aruba
a Hewlett Packard Enterprise company

LET'S TALK ABOUT PHYSICAL SECURITY

Steve Weingart, CISA, CRISC

Aruba, a Hewlett Packard Enterprise Company

Overview

- Definition
- FIPS 140-2 Requirements
- Types and Levels
- Discussion of Approaches by Type and Level

Definition:

- Physical security is a barrier placed around a computing system to deter unauthorized physical access to the computing system itself.
- This concept is complementary to logical security, the mechanisms by which operating systems and other software prevent unauthorized access to data.
- Both physical and logical security are complementary to environmental security.

Definition (Types):

- Physical Security should resist access (tamper resistant), detect tampering attempts (tamper detecting) and respond (tamper responding), and/or provide evidence of attempted tampering at a later audit (tamper evident).

- A combination of tamper evidence, response or resistance can be used to create sufficiently strong level of protection to thwart many attacks

Attacks (What we are typing to Prevent)

- Machining: Drilling, milling, cutting; using conventional manual, mechanical, or exotic methods (water, sandblasting, laser, chemical, shaped charge)
  - Manual methods are surprisingly effective!
  - But it does take some skill & practice
- Simple versions of exotic methods can be even more effective
  - ‘Water Torture’ version of water machining is very effective

Attacks (What we are typing to Prevent)

- Conventional sandblasting techniques can remove microns of material at a time
- Drano can be used on epoxies
- Orange Oil based solvents (Goo Gone) can remove almost any label

The goal is to get past any protection mechanisms so that the circuitry can be probed to extract and/or modify data and/or code.

PHYSICAL SECURITY FOR FIPS 140-2

aruba
a Hewlett Packard
Enterprise company

Types

- Single chip
  - Smart Card
  - USB Drive or Key (maybe)
- Multi Chip Embedded
  - Crypto Card
- Multi-Chip Standalone
  - Hardware Security Module
  - Network Box
  - USB Drive or Key (maybe)

Levels

- Level 1 - No Physical Security Requirement
  - No Physical Security Requirement
- Level 2 – Tamper Evidence
  - Tamper Evidence
- Level 3 - Tamper Resistance
  - Tamper Resistance/Response
- Level 4
  - All the Above and More

NOTE: Requirements are cumulative

Types and Levels

	General Requirements for all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
Security Level 4	EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/ response envelope with tamper response and zeroization circuitry.

Table 2: *Summary of physical security requirements*

Level 1

- Single Chip
  - No Physical Security Requirement
- Multi-Chip Embedded
  - No Physical Security Requirement
- Multi-Chip Standalone
  - No Physical Security Requirement

At Level 1, the only requirement is that the module' s construction be 'Production Grade.'

Level 2

- Single Chip
  - Opaque, tamper evident coating
- Multi-Chip Embedded
  - Opaque packaging, tamper evident seals, or pick resistant locks on doors/covers
- Multi-Chip Standalone
  - Opaque packaging, tamper evident seals, or pick resistant locks on doors/covers

At Level 2, the main requirement is tamper evidence, plus some tamper resistance

Level 3

- Single Chip
  - Hard, opaque, tamper evident coating, or strong enclosure
- Multi-Chip Embedded
  - Hard, opaque, tamper evident encapsulation, or strong enclosure, or …
- Multi-Chip Standalone
  - Hard, opaque, tamper evident encapsulation, or enclosure. Removal will likely damage. Response for covers and/or doors.

At Level 3, tampering should leave evidence and cause serious damage and/or initiate a tamper response

Level 4

- Single Chip
  - Hard opaque, removal resistant coating
- Multi-Chip Embedded
  - Tamper detection and response with zeroization for the entire envelope
- Multi-Chip Standalone
  - Tamper detection and response with zeroization for there entire envelope

At Level 4, it is anything goes! Any attack must be repelled, completely damage, or be detected and the CSPs zeroized

