December 2022

SYSTEM AMD DOCK DEVICE MUTUAL LOCK

HP INC

System and Dock Device Mutual Lock

Abstract:

Peripherals is getting to use in our PC system day by day. Even now Industry usually supplies many strong software/hardware protections in person systems, but related security methodology seem doesn't grow as well. This is a new idea which leverage system power control method to peripheral which specific to docking device. Providing system/docking mutual secure lock. There're 4 major features we provide. Register specific ID in BIOS firmware for target system and Docking devices then authorized person can lock/unlock system or docking device from firmware level. Cover not only PC but also extend protection to stay alone docking devices.

Design Construction:

- BIOS/EC/PD: EC will record the specific ID (GUID) and communicate with PD (power deliver) in Docking devices and BIOS. BIOS will be in charge of UI. PD will lock/unlock docking power depends on GUID match.

Here is detail function we can implement,

Function 1: Register specific ID (GUID) in BIOS UI (F10 setup menu) for target system and docking device.

End user can enter BIOS setup menu to enable feature. At the same time, BIOS will generate specific GUID into BIOS/EC/Docking PD firmware to usage.

Function 2: Docking Device Lock

Once register GUID and Save/Exit BIOS menu, (Function1)

1. System BIOS will forward Docking GUID to Docking PD FW (Power Delivery) via System EC (Embedded control).
2. System BIOS will forward System GUID to System EC.

Once System reboot with feature enable,

1. Docking PD Firmware will compare System GUID with Docking GUID, If it doesn't match. PD will disconnect docking power.
2. If it matches. Resume docking connect power. System can detect and use docking device as usual.

Function 3: System lock from docking.

Once register GUID and Save/Exit BIOS menu,

1. System BIOS will forward Docking GUID to Docking PD FW (Power Delivery) via System EC (Embedded control).
2. System BIOS will forward System GUID to System EC.

Once System reboot with feature enable,

1. System EC firmware will compare System GUID with Docking GUID, If it doesn't match. EC will disconnect system power.
2. If it matches. Resume System power. System can boot as usual.

Function 4: System and Docking Mutual Lock

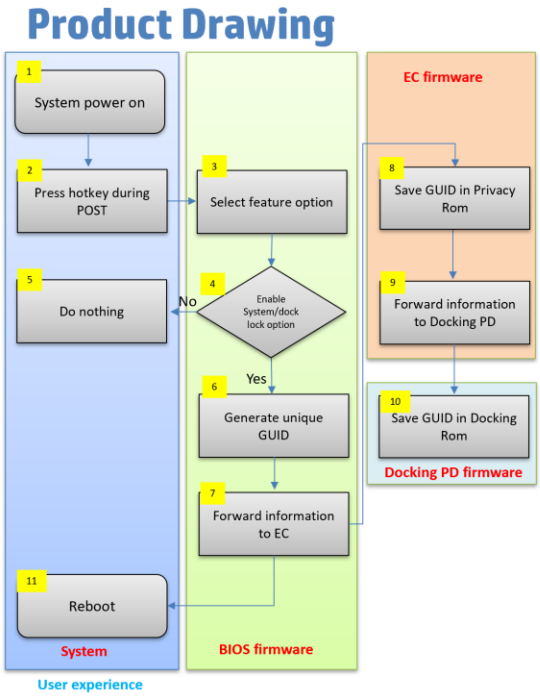
Once register GUID and Save/Exit BIOS menu, (Function1)

1. System BIOS will forward Docking GUID to Docking PD FW (Power Delivery) via System EC (Embedded control).
2. System BIOS will forward System GUID to System EC.

Once System reboot with feature enable,

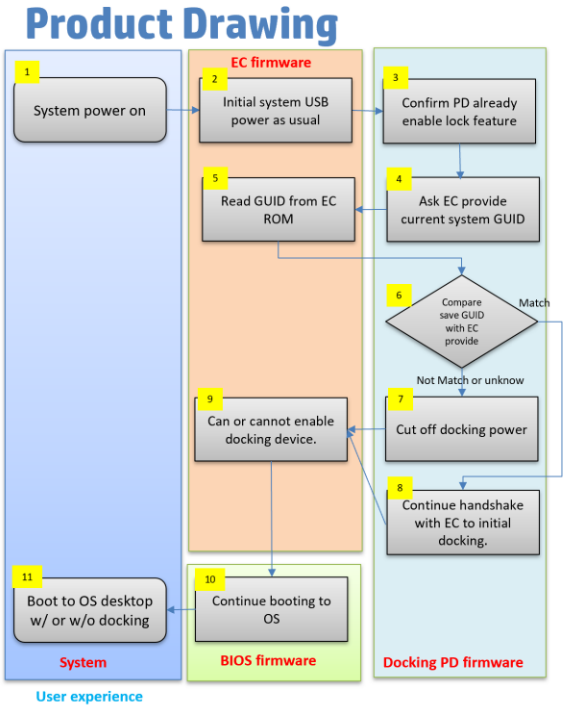
1. System EC firmware will compare System GUID with Docking GUID, If it doesn't match. EC will disconnect system power. Docking PD Firmware will compare System GUID with Docking GUID, if it doesn't match. PD will disconnect docking power.
2. If it matches. Resume System and docking power. System and docking device can work as usual.

