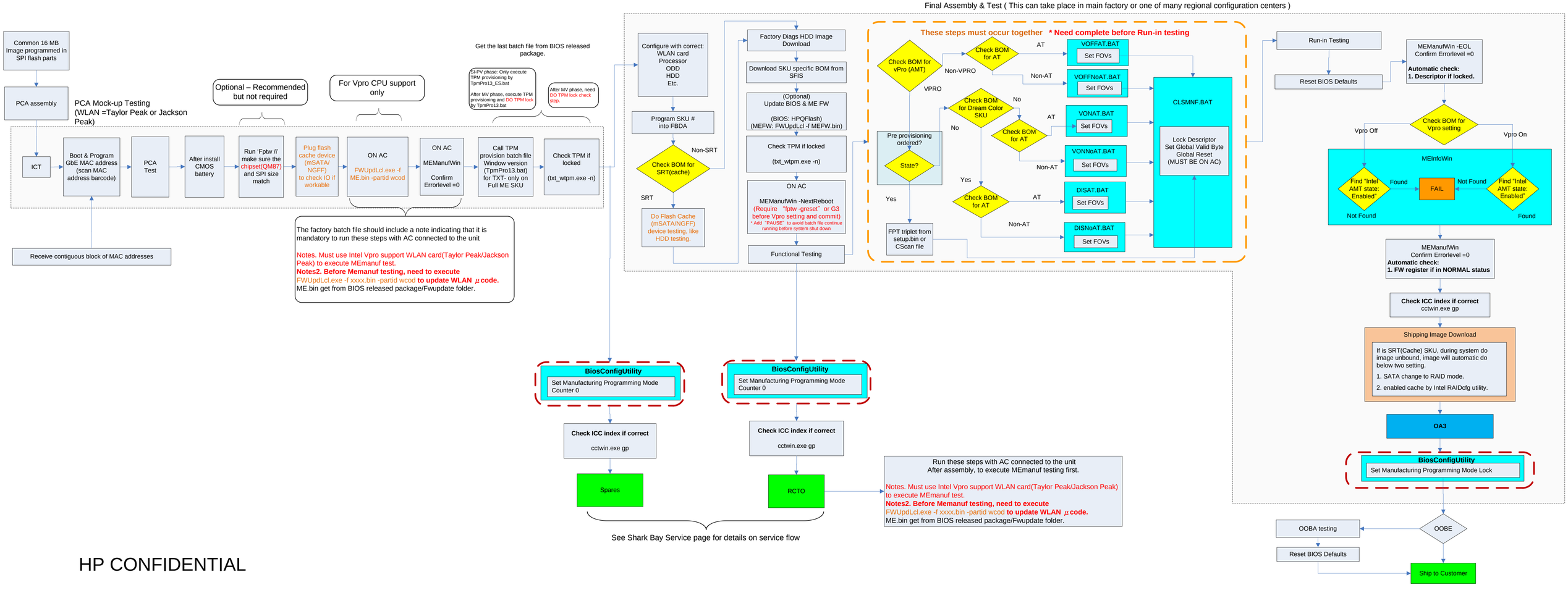
Revision History

Revision Number	Changes Made	Release Date	Author
1.0	• Initial version for Shark Bay platform.	10/16/2012	Doris Chi
1.1	• Correct MEmanufWin M3 autotest testing steps. • Remove ME power policy 1 and power policy 2 S3/S4/restart testing (Intel removes ME FOV command to do the setting.) • Adding ULT platform slide.	10/22/2012	Doris Chi
1.2	• Highlight SV (2-chips platform) and ULT (one-chip platform) as red in page title to notice.	11/01/2012	Doris Chi
1.3	• Remove Puma Peak as WLAN support list from Shark Bay SV list. • Remove WLAN micro code update command from SMT phase.	11/19/2012	Doris Chi
1.4	• Add PCH platform information.	12/12/2012	Doris Chi
1.5	• Add Vpro setting for dream color SKU	1/22/2013	Doris Chi
1.6	• Add Service and Board shop process.	3/19/2013	Doris Chi
1.7	• Update Service and Board Shop process.	6/10/2013	Doris Chi
1.8	• Update TPM provisioning process and MEmanuf test steps.	06/24/2013	Doris Chi
1.9	• Add TPM locked steps on Entry ME platform.	08/27	Doris Chi

Page 1 – Initial Manufacturing – Shark Bay **SV** 16MB Full ME(QM87) BIOS
Document Last Updated – 6/24/2013