DESIGN AND IMPLEMENTATION EXAMPLES

aruba
a Hewlett Packard
Enterprise company

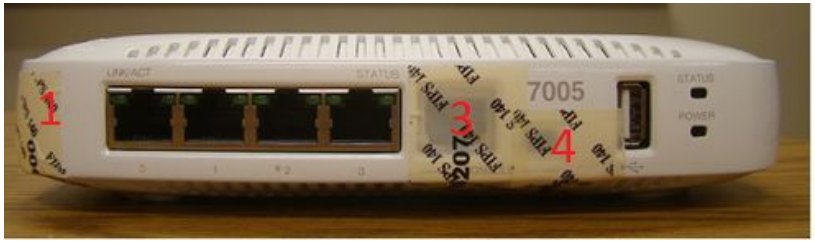
Level 1

- No Special Requirements
  - Build to Industry Standards
  - Pass FCC!

Level 2

- For single chip, it is virtually automatic
- For both multi-chip types, tamper evidence is the big requirement.
  - Tamper evidence labels can often be lifted, without damage test extensively with temperature variations and solvents.
  - Use potting materials and paints that are not easily repaired.
- The enclosure has to be opaque ‘enough.’ IG 5.1
- Vents need to be small or baffled
- Cover locks need to be ‘pick-resistant’

