February 2023

HOOD SENSOR MECHANISM ENHANCEMENT

HP INC

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Hood Sensor Mechanism Enhancement

Abstract

- The Hood Sensor is designed to notify the user of any removal of the computer cover.
- There's a potential security risk on the Z2 G9 Mini hood sensor design. Hackers can cut the hood sensor cable without removing the computer cover to break the hood sensor security protection mechanism.
- The disclosure enhances the hood sensor protection mechanism through hardware design or software solutions.

Problems Solved

- To enhance the hood sensor protection mechanism through hardware design or software solutions.

Concept

- The disclosure enhances protection mechanism in the two situations. The first one is the normal operation (removing computer cover ➡ removing cable), and the other is the abnormal operation (removing cable ➡ removing computer cover).
- The enhancement of hardware design, which controls the INTRUDER signal by hardware logical circuit according to the cable connection status.
- The enhancement of software solution, which sets up the cable detect HOOD_SW_DET# signal as an interrupt signal to monitor if the cable has been removed.

Current Mechanism

- **Hardware mechanism (Fig. 1)**
    - When the hood sensor cable is connected to the motherboard, HOOD_SW_DET# will be asserted to low and notify BIOS that the hood sensor module is existing by PCH GPIO during the system is booting.
    - When the computer cover is closed, the hood sensor button will be pressed (the internal switch will open), and SIO_INTRUDER# will be asserted to high and notify SIO that the computer cover is closed.
    - When the computer cover is opened, the hood sensor button will be released (the internal switch will close), and SIO_INTRUDER# will be asserted to low and notify SIO that the computer cover is opened.
- **Software mechanism (Flow chart 1 & 2)**
    - BIOS will detect the voltage level of HOOD_SW_DET# by PCH only during the system is booting.
    - SIO will detect the voltage level of SIO_INTRUDER# changing and record in the register.
    - If system security protection has been enabled by users, when BIOS detects that the hood sensor cable is disconnected during the system is booting, security protection will be triggered.
    - If system security protection has been enabled by users, when SIO detects that SIO_INTRUDER# voltage level change, security protection will be triggered.

Problems

- **Current mechanism under the risk (Fig. 2 / Flow chart 1 & 3 / Table 1)**
    - When the system protection has been enabled and the system has bootup(S0), if hackers remove the hood sensor cable from the motherboard without opening the computer cover, HOOD_SW_DET# will be de-asserted to high but BIOS cannot detect the cable has been removed because BIOS only detect the signal during the system is booting.
    - When the system protection has been enabled and the system has bootup(S0), if hackers remove the hood sensor cable from the motherboard and **then** open the computer cover, SIO_INTRUDER# will keep high (no voltage level change) and SIO will identify the computer cover is still closed because the hood sensor module has been removed with no function now.
    - Hackers can bypass the security protection mechanism and irrupt the system.