HP CONFIDENTIAL

For ME un-commit procedure, refer to **Shark Bay SV ME Un-commit Process** tab

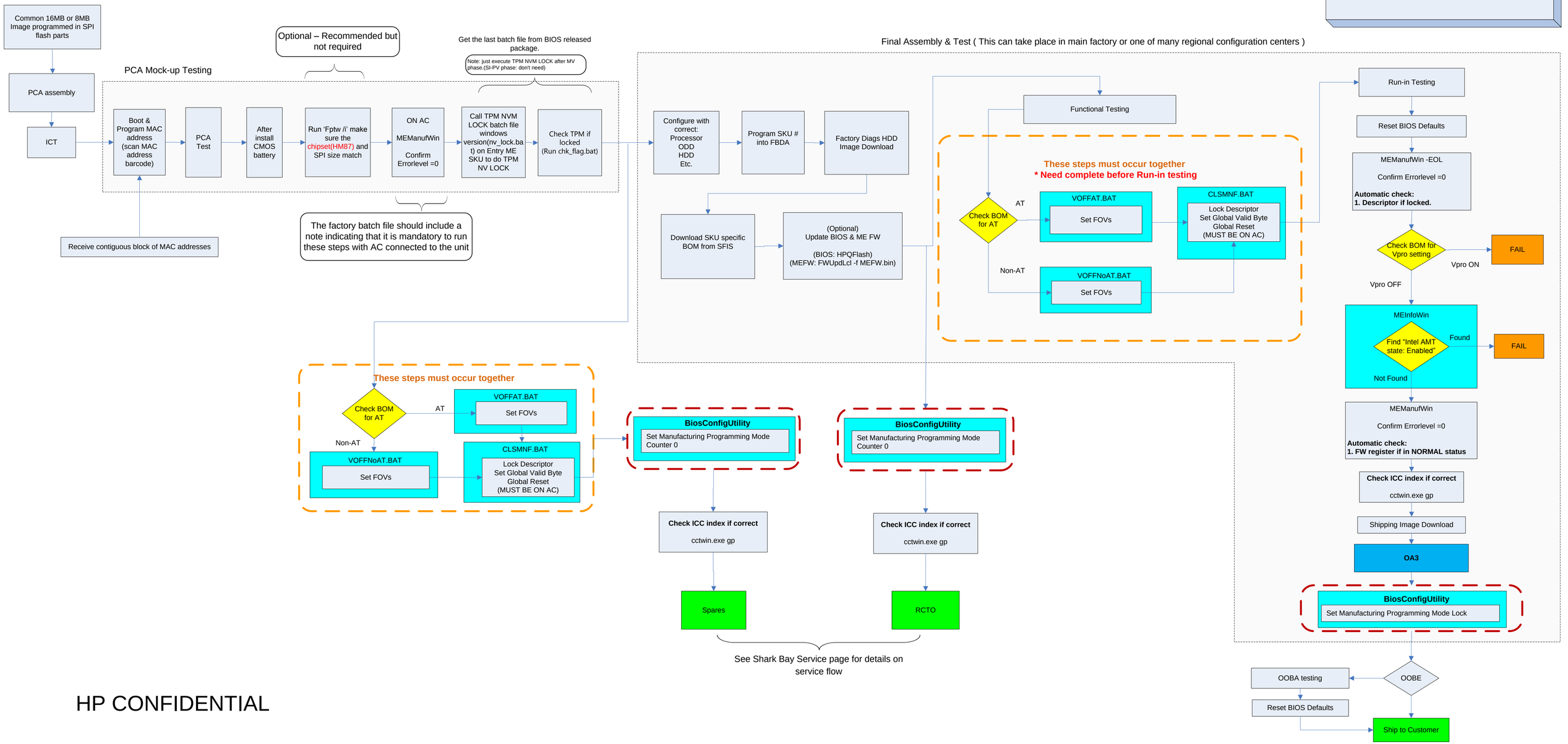


HP CONFIDENTIAL

Page 2 – Initial Manufacturing – Shark Bay **SV** Entry ME 16MB(HM87) and 8MB(HM87) BIOS
Document Last Updated – 08/27/2013

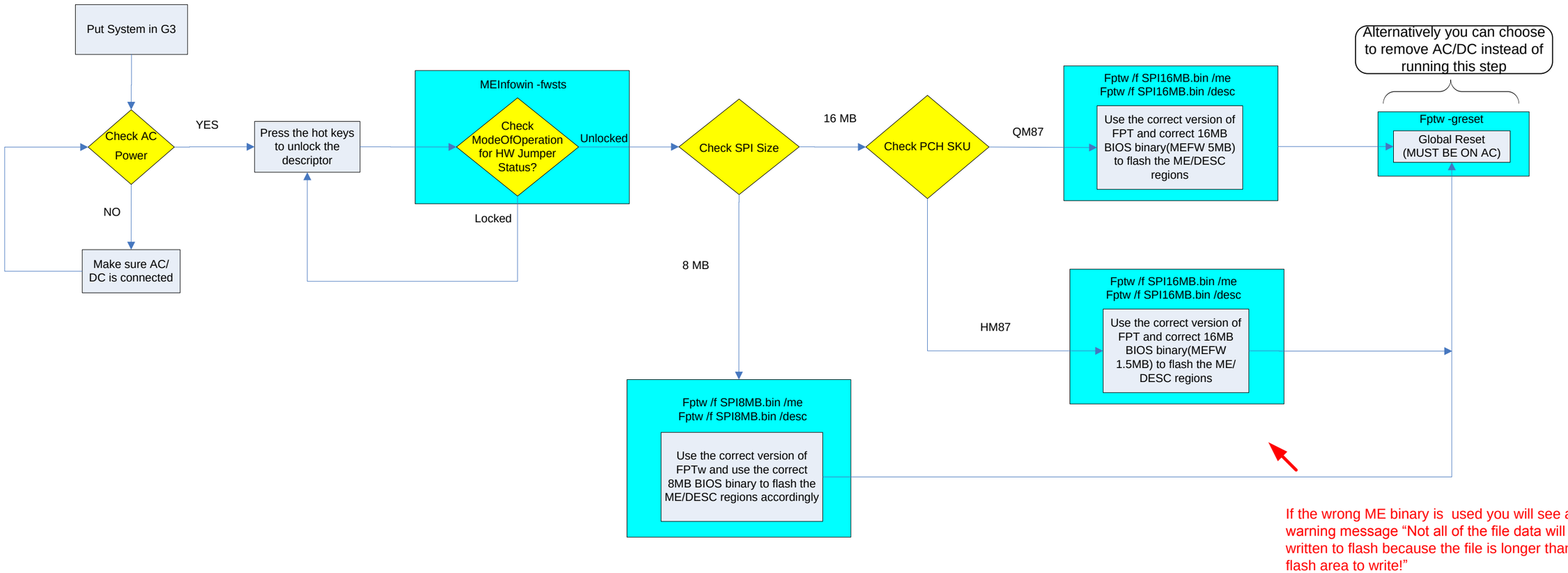
HP CONFIDENTIAL

For ME un-commit procedure, refer to **Shark Bay SV ME Un-commit Process** tab



HP CONFIDENTIAL

16/8 MB SPI_BIOS



If the wrong ME binary is used you will see a warning message “Not all of the file data will be written to flash because the file is longer than the flash area to write!”

HP CONFIDENTIAL

Configure Vpro from HPMEBrand13 folder

Need to Configure PCA

Check BOM for AMT On or Off

HPMEBrand13.efi

Choose brand (vPro ON/ vPro OFF), Commit config & Lock Descriptor

Global Reset (MUST BE ON AC)

HPMEBrand13.efi -vc

Confirm ME state is Normal.

Confirm Descriptor Locked

Passes Functional Tests

Hardware Rework Required

Board Shop

Yes

All tests pass?

