure* – a virtualized "landing zone" for SOA solutions in which hardware is managed as a utility
- TCG (TCPA): *Trusted Computing Group (formerly the Trusted Computing Platform Alliance)* -- an alliance of Microsoft, Intel, IBM, HP and AMD which promotes a standard for a more secure PC
- TPM: *Trusted Platform Module* – a hardware instantiation of the TCG (TCPA) specification for a more secure PC
- UDDI: *Universal Description, Discovery & Integration* -- a service for locating Web services by enabling robust queries against rich metadata
- WOL: *Wake-up On LAN* – to remotely boot a system on the network
- WSDL: *Web Services Description Language* -- an XML language for describing Web services using a model of what the service offers
- WS: *Web Services* – software components based on vendor-neutral specifications (XML, SOAP, WSDL and UDDI) which enable application integration and SOA solutions to run across virtually all types of systems
- XML: *eXtensible Markup Language* – a common data format used by Web services software running on any system

Manufacturing & Validation Detailed Flow

Manufacturing Flow



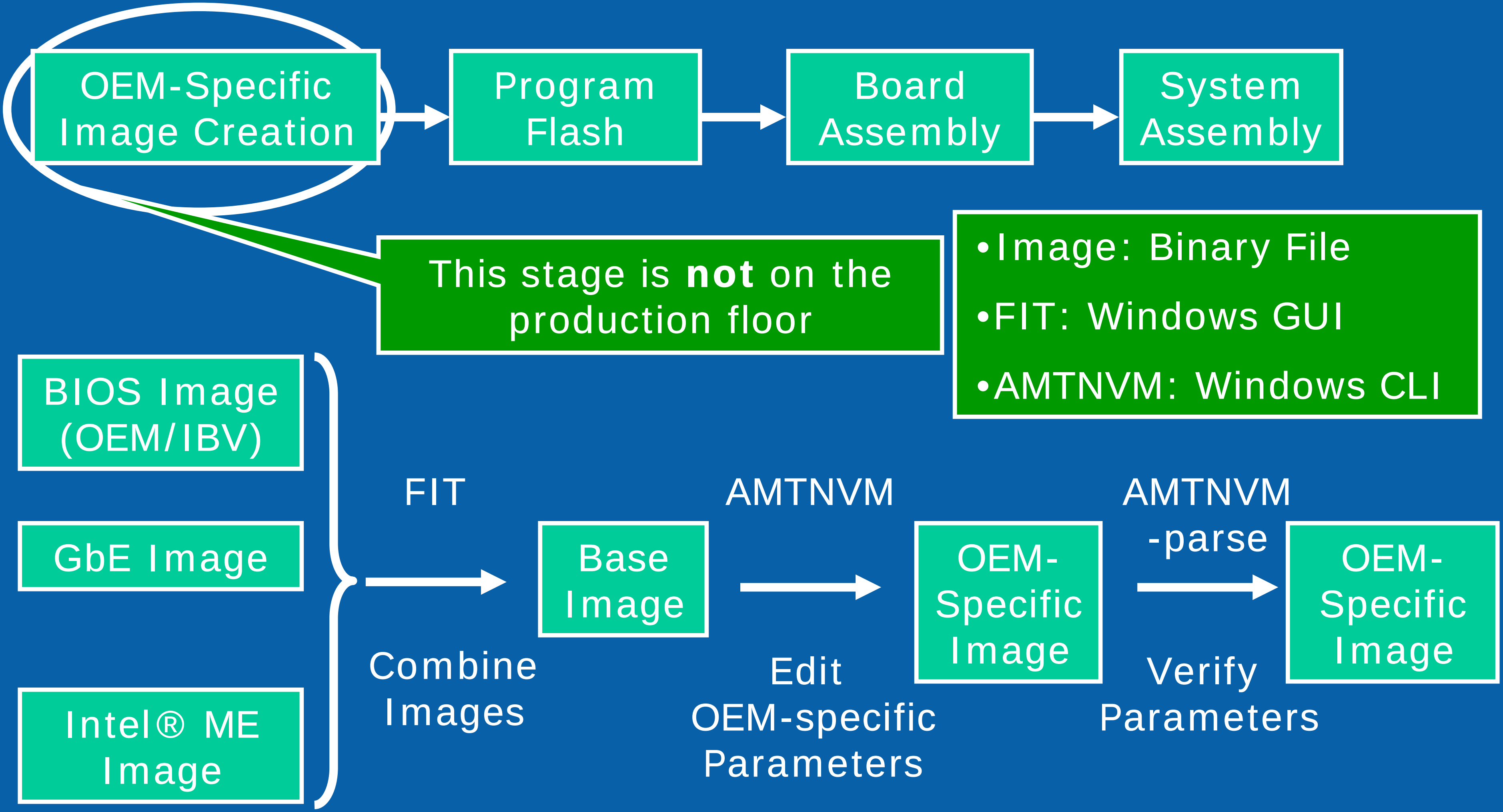
OEM-Specific Image Creation

Program Flash

Board Assembly

System Assembly

FW Image Creation



OEM-Specific Image Creation → Program Flash → Board Assembly → System Assembly

This stage is **not** on the production floor

- Image: Binary File
- FIT: Windows GUI
- AMTNVM: Windows CLI

BIOS Image (OEM/IBV)

GbE Image

Intel® ME Image

FIT

Combine Images

Base Image

AMTNVM

Edit OEM-specific Parameters

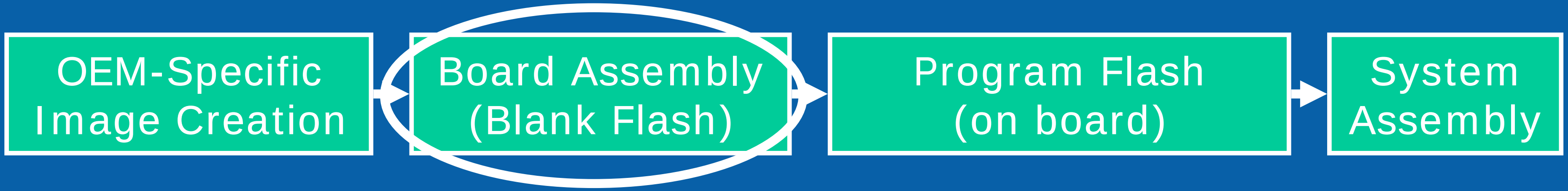
OEM-Specific Image

AMTNVM -parse

Verify Parameters

OEM-Specific Image

Board Assembly

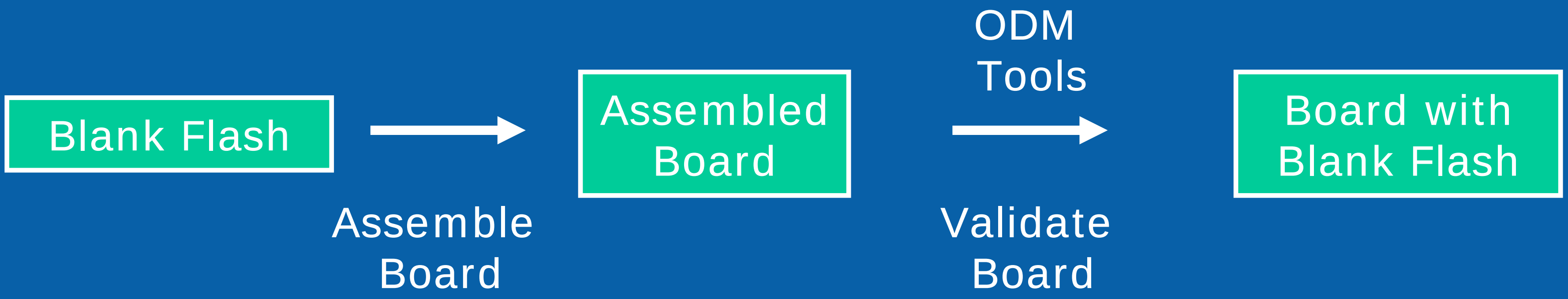


OEM-Specific Image Creation

Board Assembly (Blank Flash)

Program Flash (on board)