Enhanced Mechanism

- **Hardware mechanism (Fig. 3 / Flow chart 1 & 4 / Table 2)**
    - Add the circuit to control signal SIO_INTRUDER# through the P-MOS and N-MOS by cable detect signal HOOD_SW_DET#.
    - When the Button is pressed and the cable is connected, HOOD_SW_DET# will be low by motherboard GND, and the PMOS will be closed and NMOS will be opened, SIO_INTRUDER# will be high by the motherboard pull-up circuit.
    - When cable is disconnected by hackers without removing the computer cover, HOOD_SW_DET# will be high by motherboard pull-up circuit, and the PMOS will be opened and NMOS will be closed, SIO_INTRUDER# will be low by the motherboard GND.
- **Software mechanism (Flow chart 1 & 5)**
    - Set HOOD_SW_DET# as an interrupt signal, BIOS will detect if the signal is changing and recording in the register.
    - SIO will detect the voltage level of SIO_INTRUDER# changing and record in the register.
    - If system security protection has been enabled by users, when hackers remove the hood sensor cable from the motherboard without opening the computer cover, HOOD_SW_DET# will be de-asserted to high and notify BIOS that the hood sensor module is removed synchronously, security protection will be triggered.
    - If system security protection has been enabled by users, when BIOS detects that the hood sensor cable is disconnected during the system power-on, security protection will be triggered.
    - If system security protection has been enabled by users, when SIO detects that the computer cover is opened, security protection will be triggered.
    - If system security protection has been enabled by users, when SIO detects that SIO_INTRUDER# voltage level change, security protection will be triggered.
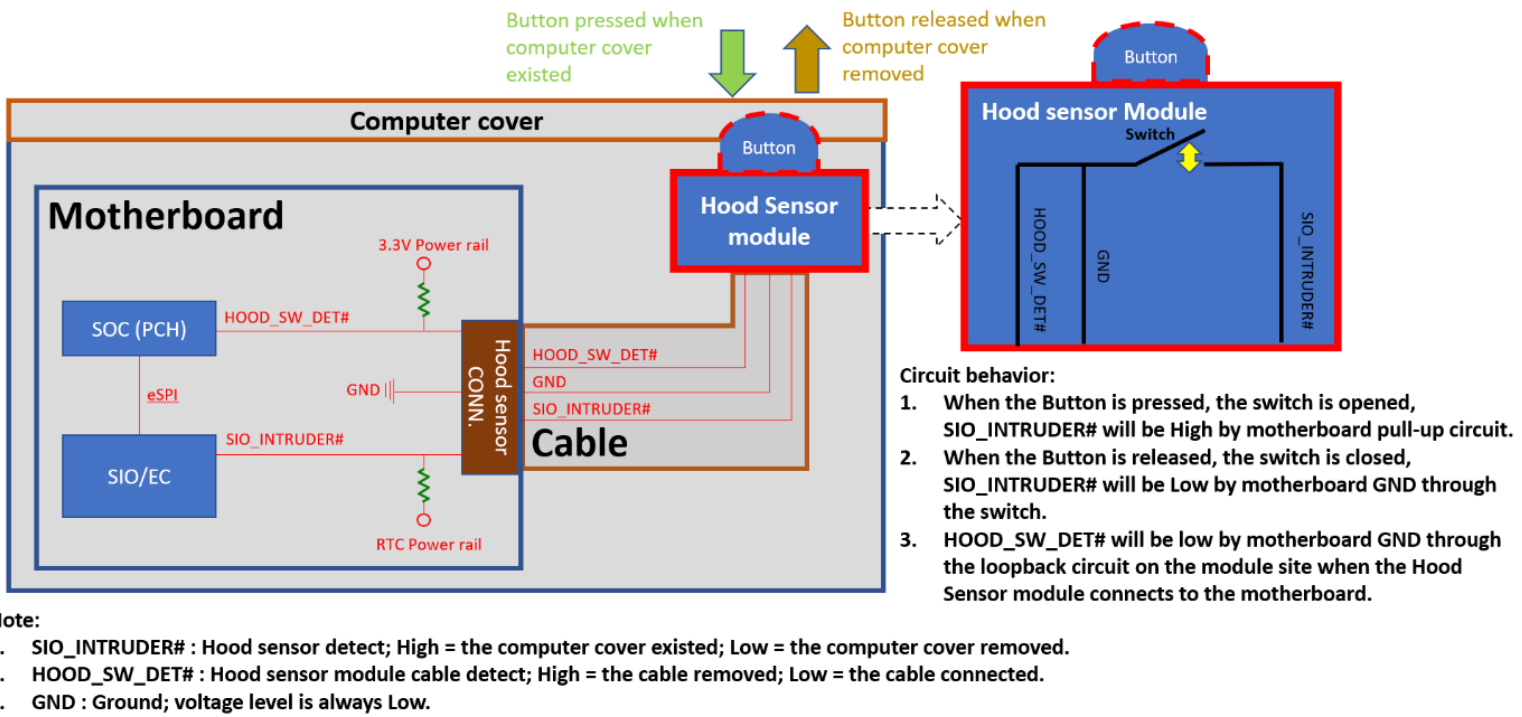
Figure list

Circuit behavior:
1. When the Button is pressed, the switch is opened, SIO_INTRUDER# will be High by motherboard pull-up circuit.
2. When the Button is released, the switch is closed, SIO_INTRUDER# will be Low by motherboard GND through the switch.
3. HOOD_SW_DET# will be low by motherboard GND through the loopback circuit on the module site when the Hood Sensor module connects to the motherboard.

Note:
1. SIO_INTRUDER# : Hood sensor detect; High = the computer cover existed; Low = the computer cover removed.
2. HOOD_SW_DET# : Hood sensor module cable detect; High = the cable removed; Low = the cable connected.
3. GND : Ground; voltage level is always Low.