No

Migrate any FBDA defaults from OLD PCA

Replace PCA

Spares

This step only used as a last resort on the customers original PCA!!!

======NOTICE======
Please use SMC tool to set MPM unclock before go through uncommit process.

Uncommit process from UNC13_9.0 folder
(SPI image get from each platform BIOS release package)

Uncommit.nsh SPI.bin
(Clear iAMT FDBA var)
(Reset Desc - enable ME & reset access restrictions)

Fpt.efi /f SPI.bin /ME
(Flash ME region)
Fpt.efi /f SPI.bin /DESC
(Flash Descriptor region)

RUN ON AC

Global Reset
Fpt.efi /greset

MEManuf.efi
Confirm Errorlevel =0

With AC and Battery connected to the unit

Global reset may also be accomplished by removing AC & Main battery.

Override Jumper
BOOT with Override Flash Protection key sequence (Hot Keys)

Intel Anti-Theft Enrolled/Stolen?

ME subsystem OK?

Board OK?

Needs ME Firmware Update?

Flash ME FW using Intel end user update tool FWUpdLcl

Needs BIOS Update?

Flash BIOS using HP tool HPQFLASH

Emergency Recovery Boot?

PCA Boots?

Service Event –
Start Here

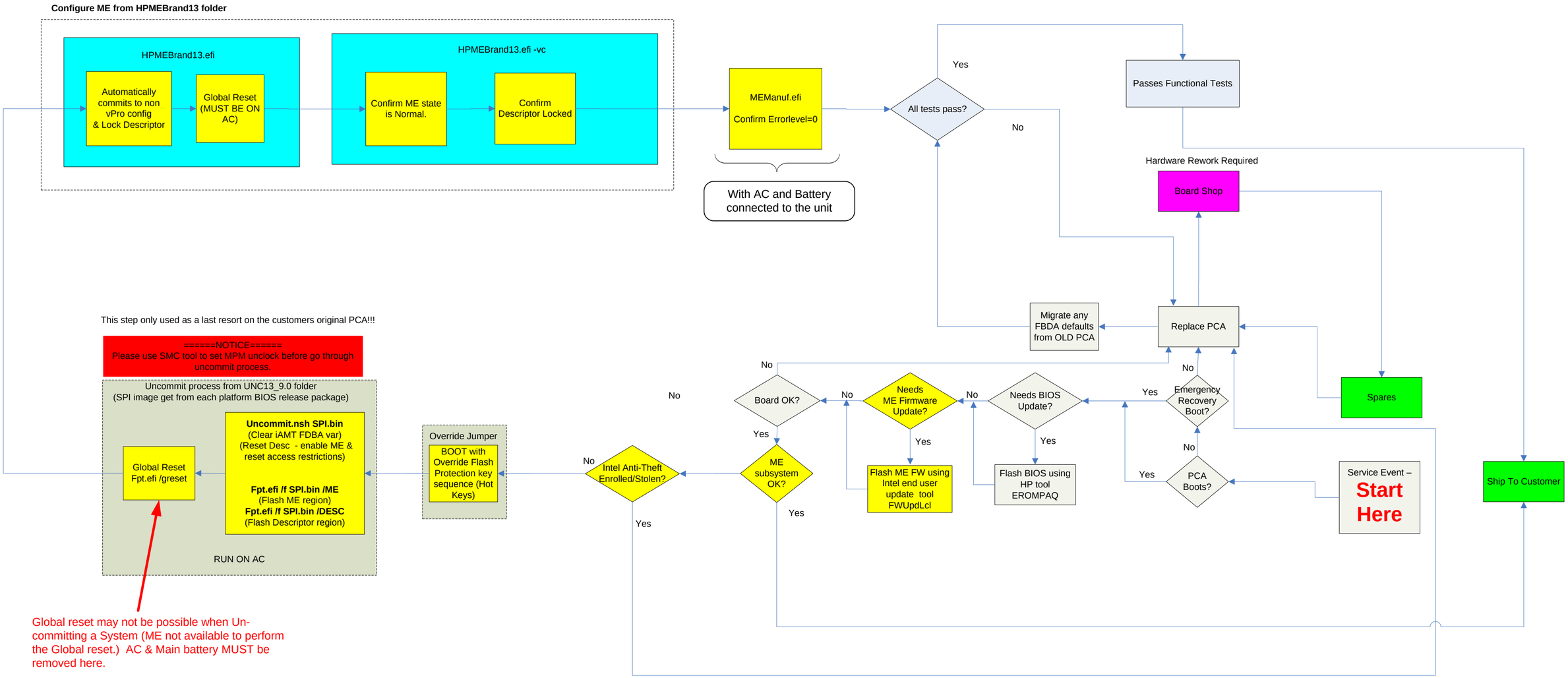
Ship To Customer

Replace Board

Any time during the service event, if an Intel Anti-Theft enrolled unit moves to a 'Stolen' State (been blocked by recovery screen at boot), replace the board

