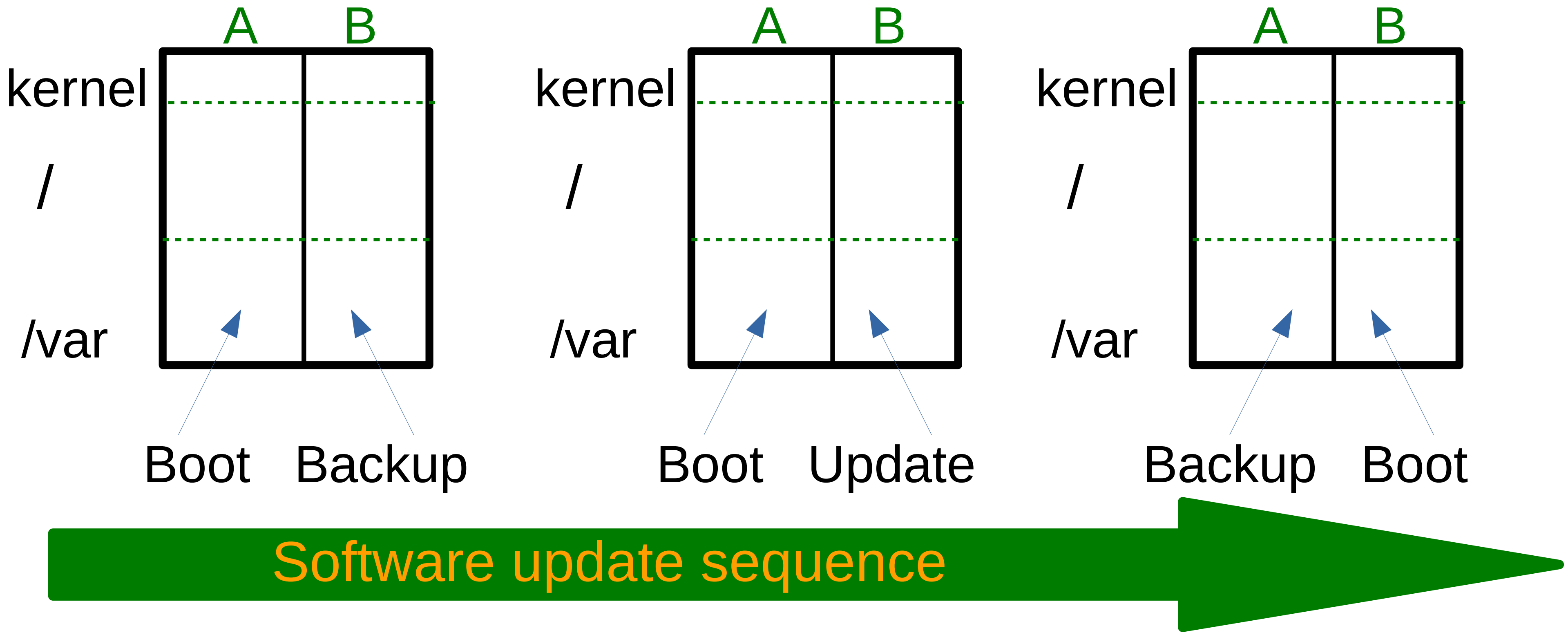
Supporting SW Update via u-boot and GPT/EFI

