Portrait
of a
Byzantine
Assassin

Kevin.Driscoll@Honeywell.com
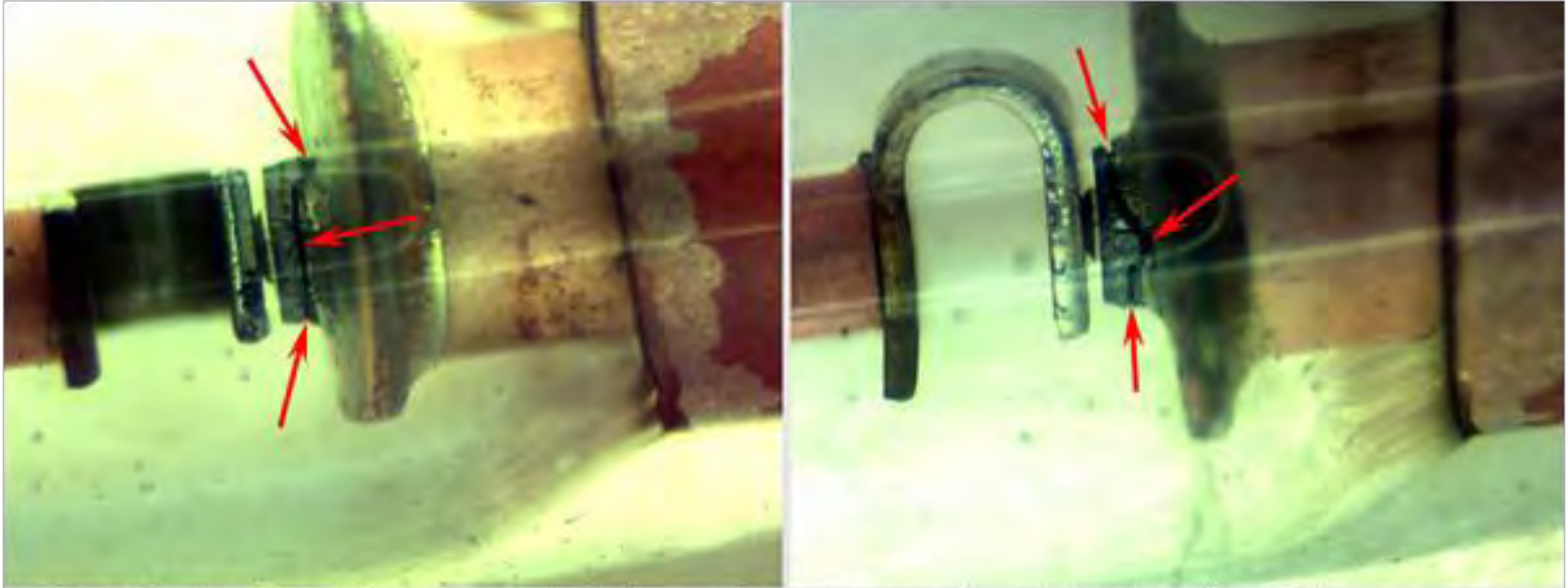
First Picture of a Byzantine Fault?

Figure 1. Two views (90 degrees apart) of a fissure that appears to go through the silicon dice - Red arrows.

A crack (fissure) through a diode appeared in a Space Shuttle while on the launch pad preparing for mission STS-124. At 12 minutes and 38 seconds past noon on 5/13/2008, this caused a 3-1 split of the four computers that control the Shuttle. Three seconds later, the split became 2-1-1. Eventually, the remaining 2 computers disagreed (1-1-1-1). But, none of the processors or their intercommunications were faulty. The fault was in a box that sends messages to the computers.
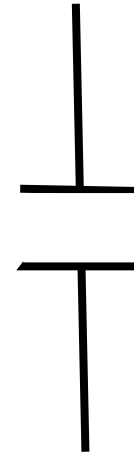
Transmogrification
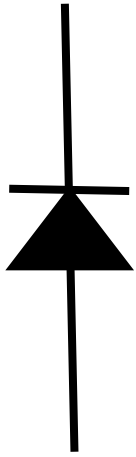
A diode …   with a perpendicular crack …   is really a capacitor

How many Failure Modes and Effects Analysis (FMEA) procedures ask what would happen if one electrical part (a diode) changed into another (a capacitor)? And, yet, the simplest of failures (a crack) can cause this transmogrification. The literature includes reports of IC traces becoming capacitors, capacitors becoming resistors, …