HP CONFIDENTIAL

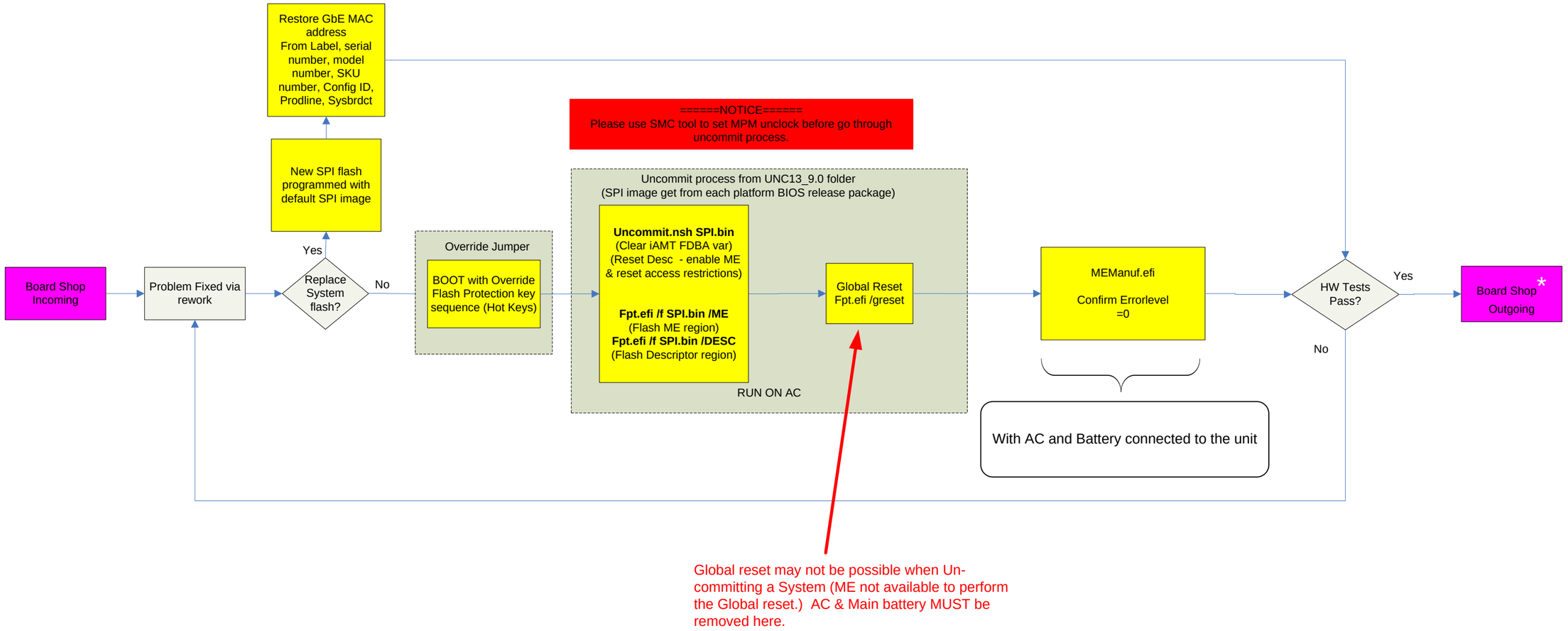
HP CONFIDENTIAL



Any time during the service event, if an Intel Anti-Theft enrolled unit moves to a 'Stolen' State (been blocked by recovery screen at boot), replace the board

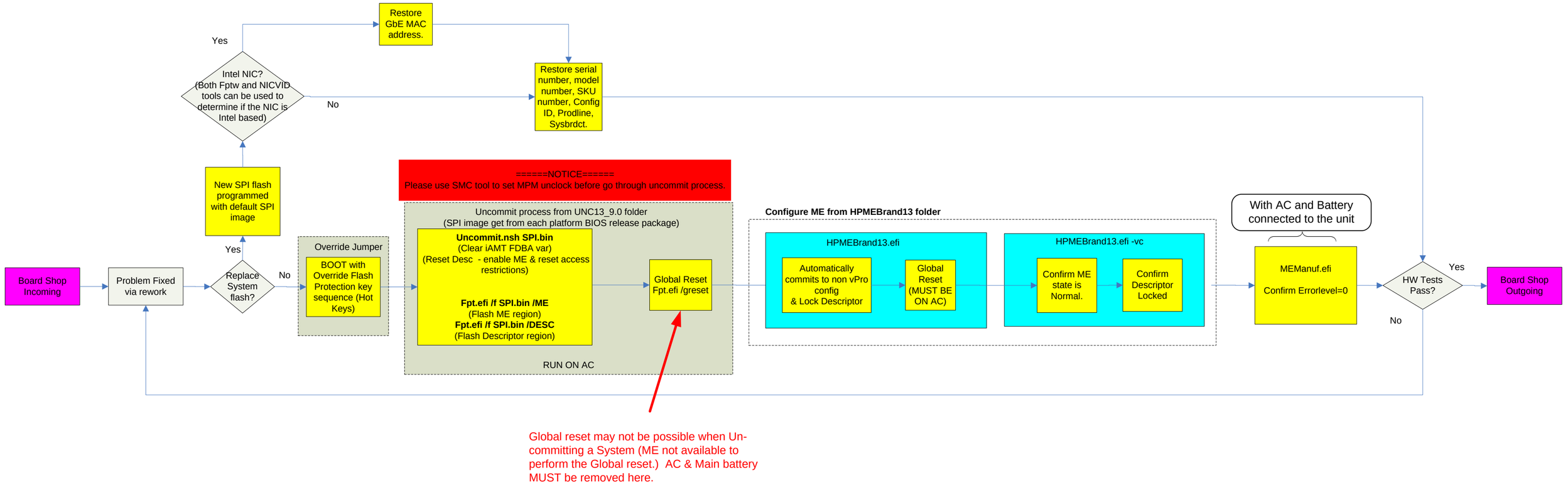
HP CONFIDENTIAL

HP CONFIDENTIAL



* - Since the board is not committed yet, the descriptor is not locked.