Alison Chaiken
alison@she-devel.com

3/10/2020

Software Update via A/B Image Flipping

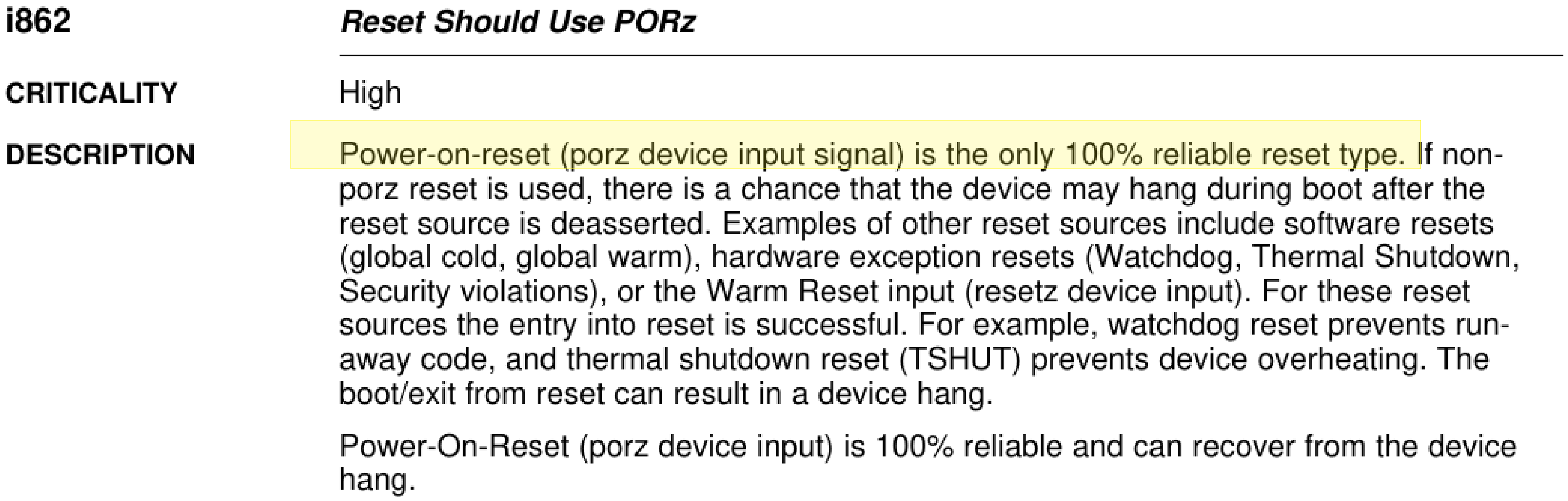


How does the bootloader choose A vs. B?

Traditionally, the operating system
writes the bootable image selection
to memory at each shutdown,
then “warm resets.”

When the bootloader runs,
it reads the selection from memory.

PMIC Errata: no “warm boot” support



i862 ***Reset Should Use PORz***

CRITICALITY High

DESCRIPTION Power-on-reset (porz device input signal) is the only 100% reliable reset type. If non-porz reset is used, there is a chance that the device may hang during boot after the reset source is deasserted. Examples of other reset sources include software resets (global cold, global warm), hardware exception resets (Watchdog, Thermal Shutdown, Security violations), or the Warm Reset input (resetz device input). For these reset sources the entry into reset is successful. For example, watchdog reset prevents run-away code, and thermal shutdown reset (TSHUT) prevents device overheating. The boot/exit from reset can result in a device hang.

Power-On-Reset (porz device input) is 100% reliable and can recover from the device hang.