Fig. 1 Current Hood Sensor Protection Mechanism

Hackers can use tweezers or needles to remove the cable from the computer chassis hole without opening the computer cover.
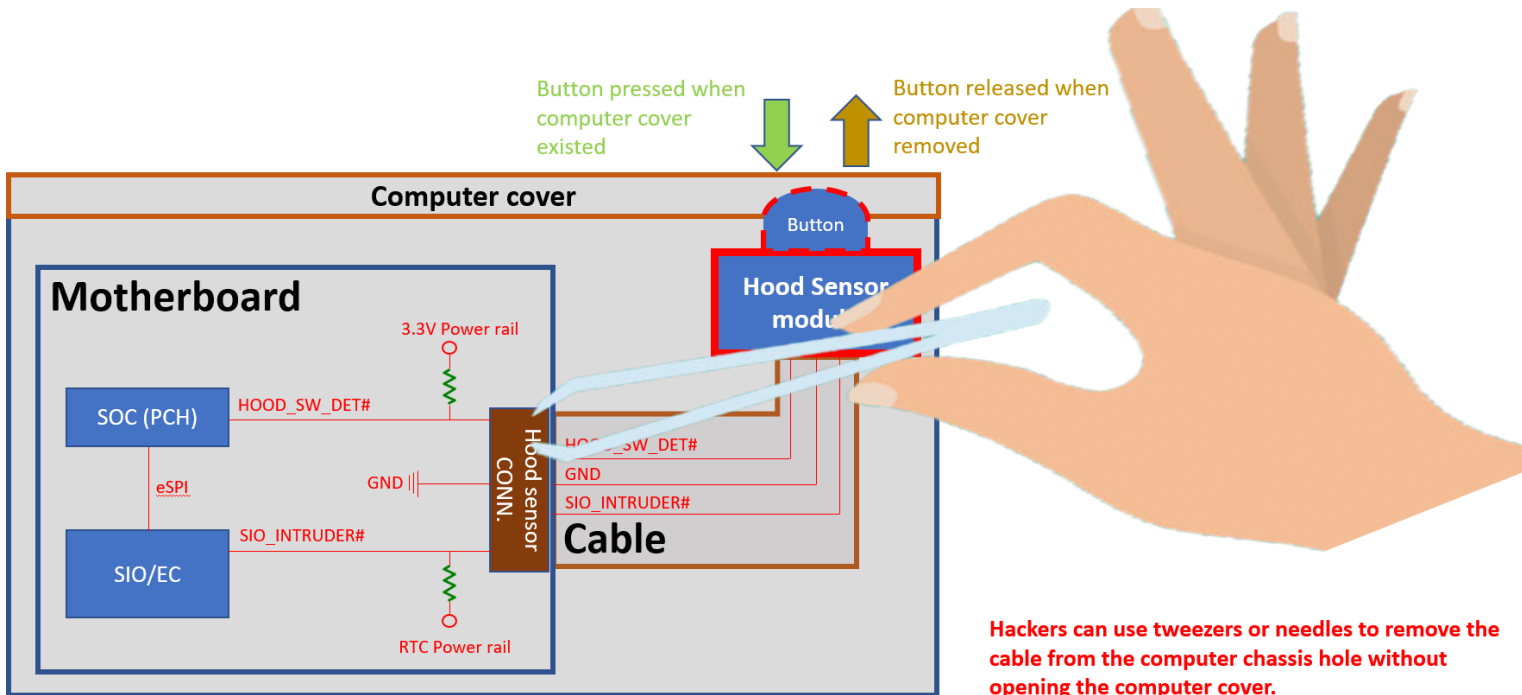
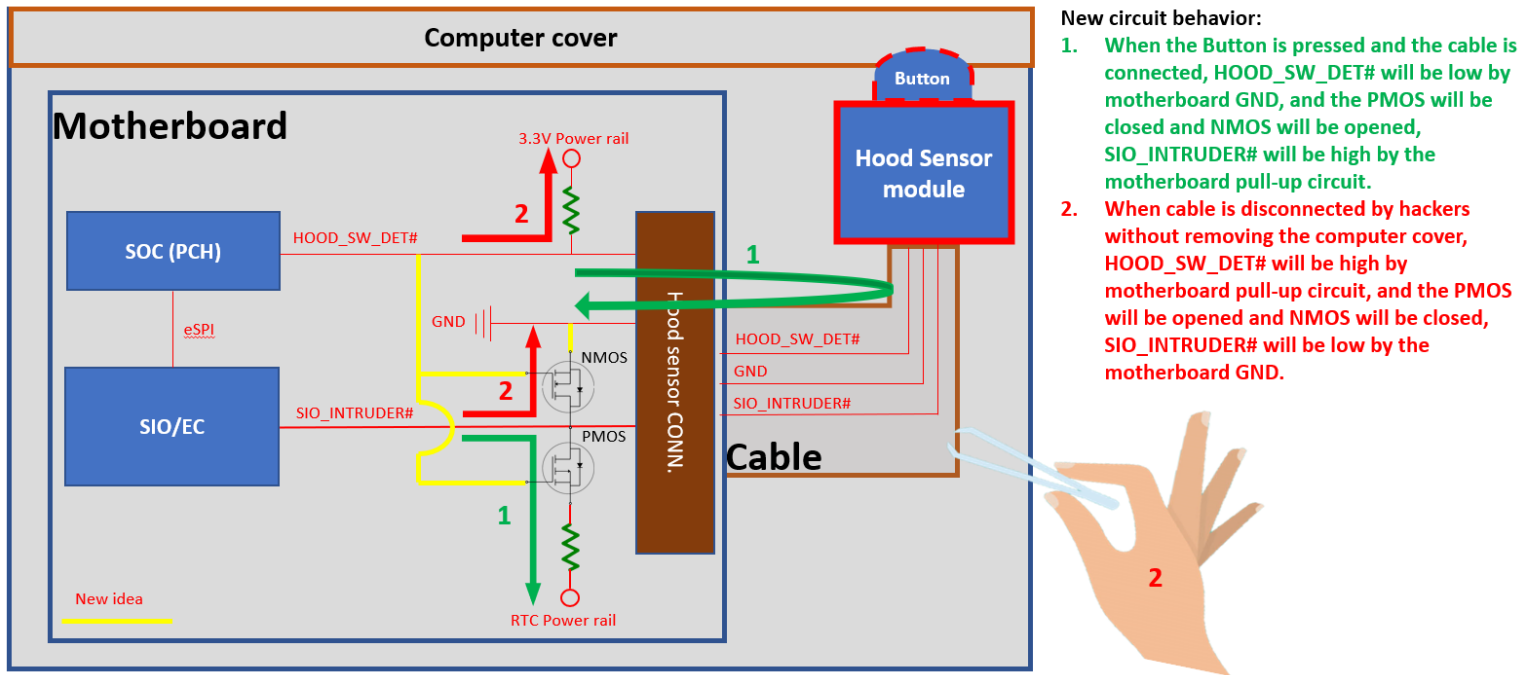