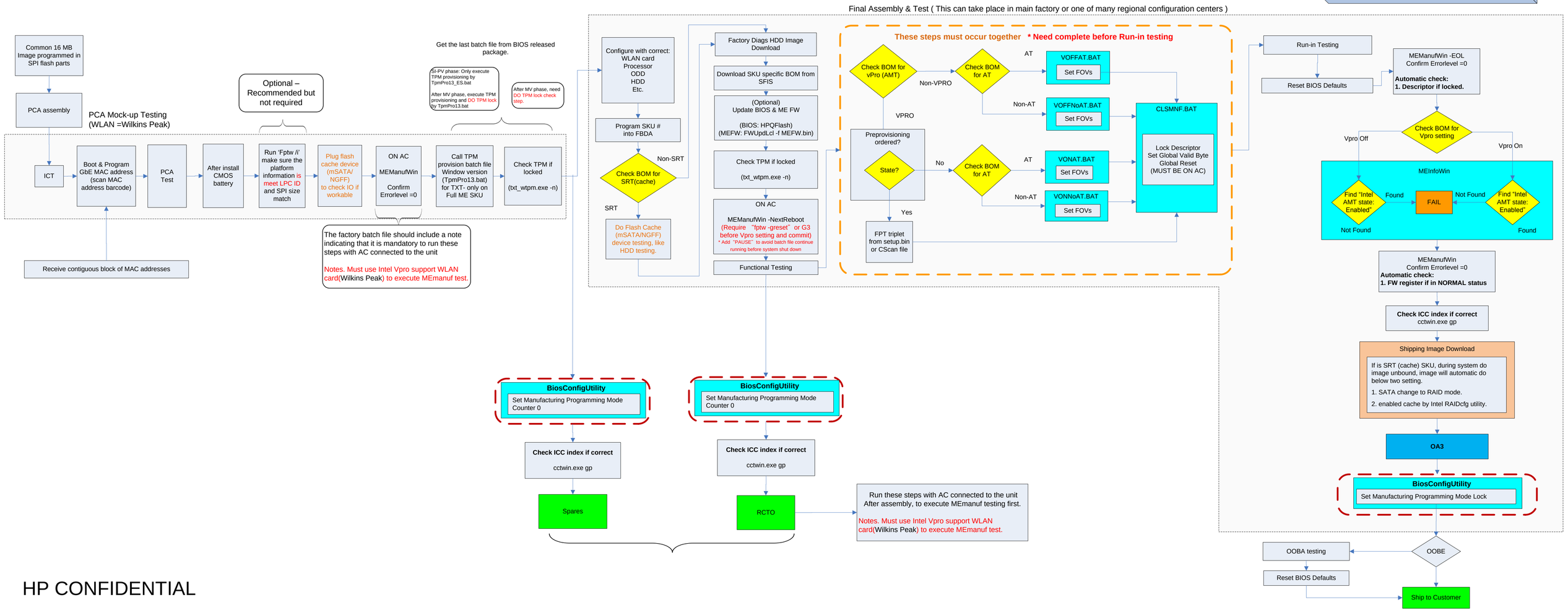
HP CONFIDENTIAL


Board Shop Incoming
Problem Fixed via rework
Replace System flash?
Yes
No
New SPI flash programmed with default SPI image
Intel NIC? (Both Fptw and NICVID tools can be used to determine if the NIC is Intel based)
Yes
No
Restore GbE MAC address.
Restore serial number, model number, SKU number, Config ID, Prodline, Sysbrdct.
Override Jumper
BOOT with Override Flash Protection key sequence (Hot Keys)
======NOTICE======
Please use SMC tool to set MPM unclock before go through uncommit process.
Uncommit process from UNC13_9.0 folder
(SPI image get from each platform BIOS release package)
Uncommit.nsh SPI.bin
(Clear iAMT FDBA var)
(Reset Desc - enable ME & reset access restrictions)
Fpt.efi /f SPI.bin /ME
(Flash ME region)
Fpt.efi /f SPI.bin /DESC
(Flash Descriptor region)
RUN ON AC
Global Reset Fpt.efi /greset
Configure ME from HPMEBrand13 folder
HPMEBrand13.efi
Automatically commits to non vPro config & Lock Descriptor
Global Reset (MUST BE ON AC)
HPMEBrand13.efi -vc
Confirm ME state is Normal.
Confirm Descriptor Locked
With AC and Battery connected to the unit
MEManuf.efi
Confirm Errorlevel=0
HW Tests Pass?
Yes
No
Board Shop Outgoing
Global reset may not be possible when Un-committing a System (ME not available to perform the Global reset.) AC & Main battery MUST be removed here.

Page 8 – Initial Manufacturing – Shark Bay **ULT** 16MB Full ME (Premium) BIOS

Document Last Updated – 06/24/2013

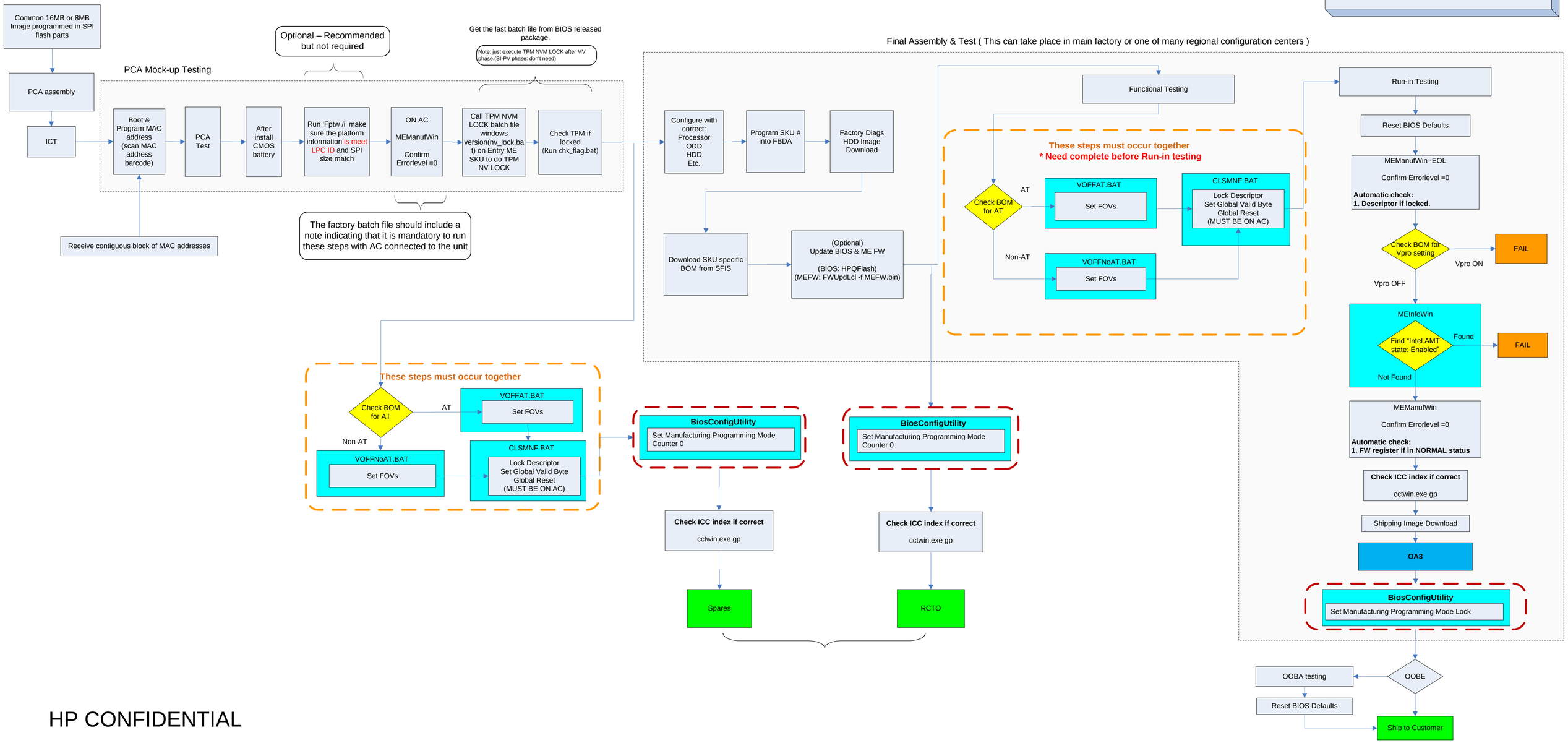
For ME un-commit procedure, refer to **Shark Bay ME ULT Un-commit Process** tab