System Assembly



Blank Flash

Assemble Board

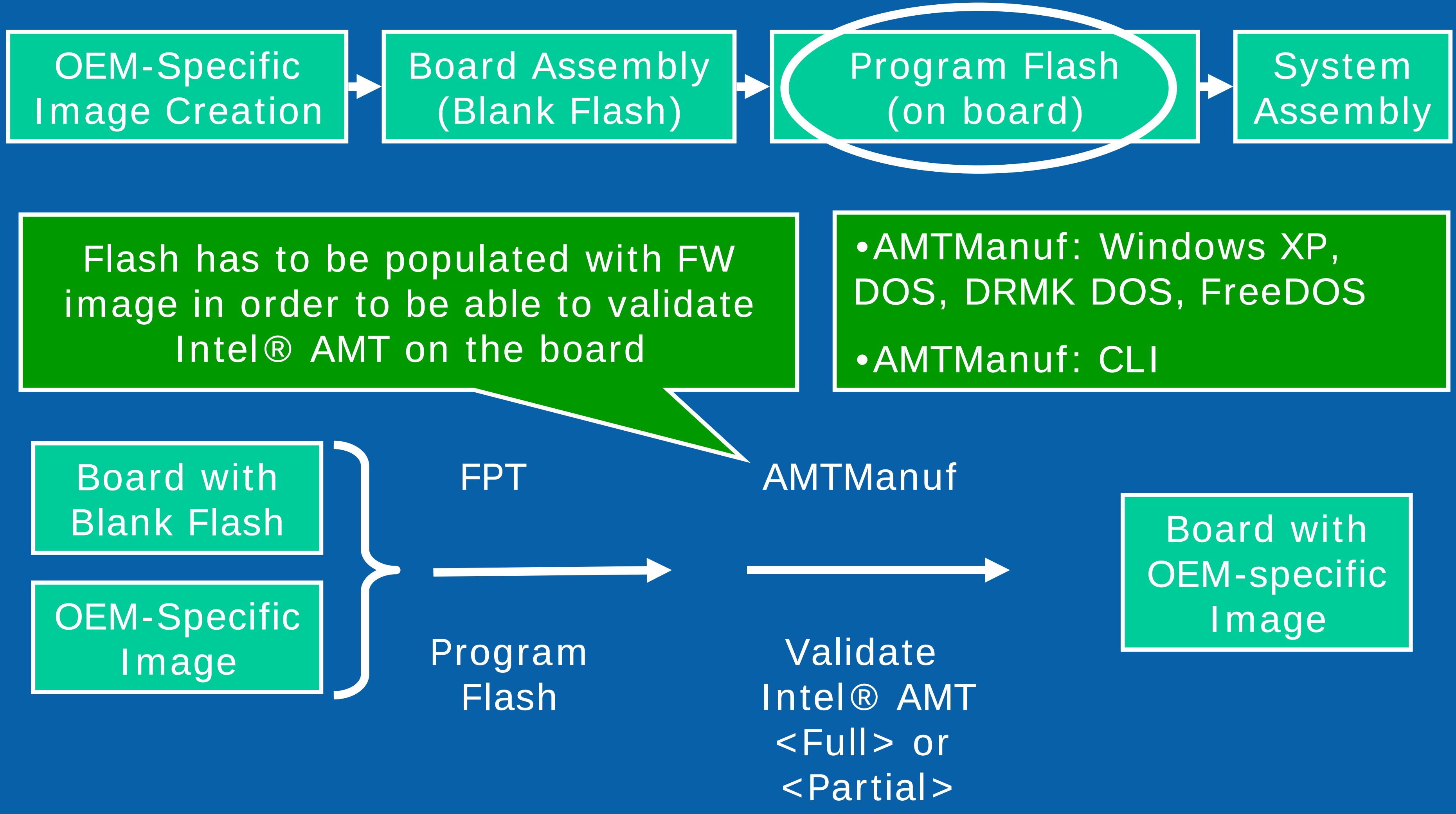
Assembled Board

ODM Tools

Validate Board

Board with Blank Flash

SPI Programming



OEM-Specific Image Creation → Board Assembly (Blank Flash) → Program Flash (on board) → System Assembly

Flash has to be populated with FW image in order to be able to validate Intel® AMT on the board