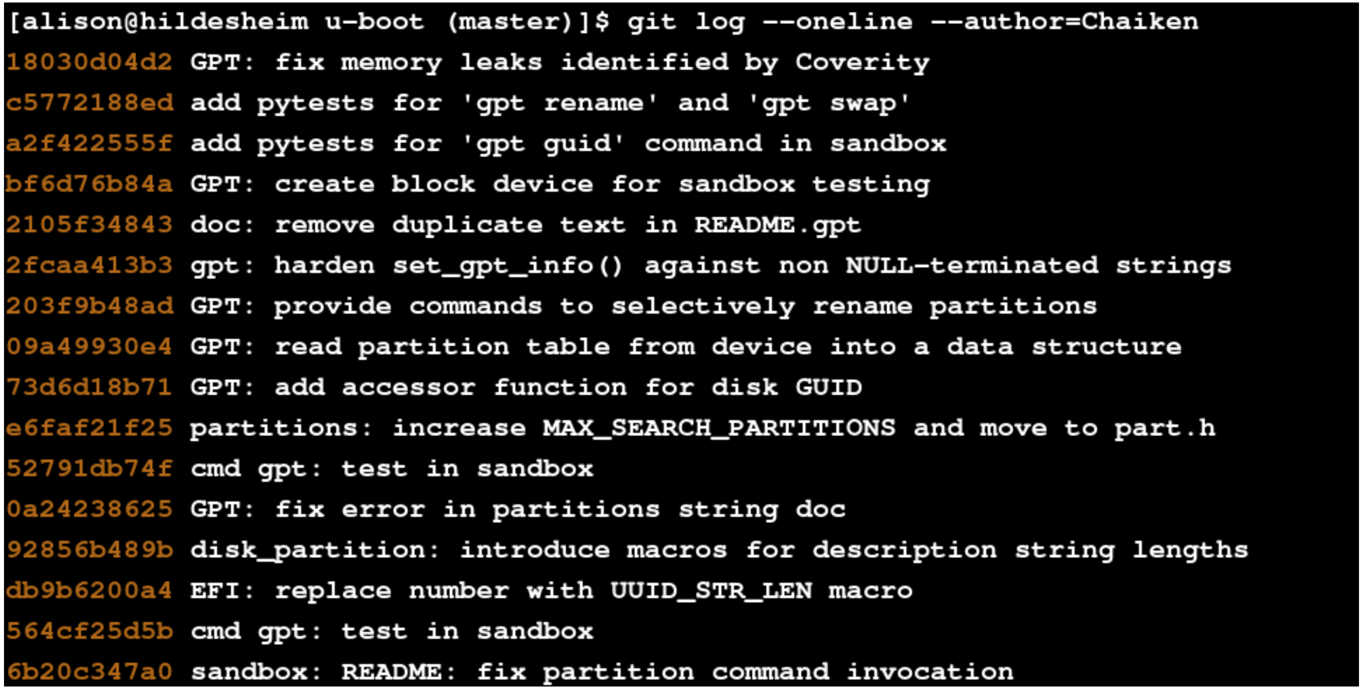
Source: TI TDA2x processor errata

Designating boot image w/o warm reset

- The information must be written to non-volatile storage: EEPROM, NAND flash, /var partition . . . ?
- Design: write all info about partitions into the existing storage device partition table.
- EFI partition tables in GPT format support a “name” string.
- A boot attempt counter can conveniently be stored there.
- 2016: u-boot had no support GPT name strings.