< Flow Chart and Block Flow Diagram >



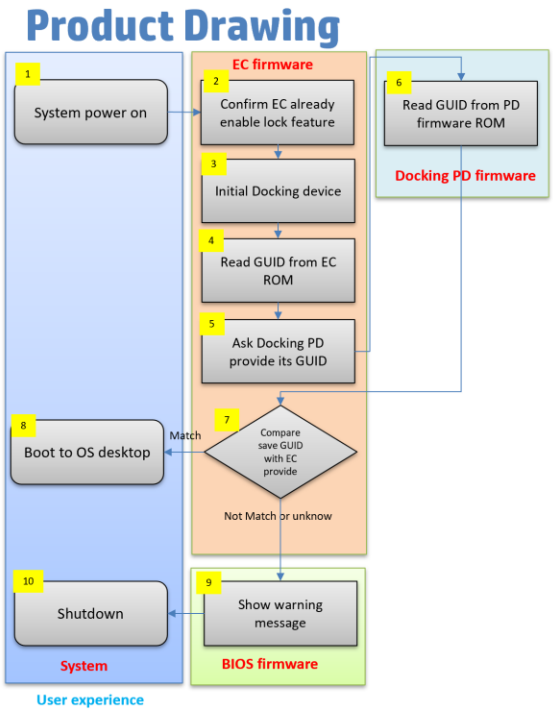
Function 1: Register specific ID (GUID) in BIOS UI (F10 setup menu) for target system and docking device.

Step1: System : Power on.
Step2: System : Press hotkey (F10) during POST.
Step3: BIOS : End user can enable lock feature in BIOS setup menu.
Step4: BIOS : BIOS detect feature enable or disable.
Step5: BIOS : In No case , Do nothing.
Step6: BIOS : In Yes case, BIOS generate unique GUID.
Step7: BIOS : Forward GUID to EC via ECRAM.
Step8: EC : Save GUID in EC Privacy Rom.
Step9: EC: Forward GUID to Docking PD via USB command.
Step10: PD : Save GUID in Docking rom.
Step11: System : System reboot after all process completed.



Function 2: Docking device lock from system.

Step1: System : Power on system.
Step2: EC : Initial system USB power.
Step3: Docking PD : Confirm docking lock feature is enabled.
Step4: Docking PD : Try to ask EC provide current system GUID.
Step5: EC : Read GUID from EC private Rom and provide to PD.
Step6: Docking PD: Compare GUID saved in PD with EC provided.
Step7: Docking PD : In Not Match case, Cut off docking power.
Step8: Docking PD : In Match case, continue docking device initial process.
Step9: EC : Will enable docking device successfully for fail.
Step10: BIOS: Continue booting to OS.
Step11: System : Result: Boot to OS desktop w/ or w/o docking



Function3: System Lock from docking.

Step1: System : Power on system.
Step2: EC : Confirm system lock by docking feature enable.
Step3: EC : Start to initial docking device.
Step4: EC : Read GUID from rom.
Step5: EC : Ask docking PD provide its GUID.
Step6: Docking PD: Read GUID from PD firmware and provide to EC.
Step7: EC: Compare 2 GUID to see match or not.
Step8: EC: In Match case, continue to boot.
Step9: BIOS : In Not Match case, BIOS will receive EC Q event and show warning message in EFI phase.
Step10: System : Result: Shutdown system in couple minutes.

Function4: System and Docking Mutual Lock

/* All step go through as Function2 + Function3. */

Business Strategy/Advantages

1. Provide a new method to secure system or docking device which may be used by unauthorized people. For example, once some people lost his/her system or docking. This feature can ensure system or docking would not be accessed. Data of system is secure and un-workable docking also useless for unauthorized people.

2. It's extendable feature that not only 1 on 1 pair but multi pair. (1 system lock different docking devices or 1 docking lock different systems)

3. No Hardware requirement. Only software and firmware efforts. Easy to implement in current system and docking.

Disclosed by **Pan Ian, Cassie Yin, Yvonne Yang, HP Inc.**