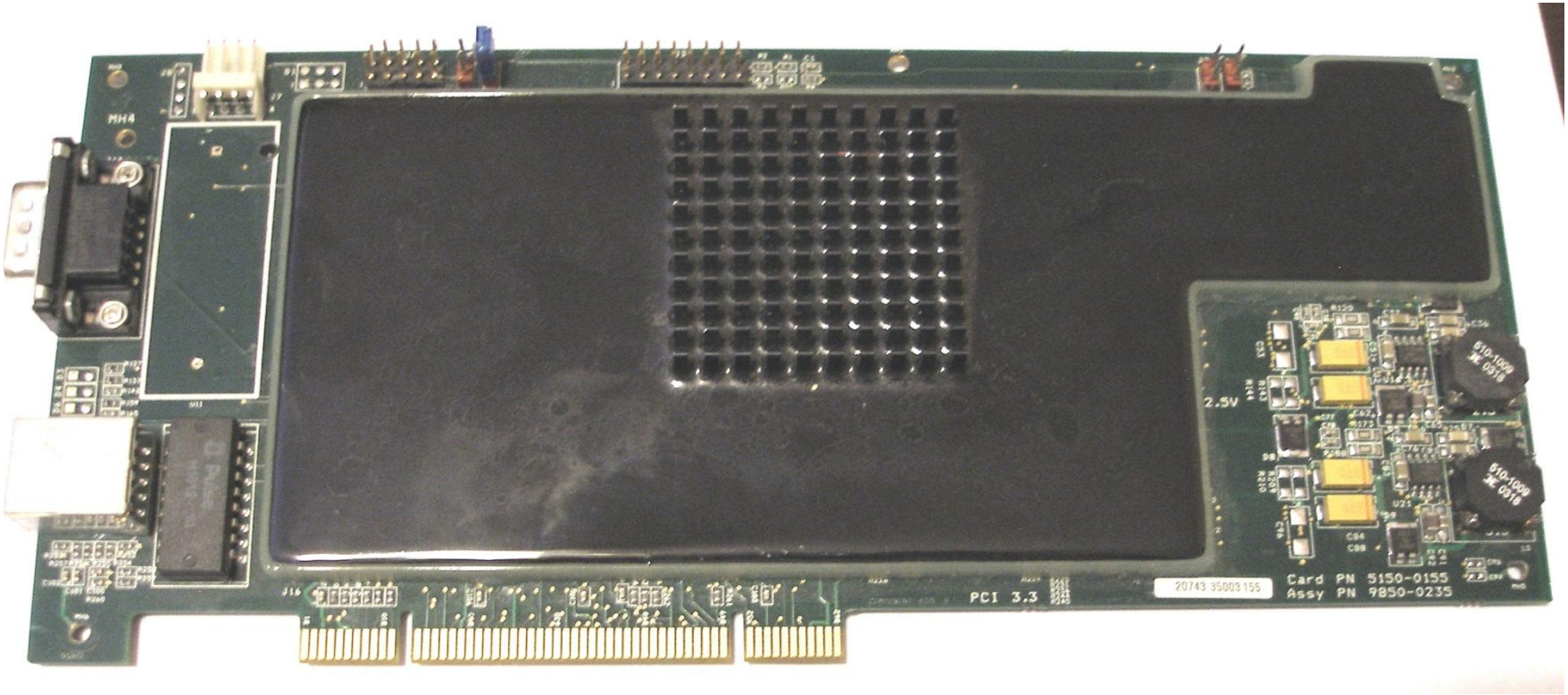
Level 2



Level 3

- For single chip, it is still virtually automatic
- The major choice for Multi-Chip (either) is tamper resistance or response or both
  - If it is convenient to pot the whole module in hard material, that is easy
  - If you have opening covers, you must go the cover locks with detect & respond route.
- Vents need to be baffled with at least a 90 degree bend

Level 3


MH4
2.5V
PCI 3.3
20743 35003 155
Card PN 5150-0155
Assy PN 9850-0235

Level 3 Notes

- For potted packages, make sure that the final surface is smooth for tamper evidence
- For cases with openable covers and sensing, make sure that the sensor can't be easily bypassed (cut/short or glue-the-switch attack)
- Latch the tamper signal (so a short duration mistake will still trigger the zeroize circuit)
- Vents need to be baffled with at least a 90 degree bend
- We need to be aware of the 'edge' and transient conditions that can affect operation.

Level 3

Good (barely)