View source code that implements GPT names

- git clone git://git.denx.de/u-boot; cd u-boot
- git log --author=Chaiken

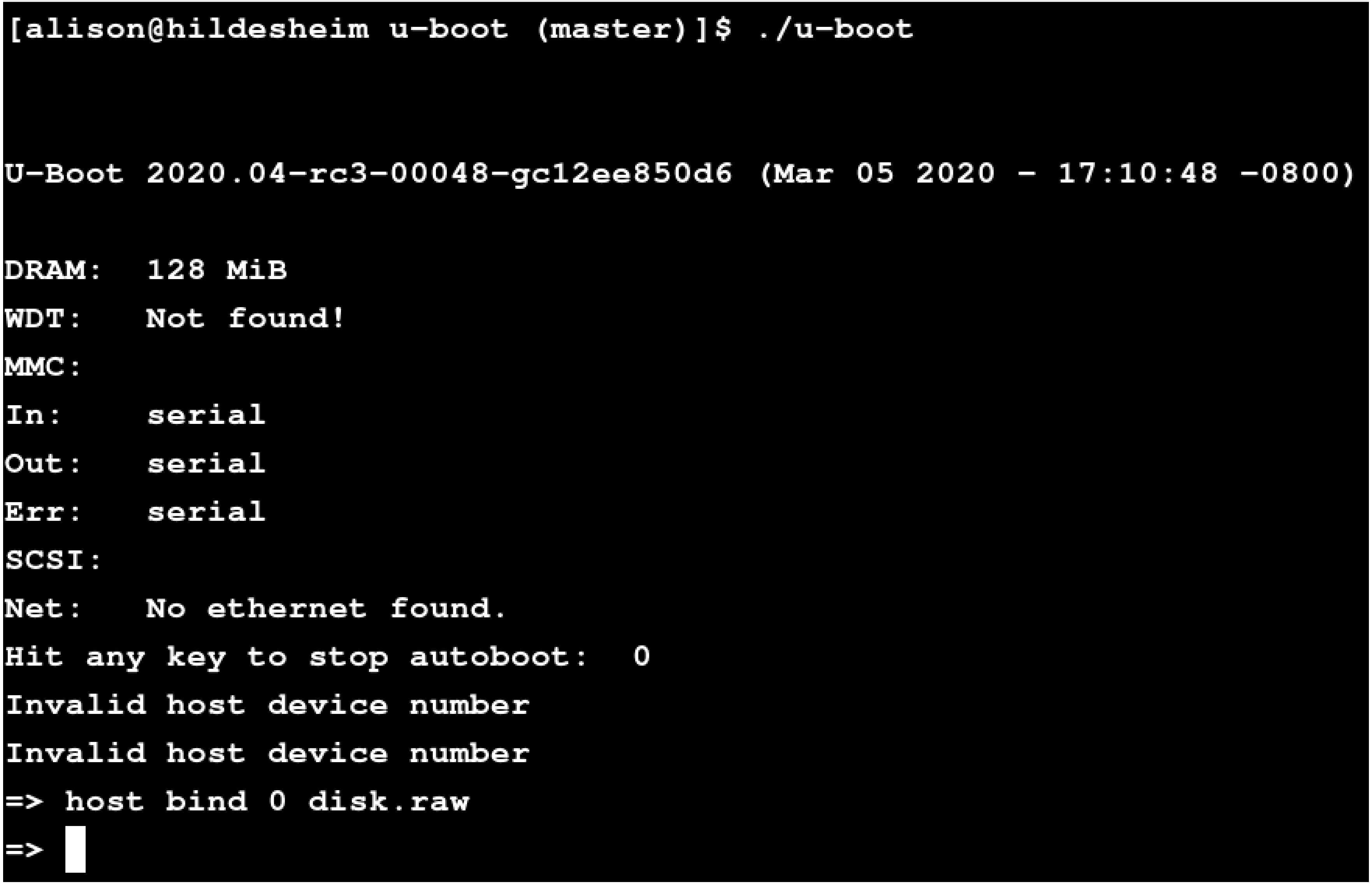


```
[alison@hildesheim u-boot (master)]$ git log --oneline --author=Chaiken
18030d04d2 GPT: fix memory leaks identified by Coverity
c5772188ed add pytests for 'gpt rename' and 'gpt swap'
a2f422555f add pytests for 'gpt guid' command in sandbox
bf6d76b84a GPT: create block device for sandbox testing
2105f34843 doc: remove duplicate text in README.gpt
2fcaa413b3 gpt: harden set_gpt_info() against non NULL-terminated strings
203f9b48ad GPT: provide commands to selectively rename partitions
09a49930e4 GPT: read partition table from device into a data structure
73d6d18b71 GPT: add accessor function for disk GUID
e6faf21f25 partitions: increase MAX_SEARCH_PARTITIONS and move to part.h
52791db74f cmd gpt: test in sandbox
0a24238625 GPT: fix error in partitions string doc
92856b489b disk_partition: introduce macros for description string lengths
db9b6200a4 EFI: replace number with UUID_STR_LEN macro
564cf25d5b cmd gpt: test in sandbox
6b20c347a0 sandbox: README: fix partition command invocation
```