- AMTManuf: Windows XP, DOS, DRMK DOS, FreeDOS
- AMTManuf: CLI

Board with Blank Flash

OEM-Specific Image

FPT

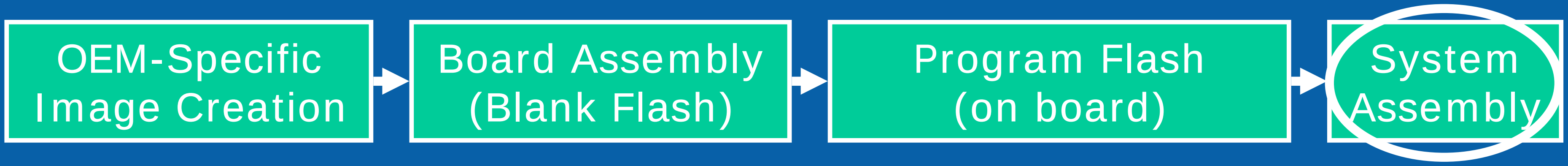
Program Flash

AMTManuf

Validate Intel® AMT <Full> or <Partial>

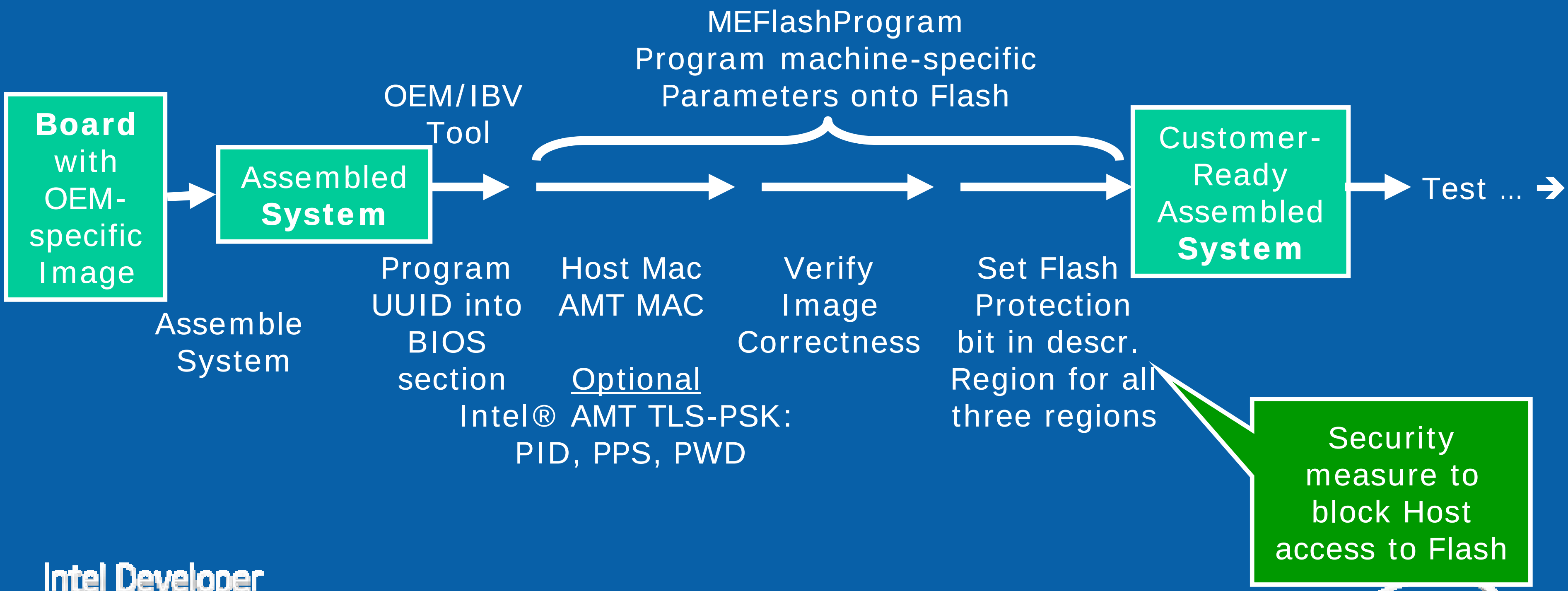
Board with OEM-specific Image

System Assembly



OEM-Specific Image Creation → Board Assembly (Blank Flash) → Program Flash (on board) → System Assembly

- MEFlashProgram: Windows XP, DOS, DRMK DOS, FreeDOS
- MEFlashProgram: CLI



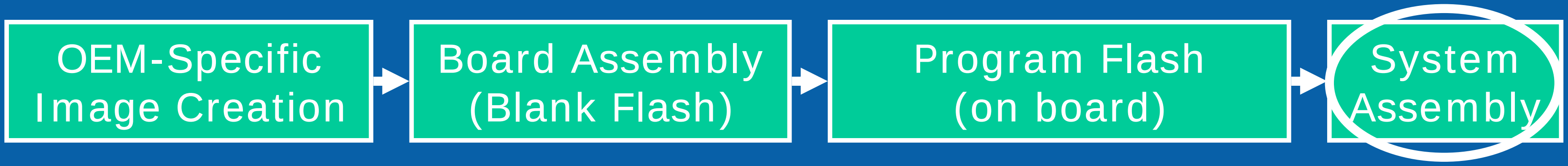
MEFlashProgram
Program machine-specific
Parameters onto Flash