Normal Messages (differential traces)
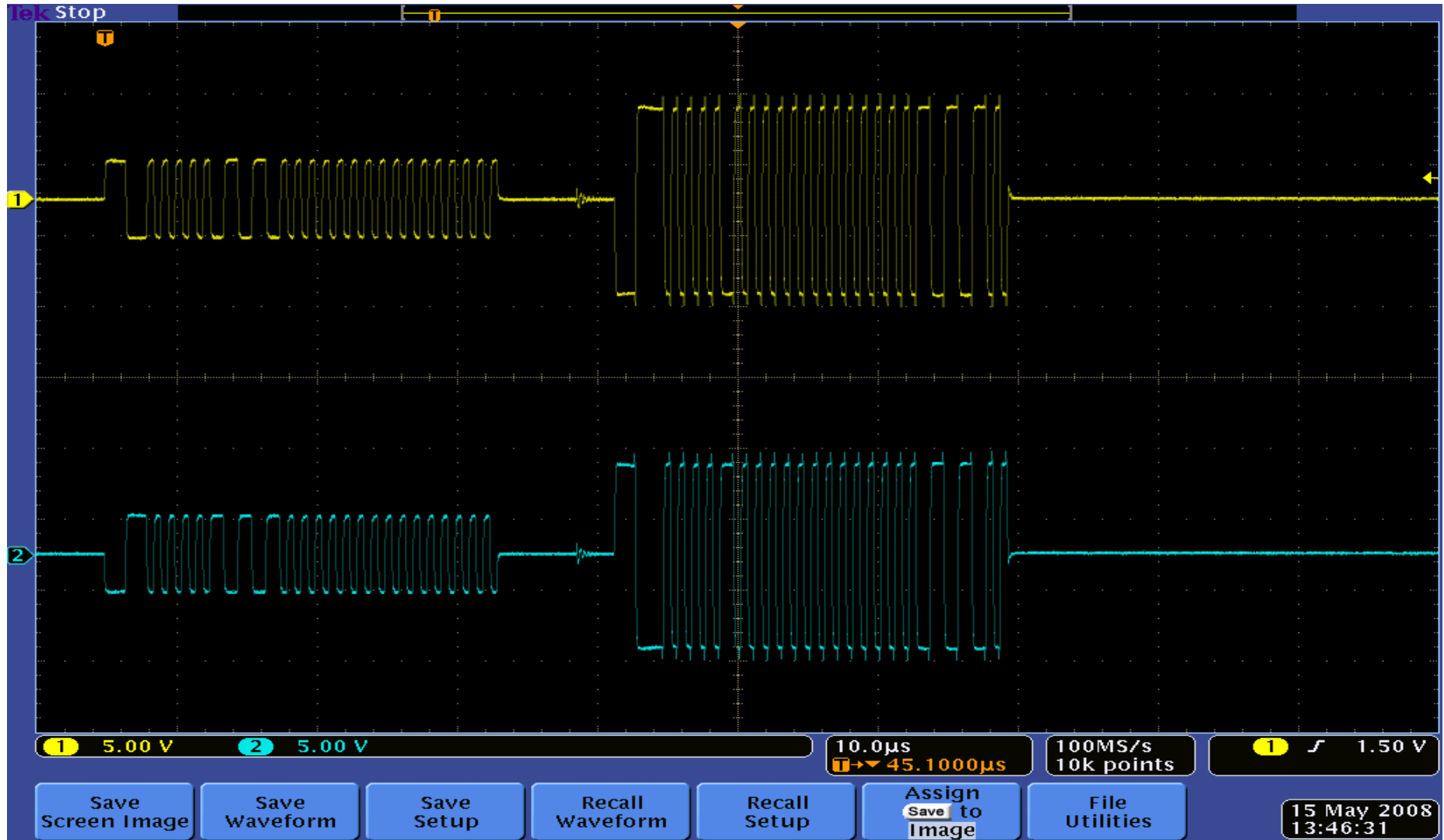
Faulty Message on the Right
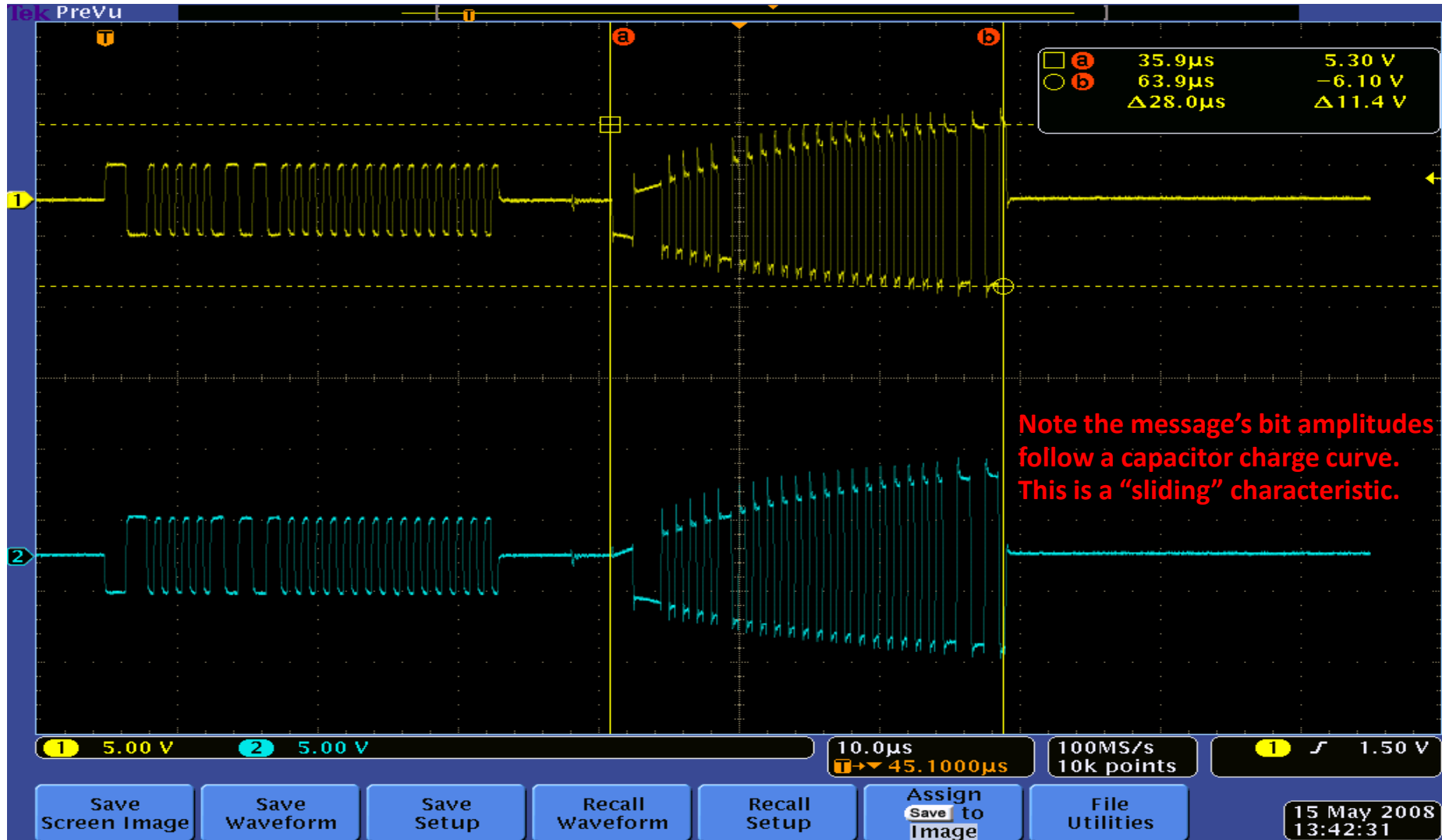
Summary of Observations