Page 9 – Initial Manufacturing – Shark Bay **ULT** 8MB Entry ME (Mainstream) BIOS
Document Last Updated – 08/27/2013

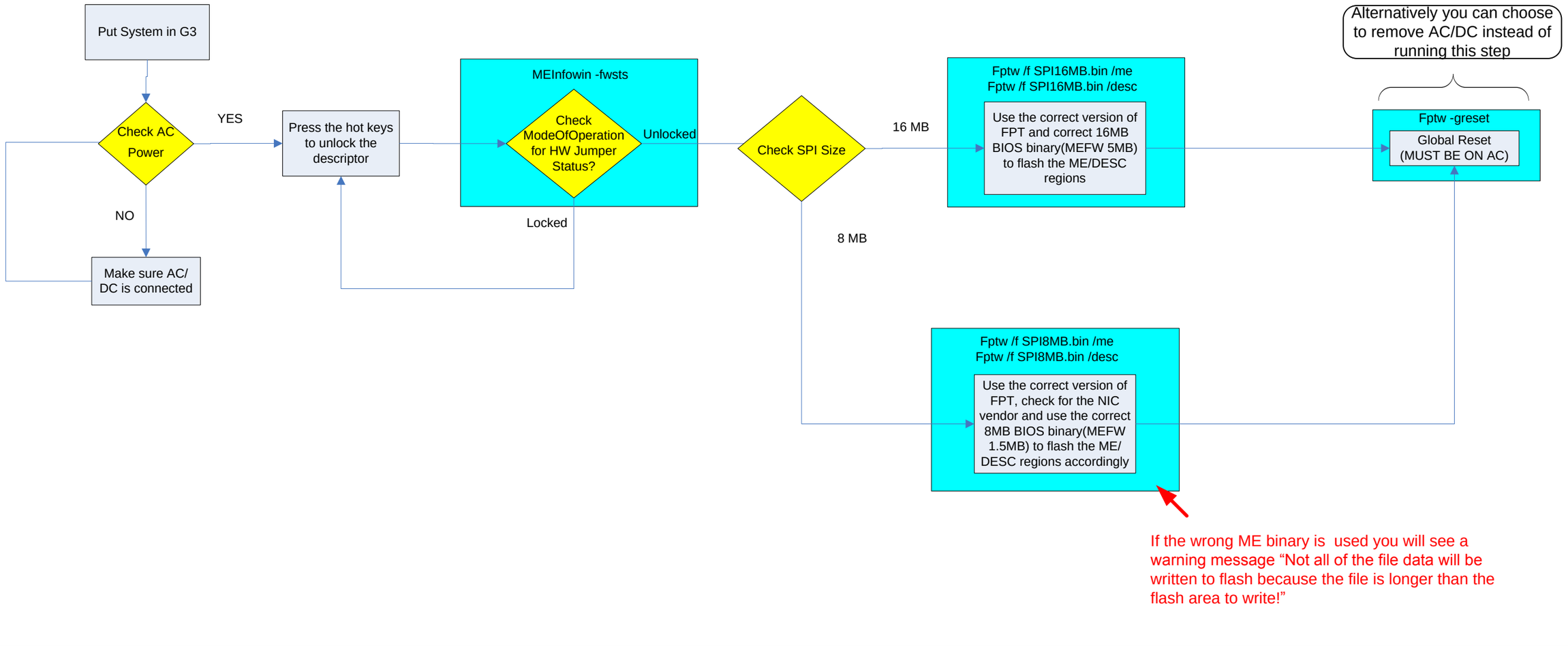
HP CONFIDENTIAL

For ME un-commit procedure, refer to **Shark Bay ULT ME Un-commit Process** tab

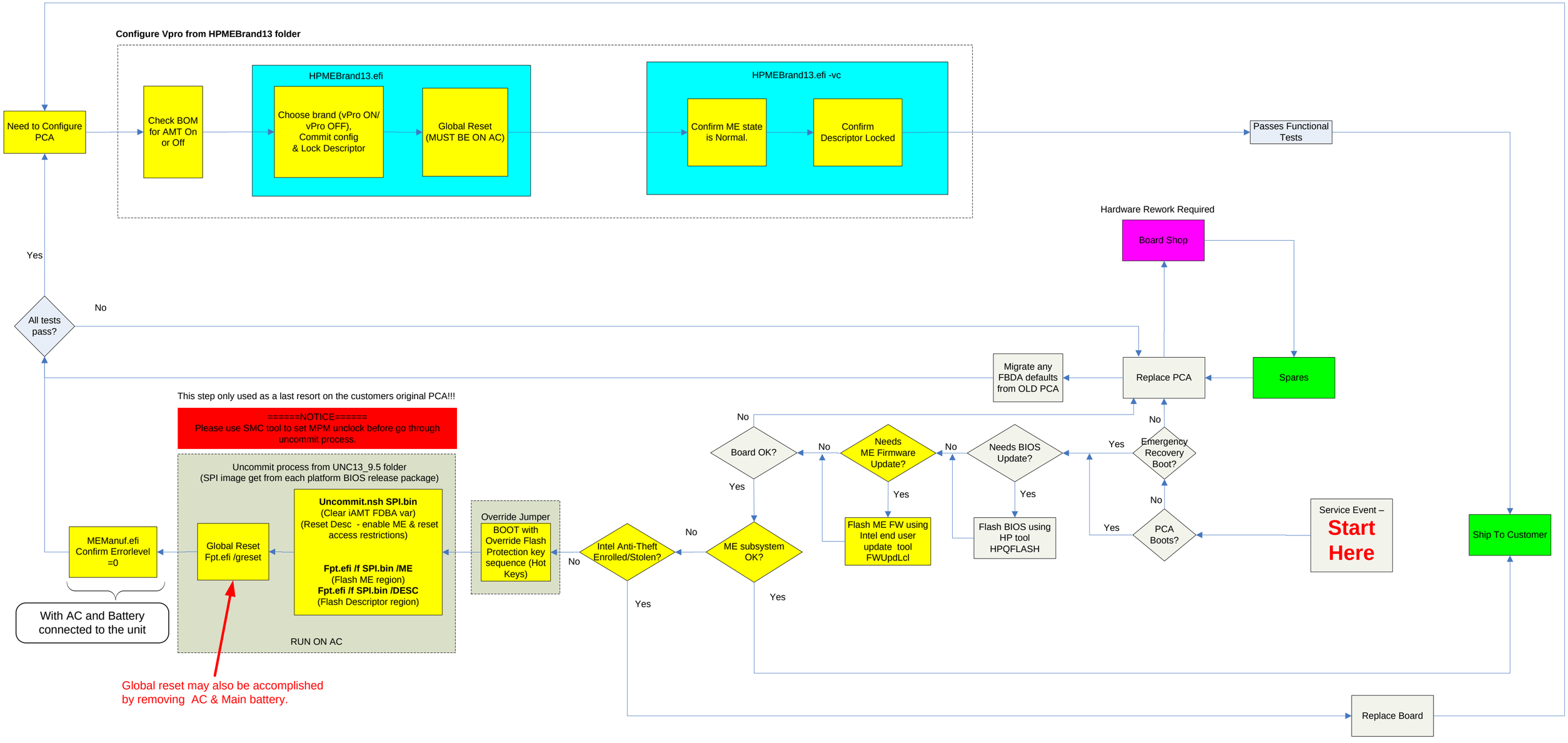