Board with OEM-specific Image → Assemble System → Assembled System → OEM/IBV Tool: Program UUID into BIOS section → Host Mac AMT MAC → Verify Image Correctness → Set Flash Protection bit in descr. Region for all three regions → Customer-Ready Assembled System → Test … →

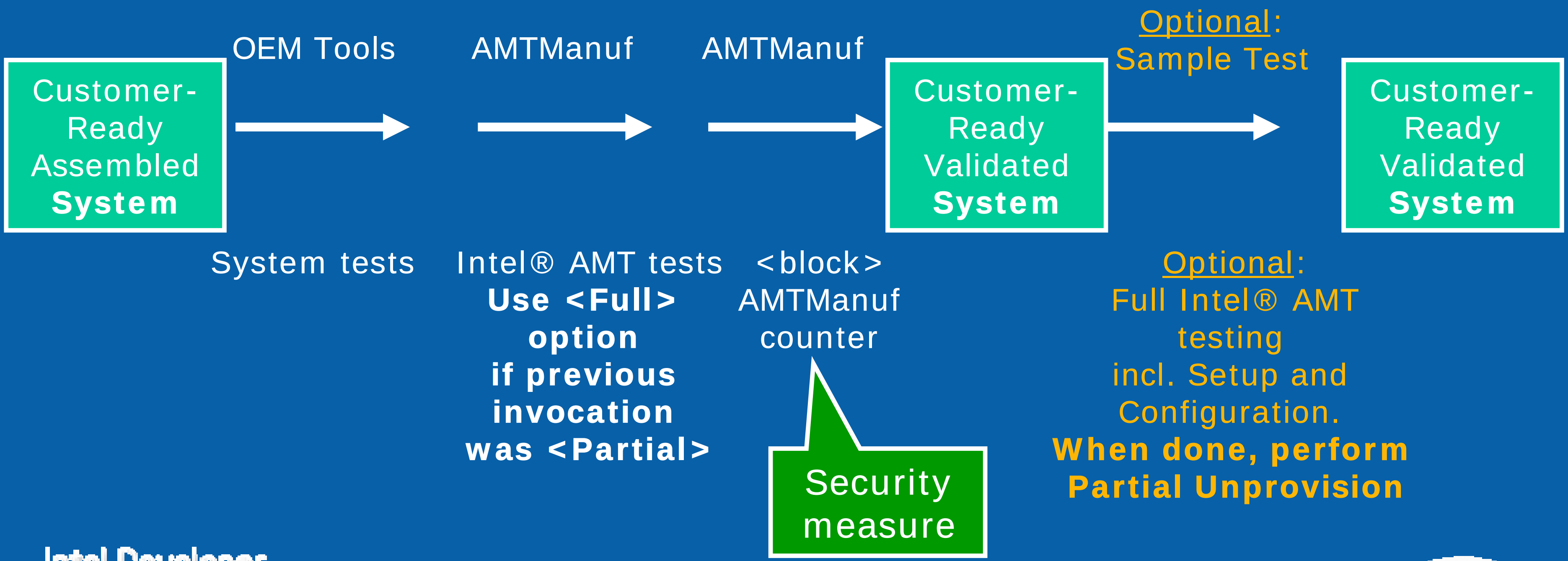
Optional
Intel® AMT TLS-PSK:
PID, PPS, PWD

Security measure to block Host access to Flash

Validation



OEM-Specific Image Creation → Board Assembly (Blank Flash) → Program Flash (on board) → System Assembly



Customer-Ready Assembled **System**

OEM Tools → System tests

AMTManuf → Intel® AMT tests **Use <Full> option if previous invocation was <Partial>**

AMTManuf → <block> AMTManuf counter

Security measure

Customer-Ready Validated **System**

Optional: Sample Test → Optional: Full Intel® AMT testing incl. Setup and Configuration. **When done, perform Partial Unprovision**

Customer-Ready Validated **System**

(Optional) Sample Test Flow

- Start Tests:
  - WebGUI
  - AMTFeaturesLocal and AMTFeaturesRemote
  - AMTCB, AMTRedirection
- Partial Unprovision in order to return machine to exact previous state (keeping the same PSK information)
- Sample test completed

- Note:
  - If test fails and machine is repaired, note that image should be reprogrammed with new counter in order to run AMTManuf again:
    - Override protection (OEM-dependent)
    - Reprogram Flash image (possibly using MEFlashProgram), resetting AMTManuf counter
    - Run AMTManuf
    - Run Sample Test again