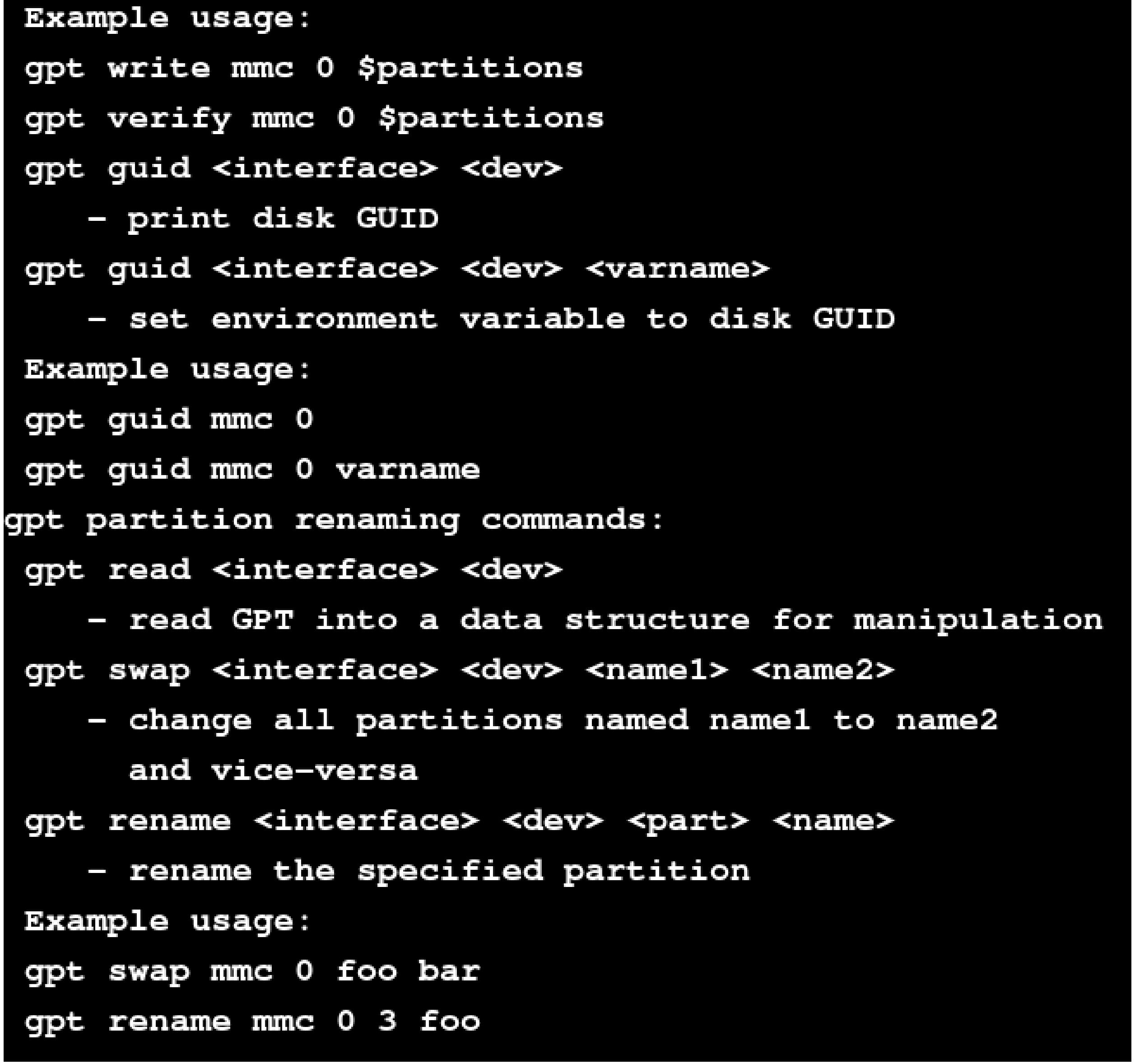
Demo via u-boot's sandbox

- make sandbox_defconfig
- make all NO_SDL=1
- Follow instructions in doc/README.gpt to make a soft block device.
- ./u-boot

which produces . . .