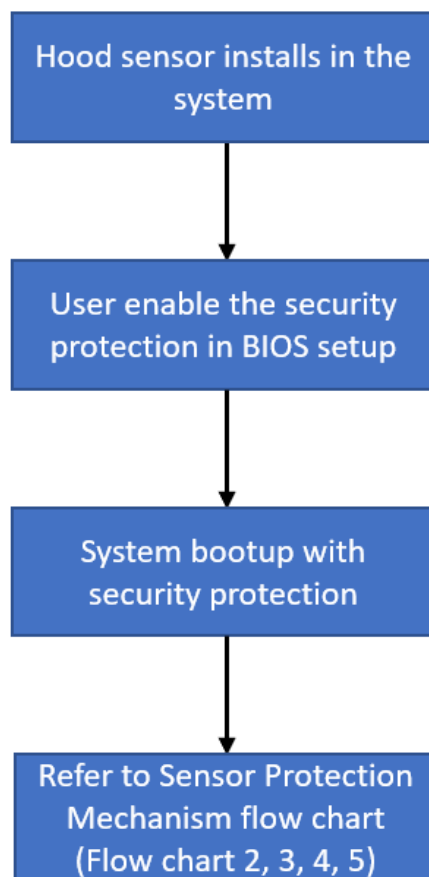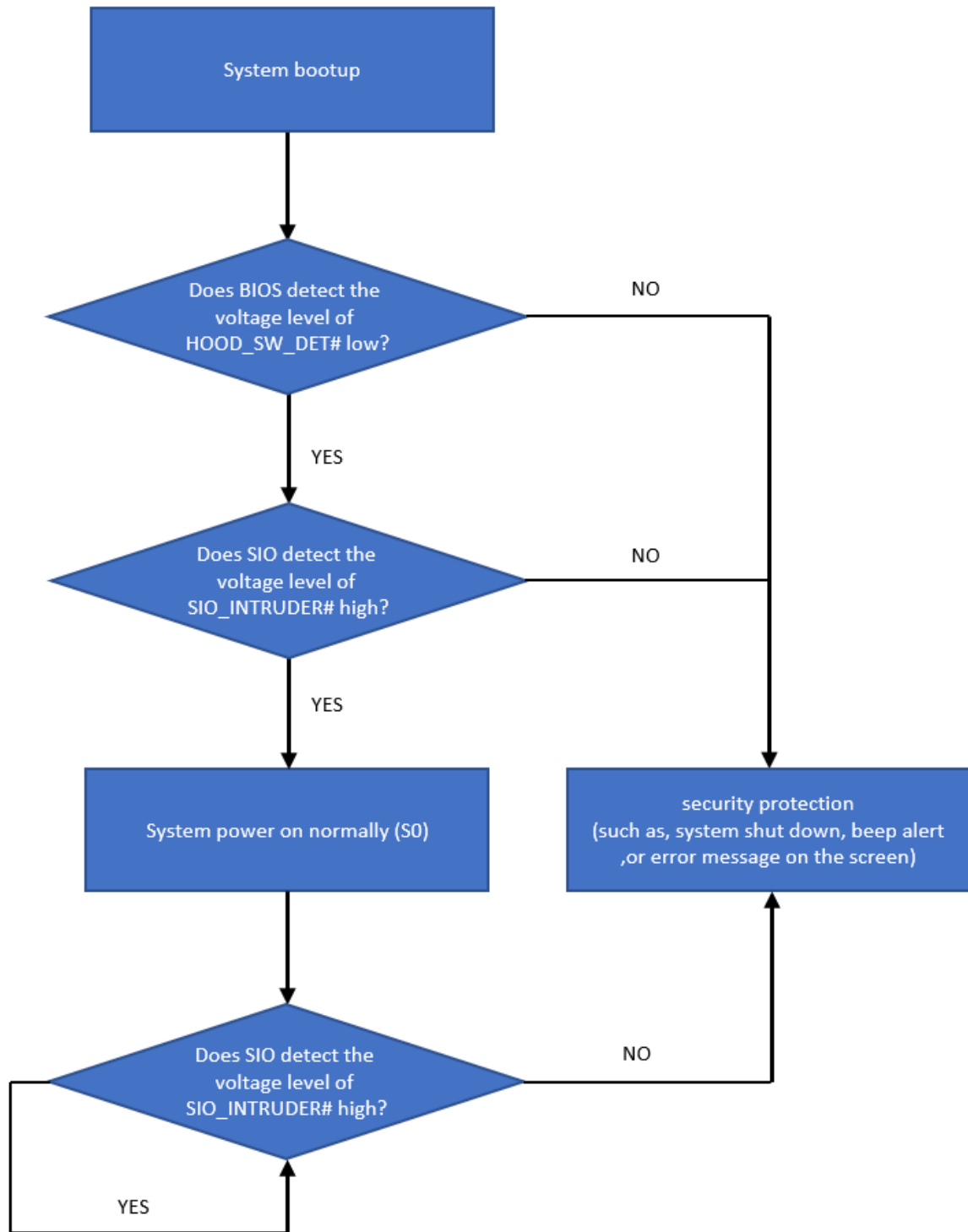Fig. 2 Security Risk of The Current Hood Sensor Protection Mechanism

