Redundant Booting with U-Boot

Welcome to the Redundancy Theater Playhouse
Thomas Rini
Overview

• Historically how redundancy has been developed and implemented
• What we have today
  – And have had for a while
• What we'll have soon
• Sample use cases
  – Deployed product
  – Developers
• Example
Historically...

- One-off custom creations
- Hacks to U-Boot
- And sometimes, working with upstream and leveraging existing features
Features Available Now

• Redundant U-Boot environment
• Hardware Watchdogs
• Boot counting
  - Requires a “good” location to work with
• Cryptographic image signature checking
  - Software only, currently
• TPM (Trusted Platform Module) support
• “Falcon Mode”, aka SPL boots OS

Some of this is relatively new, much of it is not. We're working to address needs and enhance support, as developers come forward.
How it looks

- **Is bootlimit set and exceeded?**
  - **No**
    - **Start Linux**
  - **Yes**
    - **Start U-Boot, run altbootcmd**

- **Increment bootcount**

- **Get environment**

- **Watchdog kicking things over**

- **Start watchdog**

- **Load SPL**
Features In Progress

• Linux Kernel side of Boot counting
  – Have to clear the counter once the system decides it's up and stable

• Hardware / ROM Cryptographic image signature checking

• “Falcon Mode” enhancements

• SPL / Bootcount enhancements using environment
Sample Use Cases: Deployed Products

- ROM provides a level of security and redundancy
- SPL OS boot provides quick path into the Linux kernel
- Redundant environment is consulted for where to find what to boot, how many times to try
- A fail-safe alternative exists as backup (failed upgrades, etc)
- Watchdog is enabled to reset the board when things have gone bad
- Images are cryptographically signed
- A TPM is enabled to allow for only trusted upgrades to happen
Sample Use Cases: Developer

- SPL OS boot enabled, environment consulted for what Linux kernel to be booting and testing
- Watchdog enabled, relatively short timeout set
  - Catch failure quicker
- Bootlimit is set low, just 1 or 2
  - Again, catch failure quicker
- Environment again points to a known working backup image to use, for when things fail
- `fw_setenv` in Linux to point at new test images / etc

Development cycle improved, fallback available without external hardware.
Example

• BeagleBone Black
  - Watchdog Support
  - SPL OS boot enabled
  - Bootlimit is set, clearable from the kernel
  - Persistent Environment (redundant)
    • fw_setenv/getenv supports this