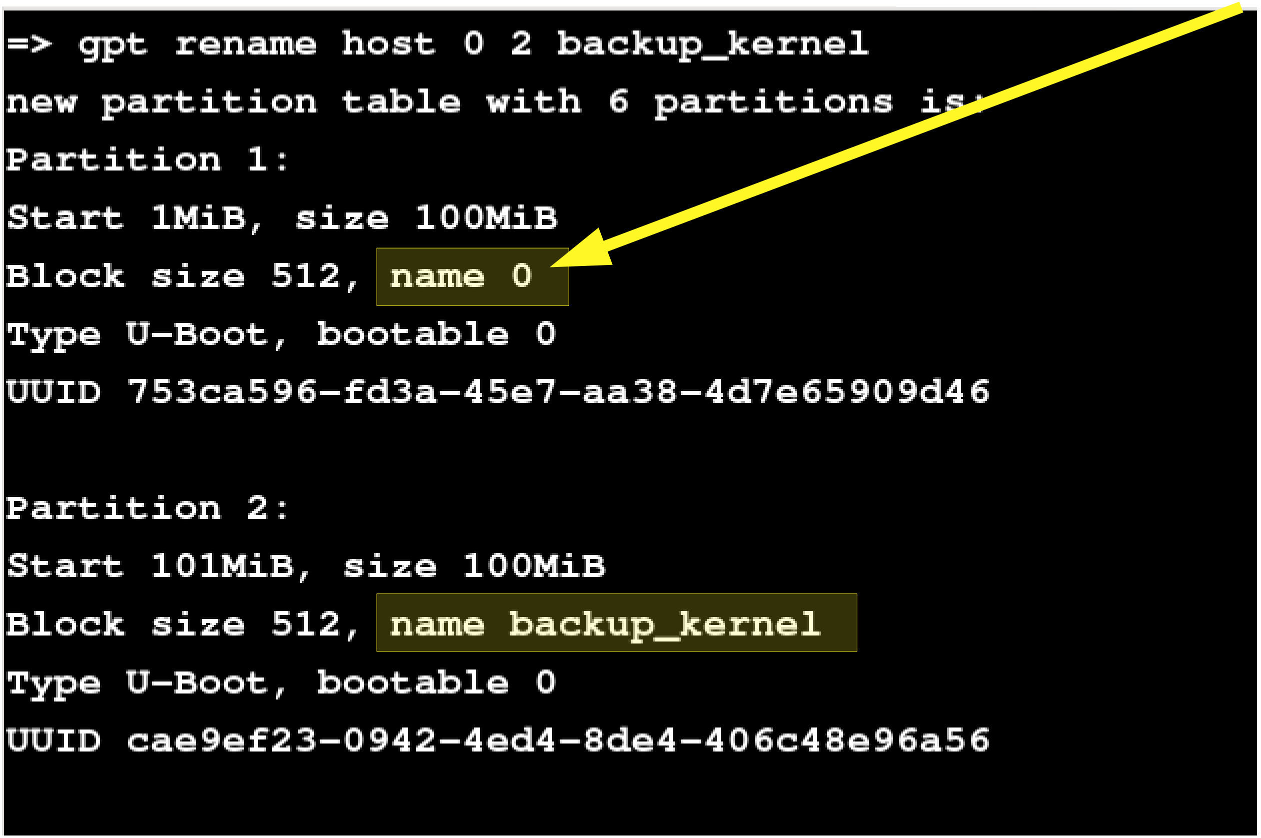


```
[alison@hildesheim u-boot (master)]$ ./u-boot


U-Boot 2020.04-rc3-00048-gc12ee850d6 (Mar 05 2020 - 17:10:48 -0800)

DRAM:  128 MiB
WDT:   Not found!
MMC:
In:    serial
Out:   serial
Err:   serial
SCSI:
Net:   No ethernet found.
Hit any key to stop autoboot:  0
Invalid host device number
Invalid host device number
=> host bind 0 disk.raw
=> 
```



```
 Example usage:
 gpt write mmc 0 $partitions
 gpt verify mmc 0 $partitions
 gpt guid <interface> <dev>
    - print disk GUID
 gpt guid <interface> <dev> <varname>
    - set environment variable to disk GUID
 Example usage:
 gpt guid mmc 0
 gpt guid mmc 0 varname
gpt partition renaming commands:
 gpt read <interface> <dev>
    - read GPT into a data structure for manipulation
 gpt swap <interface> <dev> <name1> <name2>
    - change all partitions named name1 to name2
      and vice-versa
 gpt rename <interface> <dev> <part> <name>
    - rename the specified partition
 Example usage:
 gpt swap mmc 0 foo bar
 gpt rename mmc 0 3 foo
```

Boot attempt counter



```
=> gpt rename host 0 2 backup_kernel
new partition table with 6 partitions is:
Partition 1:
Start 1MiB, size 100MiB
Block size 512, name 0
Type U-Boot, bootable 0
UUID 753ca596-fd3a-45e7-aa38-4d7e65909d46

Partition 2:
Start 101MiB, size 100MiB
Block size 512, name backup_kernel
Type U-Boot, bootable 0
UUID cae9ef23-0942-4ed4-8de4-406c48e96a56
```

Summary

- A/B partition flipping is a conservative strategy when storage capacity allows it.
- Traditional flip is accomplished by Linux message in memory to u-boot.
- PMIC bug in TI TDA2 prevented message in memory.
- Work-around: write the message into the storage partition table.
- Contributed the implementation code to upstream u-boot.