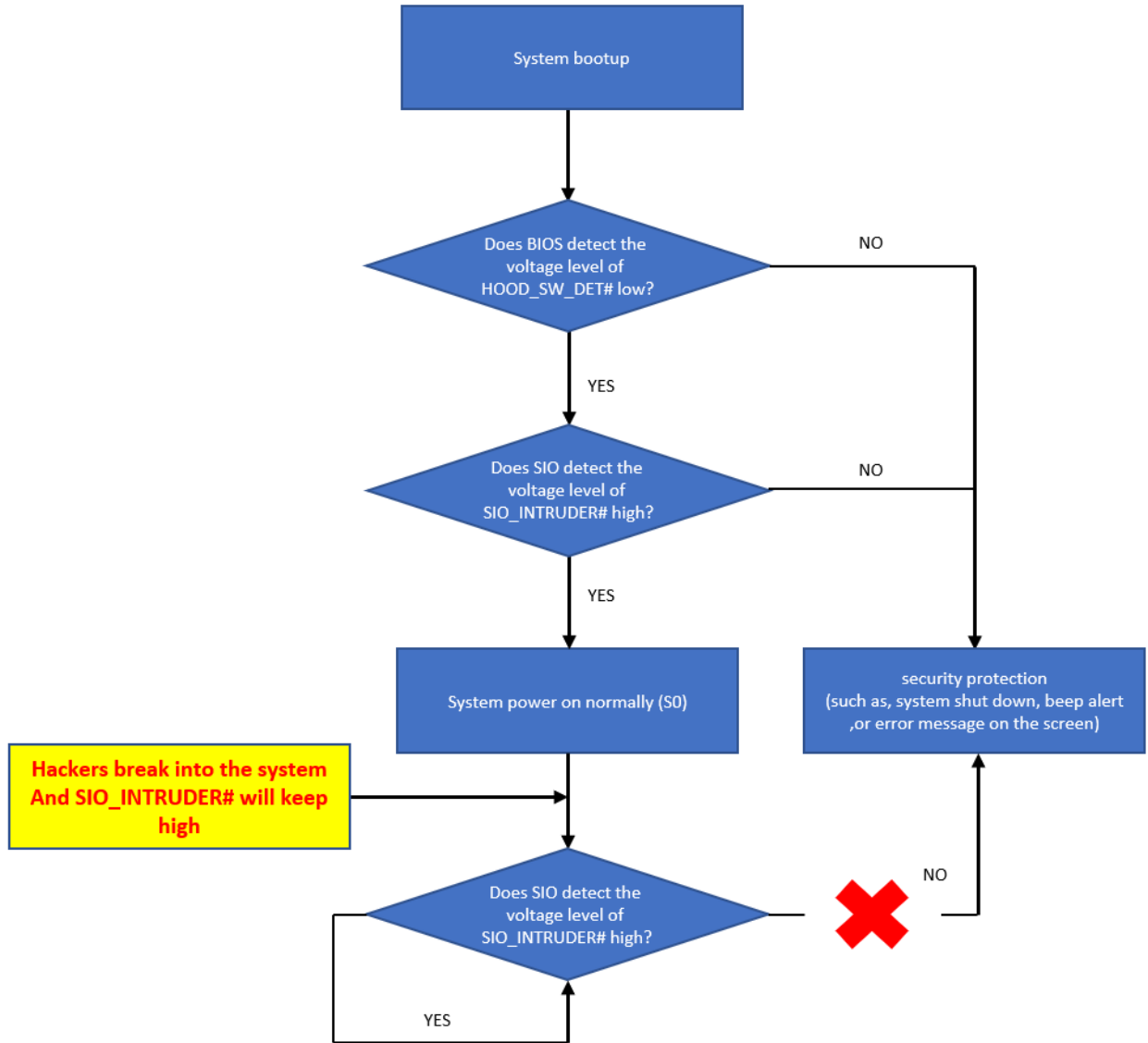Fig. 3 Hardware Enhancement of Hood Sensor Protection Mechanism
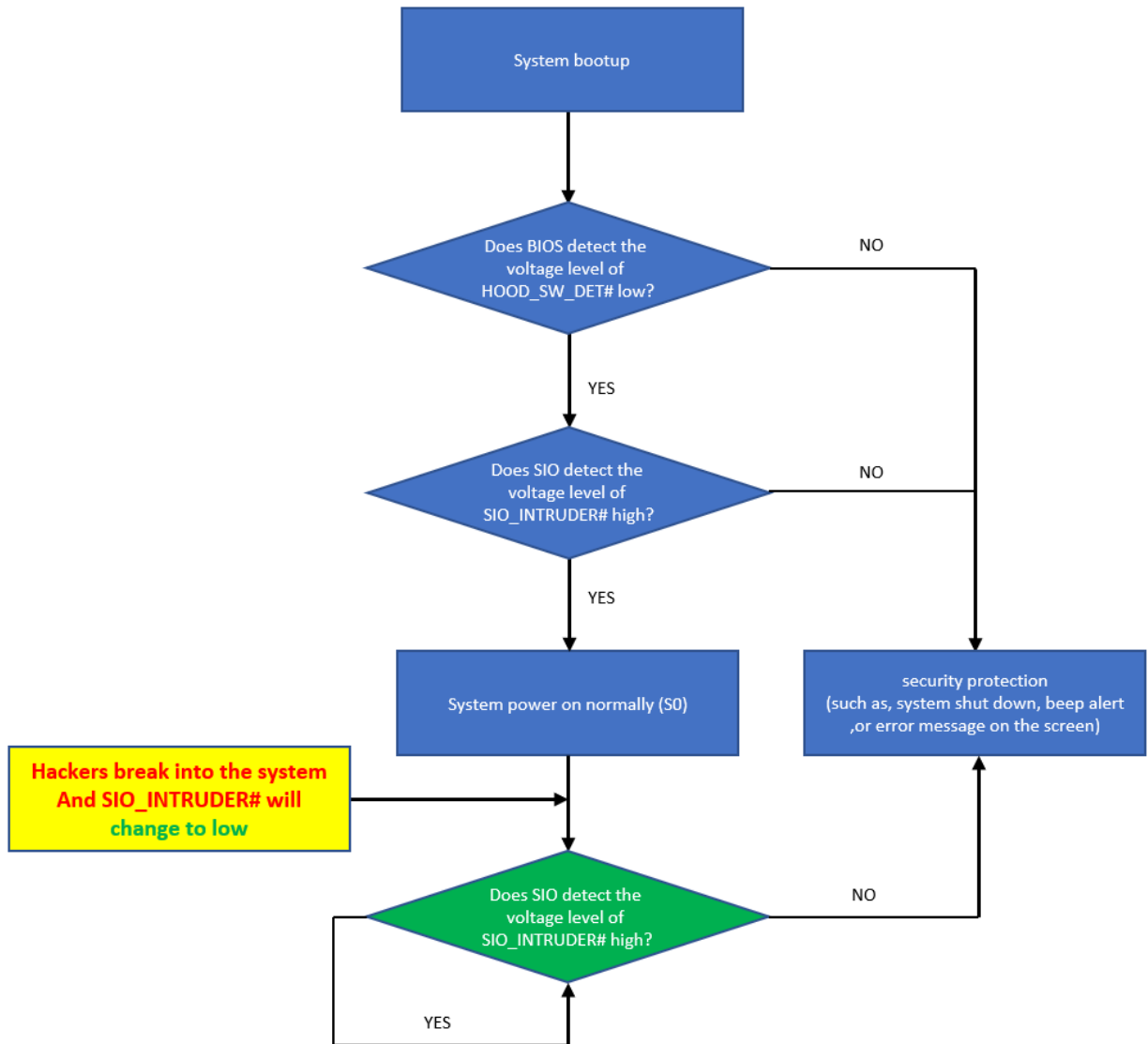
Flow chart list