Better

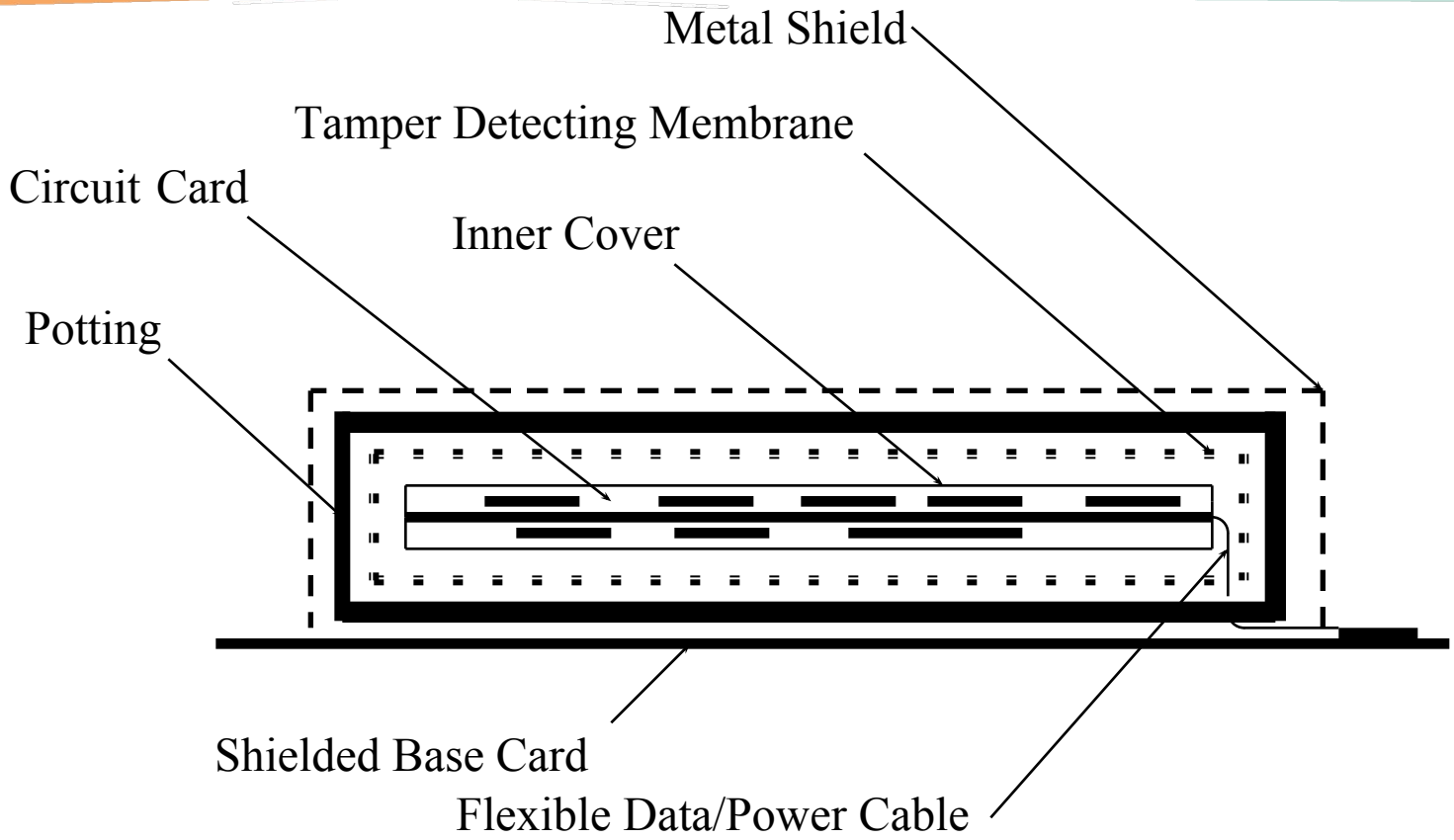
Level 4

- For single chip, hard opaque coating that will cause damage if removed by any means.
- For Multi-Chip (either) tamper resistance and response are required
  - A strong case or hard encapsulation, plus
  - Tamper detection/response with zeroization.
- Unlike lower levels there are no restrictions on what methods may be applied. Drilling, milling, cutting, etc., which are out of scope at lower levels are all allowed