HP CONFIDENTIAL

16/8 MB SPI_BIOS



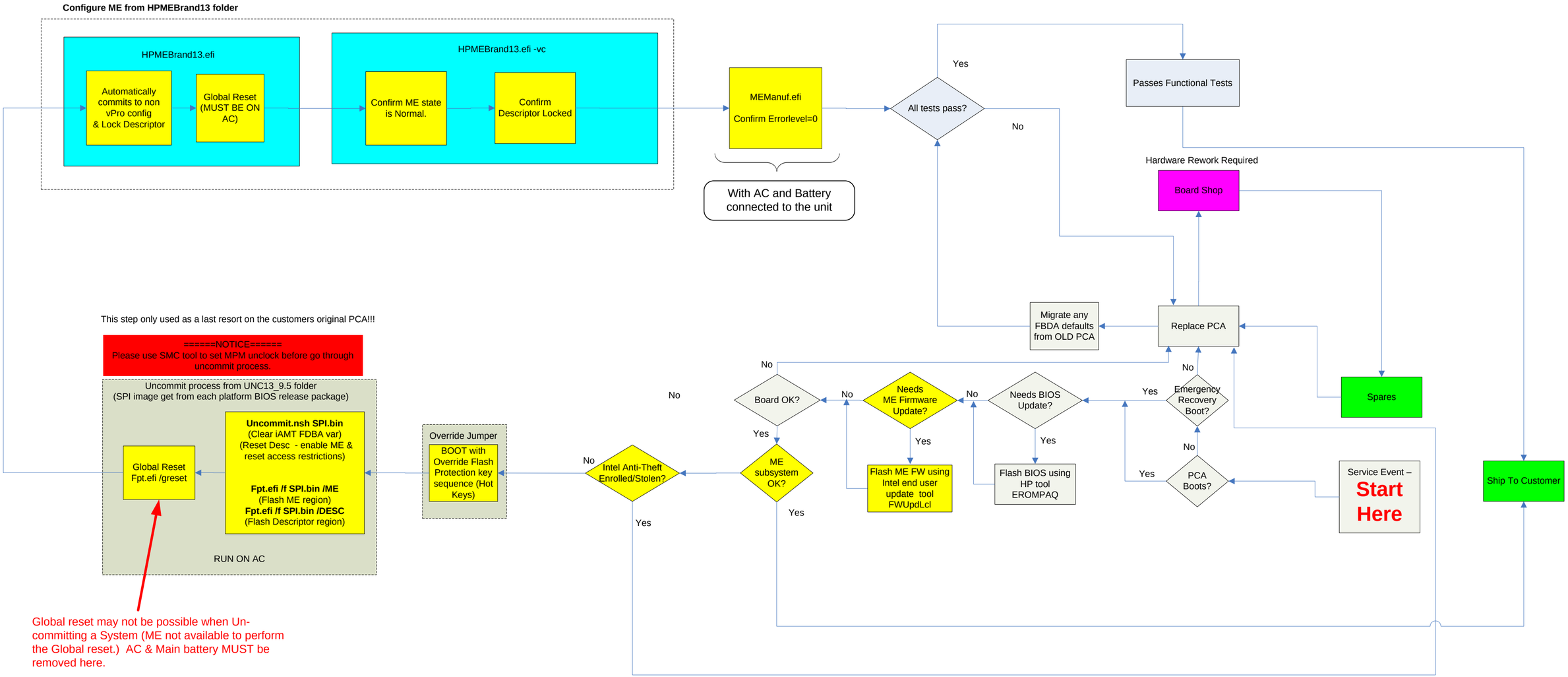
HP CONFIDENTIAL



HP CONFIDENTIAL

Any time during the service event, if an Intel Anti-Theft enrolled unit moves to a 'Stolen' State (been blocked by recovery screen at boot), replace the board