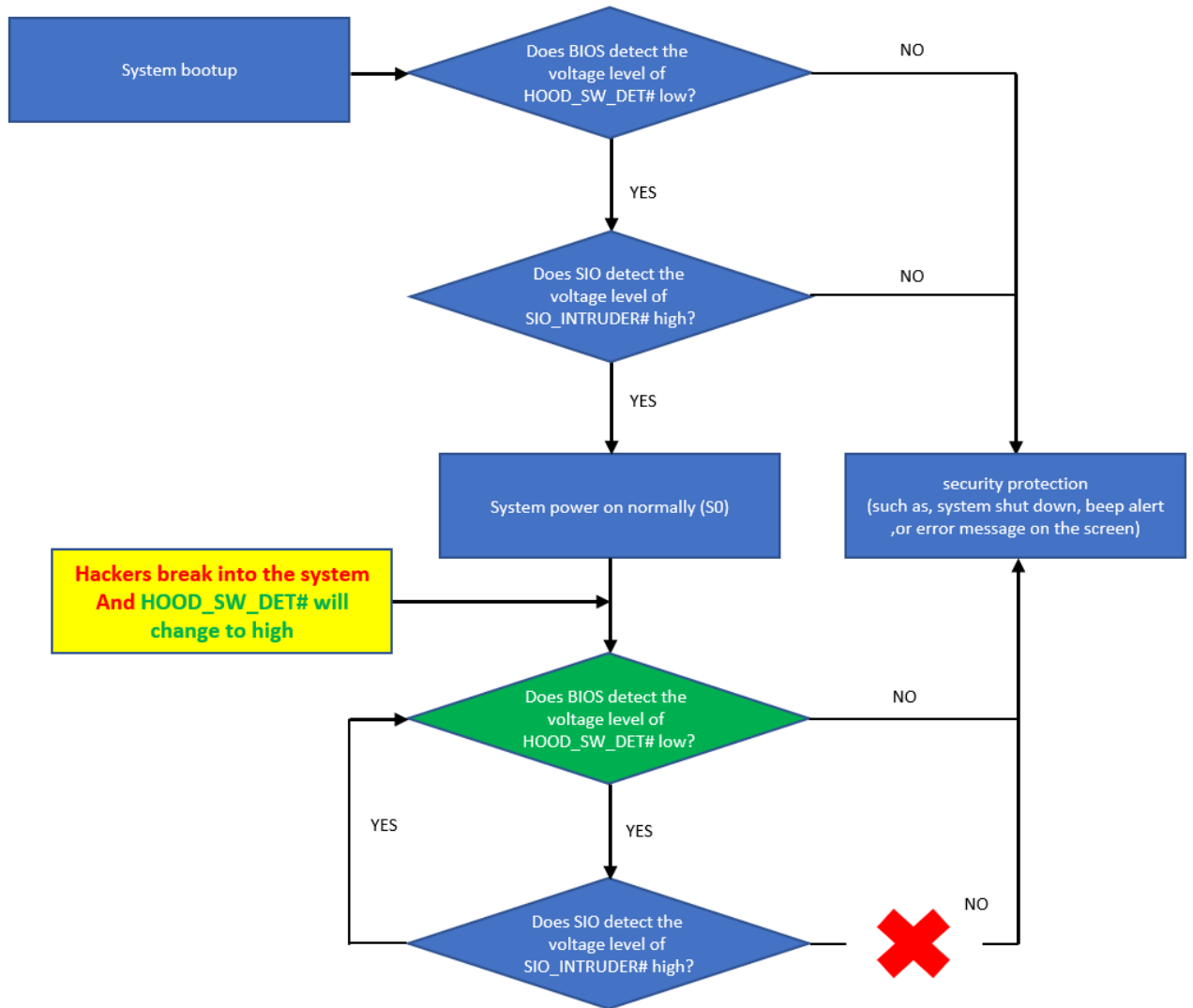Flow chart 1 Hood Sensor Protection Enable Flow Chart