- Byzantine Assassin
  - convinces "good guys" to kill (or ostracize) themselves
  - can cause as many corpses or cliques as there are fault sets (containment zones)
  - without Byzantine Fault tolerance, no amount of redundancy is enough
  - murder mechanisms (e.g. hybrid NMR) are inherently dangerous
    - an Assassin can subvert them into accomplices for mass murder
    - suicide is safer; that is a reason to use atomic self-checking pairs
  - can be an Outsider (not a General nor one of the Generals' Messengers)
  - can be created by the simplest of faults in the simplest of parts
- Faults can convert one type of part into another
  - diode → capacitor, trace → capacitor, capacitor → resister, analog circuit → digital circuit, digital circuit → analog circuit
  - related phenomenon: a fault can create a part from "nothing" ("partogenesis" ☺)
    - typically, via the fault causing a large increase in parasitic properties
- FMEA teams should include:
  - curmudgeons, skeptics, "pathological thinkers" (to counterbalance designers who are optimists)
  - members of related/neighboring disciplines
  - physicists (find another Feynman)
- "Sliding" failure
  - a part's behavior gradually changes
  - from in specification to (slightly) out of specification, or vice versa
  - higher probably of hitting a Byzantine region of behavior than one would expect

Arthur C. Clark's 1st law of prediction: "When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is very probably wrong."