Level 4

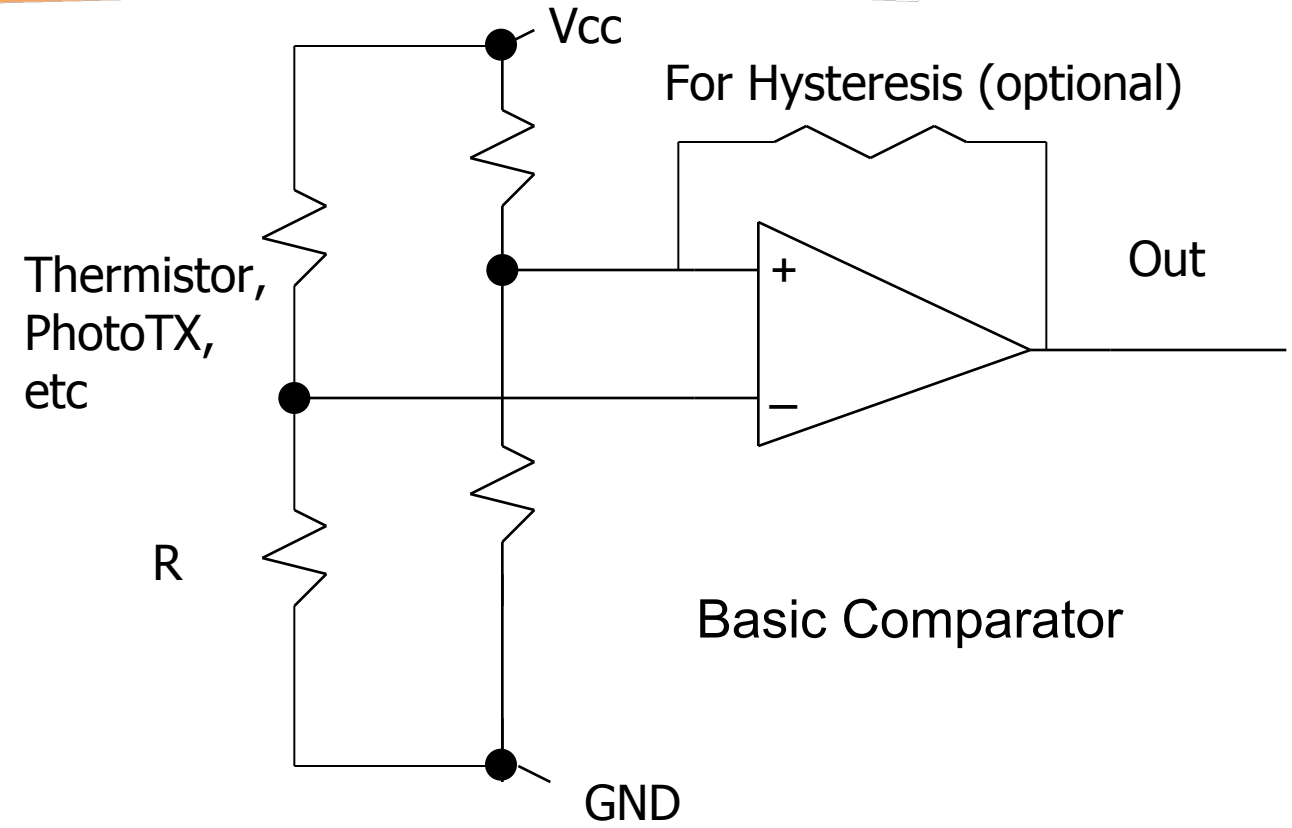
- EFT/EFP are pretty unique requirements
- The intent is to keep the circuitry in its defined operational zone, or to call tamper if the circuit can’t maintain reliable operation.
  - EFT ensures that the module fails gracefully, with no security vulnerability
  - EFP ensures that the module detects that it is going out of the safe zone and triggers tamper.