Flow chart 2 Current Hood Sensor Protection Mechanism

Flow chart 3 Security Risk of The Current Hood Sensor Protection Mechanism

Flow chart 4 Hardware Enhancement of Hood Sensor Protection Mechanism

Flow chart 5 Software Enhancement of Hood Sensor Protection Mechanism

Value-added table

Module Cable connect		
Signals	**Computer cover open**	**Computer cover close**
HOOD_SW_DET# (PCH)	L	L
SIO_INTRUDER# (SIO)	L	H

Module Cable disconnect		
Signals	**Computer cover open**	**Computer cover close**
HOOD_SW_DET# (PCH)	H	H
SIO_INTRUDER# (SIO)	H*	H

*If hackers remove the hood sensor cable from the motherboard and **then** open the computer cover, SIO_INTRUDER# will keep high(no voltage level change) and SIO will identify the computer cover is still closed because the hood sensor module has been removed with no function now.

Table 1 Current Hood Sensor Protection Mechanism

Module Cable connect		
Signals	**Computer cover open**	**Computer cover close**
HOOD_SW_DET# (PCH)	L	L
SIO_INTRUDER# (SIO)	L	H

Module Cable disconnect		
Signals	**Computer cover open**	**Computer cover close**
HOOD_SW_DET# (PCH)	H	H
SIO_INTRUDER# (SIO)	L*	L*

*If hackers remove the hood sensor cable from the motherboard, SIO_INTRUDER# will change to low and notify SIO to trigger the security protection.

Table 2 Hardware Enhancement of Hood Sensor Protection Mechanism

Disclosed by ChiWei Ding and Poying Chih, HP Inc.