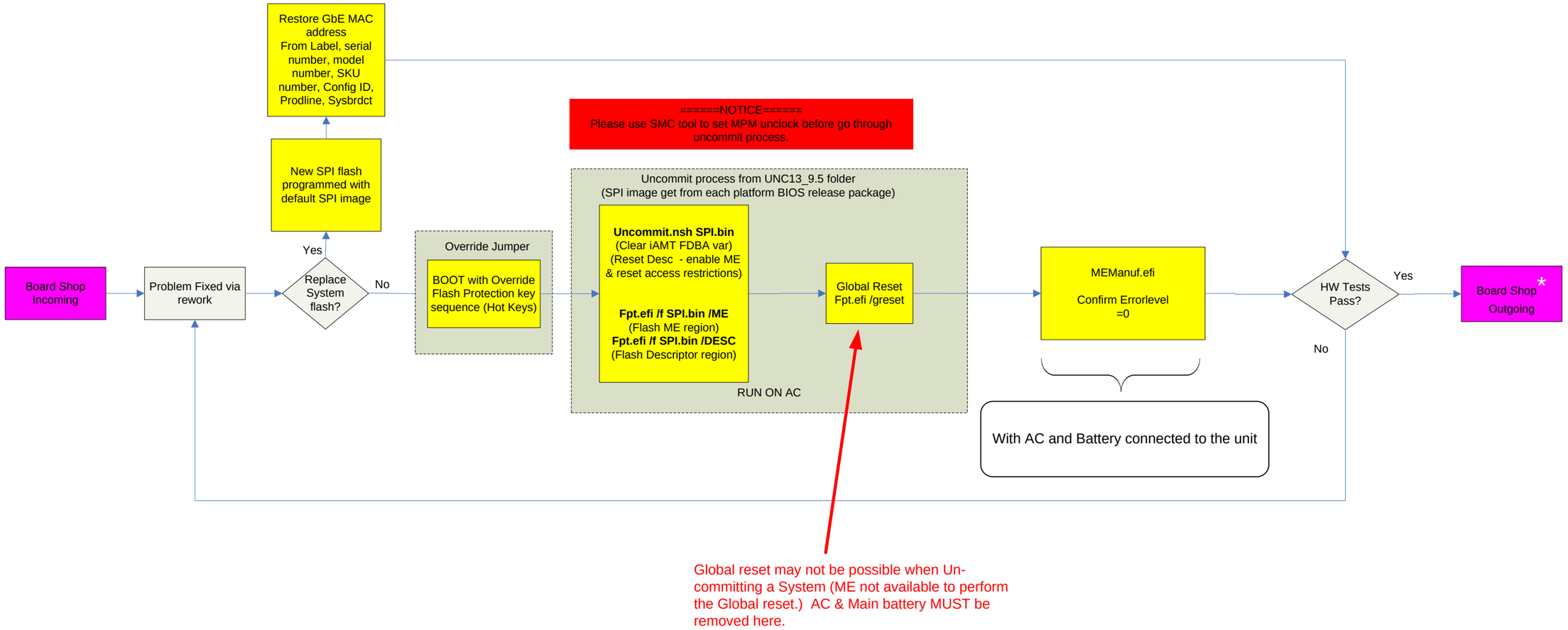
HP CONFIDENTIAL



HP CONFIDENTIAL

Any time during the service event, if an Intel Anti-Theft enrolled unit moves to a 'Stolen' State (been blocked by recovery screen at boot), replace the board

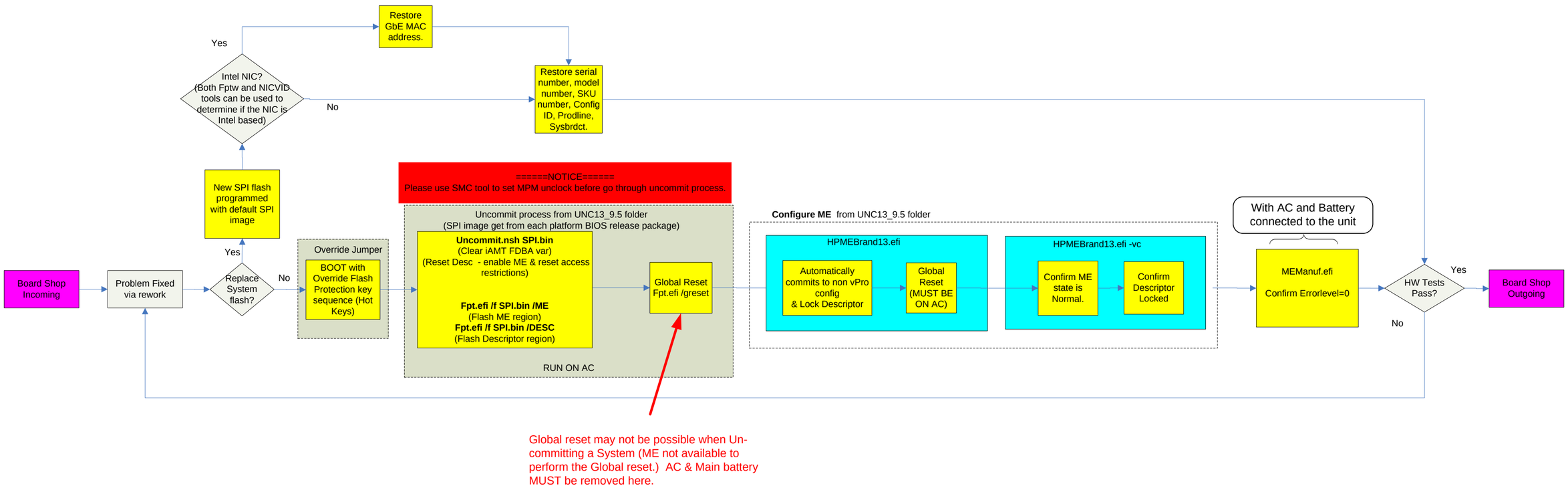
HP CONFIDENTIAL



* - Since the board is not committed yet, the descriptor is not locked.

HP CONFIDENTIAL

HP CONFIDENTIAL



HP CONFIDENTIAL