Level 4

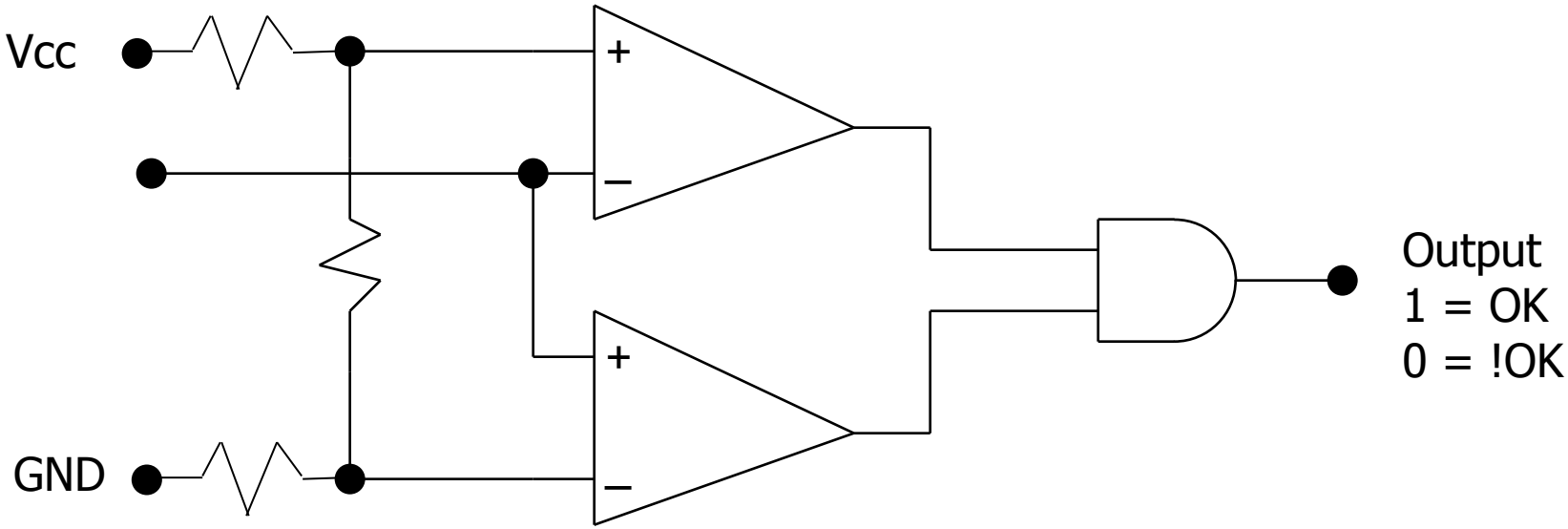

Metal Shield
Tamper Detecting Membrane
Circuit Card
Inner Cover
Potting
Shielded Base Card
Flexible Data/Power Cable

Level 4

Levels 3 & 4: Circuitry Examples



Levels 3 & 4: Circuitry Examples

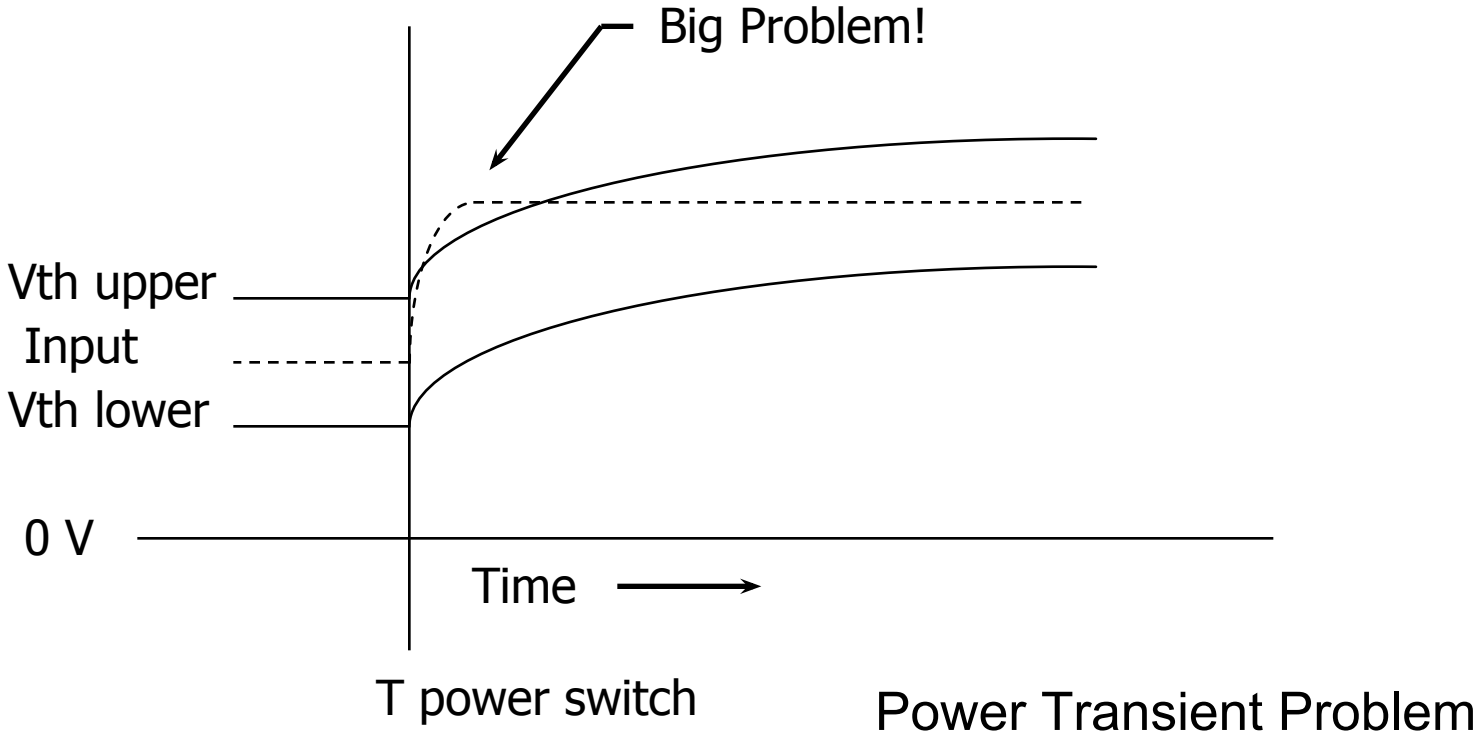


Basic Window Comparator

Levels 3 & 4: Circuitry Examples

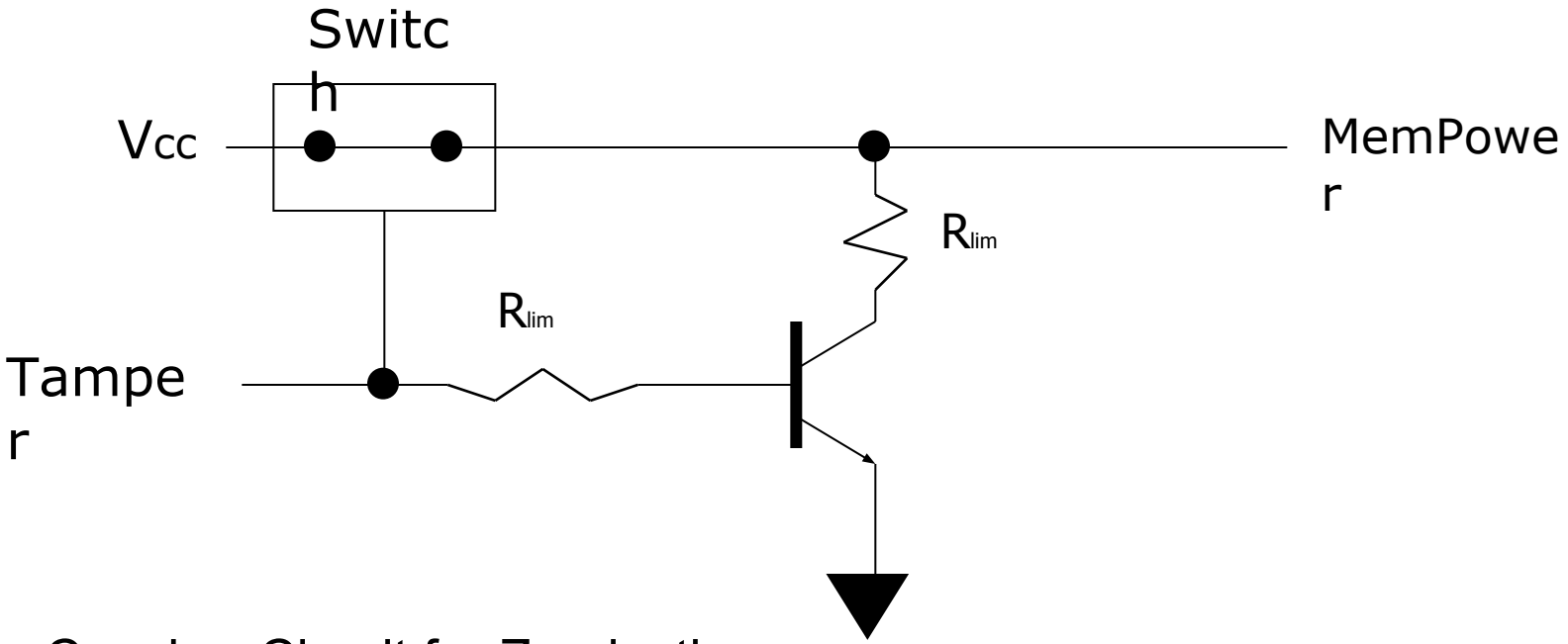
Same Pattern
can be Interleaved on
Top and Bottom

Levels 3 & 4: Circuitry Examples



Power Transient Problem

Levels 3 & 4: Circuitry Examples



Crowbar Circuit for Zeroization

Levels 3 & 4: Circuitry Examples Notes

- For power/cost savings, use open collector gates or comparators to sum up the tamper inputs with a single pull-up (wire ‘OR’).
- Latch the tamper detect signal (catch short goofs)
- Doing the entire tamper detect/response circuit can be done for ~35uA, long battery life is not difficult.
- Be careful to avoid vulnerability to direct sensor attacks such as switch gluing or cover bending.

Levels 3 & 4: Circuitry Examples Notes

- Overwrite zeroization is often not feasible, power removal works well.
- But, beware of back powering and imprinting!!!!!!.
- A Crowbar works reliably, in the absence of attacks such as switch gluing or cover bending.
- Tamper mesh/grid wiring can be EMI susceptible, use placement that results in EMI cancellation
- R/C ‘timers’ can ensure proper initialization on power up

THANK YOU!

QUESTIONS?

aruba
a Hewlett Packard
Enterprise company