Platform Management

Presented By

Jerry Wong
System Software & SoC Solutions – Product and Technical Marketing
Part 1 of 4: Platform Management Overview and Boot ...
Platform Management Firmware

- **Base Firmware**
  - Required

- **Programmable Logic Configuration Manager**
  - Optional

- **Power Management Framework**
  - Required

- **Warm Restart Manager**
  - Optional

- **Functional Safety Software Test Library (STL)**
  - Optional

- **User Firmware**
  - Optional

... Select from optional functions...
## Platform Management Functions - Associated Markets

<table>
<thead>
<tr>
<th>Platform Management Feature</th>
<th>Primary Markets</th>
<th>Secondary Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot &amp; Configuration</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>A&amp;D, Auto, ISM</td>
<td>Wired</td>
</tr>
<tr>
<td>Partial Reconfiguration</td>
<td>Data Center</td>
<td>A&amp;D, Auto, Wired</td>
</tr>
<tr>
<td>Power Management</td>
<td>A&amp;D (MILCOM, SATCOM), Auto</td>
<td>ISM</td>
</tr>
<tr>
<td>Reset</td>
<td>Wired, A&amp;D</td>
<td>Auto, ISM</td>
</tr>
<tr>
<td>Functional Safety</td>
<td>Auto, ISM</td>
<td>A&amp;D (Aerospace &amp; Defense)</td>
</tr>
<tr>
<td>PL Health Monitor</td>
<td>A&amp;D, Space, Data Center</td>
<td>Wired</td>
</tr>
</tbody>
</table>

Note: Functions can be selected up to the available 128KB RAM …

… Often “enabling” functions to various applications …
Customizing PMU Firmware

> Modules can be enabled in code
  >> xpfw_config.h
  >> ENABLE_PM - Enable Power Management Module
  >> ENABLE_EM - Enable Error Management Module
  >> ENABLE_RTC_TEST - Enable RTC Event Handler Test Module
  >> ENABLE_SCHEDULER - Enable Scheduler Module
  >> ENABLE_SAFETY - Enable Safety Code

> UART output
  >> fw_printf() – useful for standard debug techniques
  >> Default is to print on UART0 – can be changed to UART1 in BSP settings

> EEMI Implementation
  >> Found in pm_core.c

... See PMU Firmware Wiki for more...
Zynq UltraScale+ MPSoC Boot

> **FSBL (First Stage Boot Loader)**
  >> Configures Processing Subsystem (PS)
  >> Loads Partitions - Bitstream, ATF, U-boot, & RPU-Application

> **PMU(Platform Management Unit) Firmware**
  >> Provides Platform Management Services - Power Management, Restart, Safety, Error Management, PL Config

> **ATF (ARM Trusted Firmware)**
  >> Mandatory component of the ARMv8 security architecture

> **U-Boot**
  >> Universal Boot Loader, used by Linux Community

> **Linux / RPU-SW**
  >> Design specific Software layers on APU or RPU respectively

… Boot functions in order…
An Example - Understanding Boot Levels

... Boot has various dependencies...

- FSBL
- UBoot
- Linux
- Bitstream
- RPU (Lockstep mode)
- Tamper Monitoring (SEU, PS JTAG covered in Security Workshop)
- Load FSBL

PMU
CSU
RPU
APU
PL

Time
FPGA Configuration Manager

> Use Case
  >> Secure/Non-Secure Bitstream Download from Linux/U-Boot/RPU (See Security session)

> Two Components for FPGA Manager in PMU
  >> xilsecure – Provides an interface to access CSU resources (SHA3, AES, RSA engines)
  >> xilfpga – Provides an interface for configuring PL via PCAP (Processor Configuration Access Port) from the PS

> Summary
  >> Source available and up streamed to GitHub
  >> Runs as Secure Master
  >> Service can be used by A53 or R5 code
  >> IPI is used as interface for the API
  >> PMUFW uses xilfpga and xilsecure libraries to perform bitstream decryption, authentication and download

... Security is done during Configuration ...
Isolation Configuration

> Text and Tree Diagram applies to
  >> Power Management
  >> Warm Restart
  >> Safety

> Define Subsystems based on Use-case
  >> Subsystem Restart - Restarts the subsystem from a clean state without effecting the other active subsystems
  >> Subsystem idling is a function of idling of all components of a defined subsystem

> Subsystems can be defined in Vivado via isolation configuration menu

... Define a tree once in Vivado ... Info is shared with other tools ...
PMU: Xilinx & User Firmware

> PMU Firmware extends the PMU ROM functionality
  - Closely interacts with the PMU ROM as needed
  - SW Framework provided for management functions
    - For specialized applications may be customized for application specific tasks
  - Uses Inter-Processor Interrupts (IPI) standard to communicate with other on-chip Processors

> The home for critical platform management functions:
  - Power
  - Post boot (after initial CSU PL configuration) programmable logic configuration
  - Warm Restart
  - Functional Safety Software Test Library

> User Code – Xilinx provides framework
  - System error handling
  - High reliability code
  - ….

> Loaded in PMU RAM by CSU ROM / FSBL

… Many functions usable as-is …
Part 2 of 4:
Power Management

... Power state of shared peripherals managed centrally ...
Platform Management for Zynq UltraScale+ Devices

- Dedicated Platform Management interface
- Key component of the Xilinx Power Management Framework
  - Implements the core of EEMI architecture

... Platform Management is built around communication ...
Platform Management Software Stack

What is communicated ...

PMU knows “state” and provides central services to all ...
Power Off Suspend to DDR

> Power Advantage Tool lets you see the power of your design (ZCU102, ZCU106, ZCU111)

> Suspend to DDR retains DDR contents via self-refresh. Allows detecting resume by the return value of XPm_GetBootStatus.

> Power Off Suspend to DDR supports very low standby power designs

… The Power Off state suspends to a nice low standby power …
What Typical Power States are Available

> Wiki example demonstrates **Typical Power States**

("Dimmer"):

> PS Power States:

  >> Full Performance
  >> APU Hotplug Cores
  >> APU Frequency Scaling
  >> APU Suspend
  >> FPD Off
  >> RPU Suspend
  >> Deep Sleep
  >> Power Off Suspend

… Several PS Power States that require no coding …

<table>
<thead>
<tr>
<th>Use case / mA</th>
<th>2.5W</th>
<th>1.8W</th>
<th>1.6W</th>
<th>1.6W</th>
<th>0.4W</th>
<th>0.3W</th>
<th>35mW</th>
<th>3uW</th>
</tr>
</thead>
<tbody>
<tr>
<td>APU, Full Power Domain (FPD)</td>
<td>ON</td>
<td>ON</td>
<td>1-APU ON, FPD ON</td>
<td>1-APU ON, FPD ON</td>
<td>APU OFF, FPD ON</td>
<td>OFF</td>
<td>OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>RPU, Low Power Domain (LPD)</td>
<td>RS Active, LPD ON</td>
<td>RS Active, LPD ON</td>
<td>RS Active, LPD ON</td>
<td>RS Active, LPD ON</td>
<td>RS Active, LPD ON</td>
<td>RS Active, LPD ON</td>
<td>RS Off, LPD ON</td>
<td>OFF</td>
</tr>
<tr>
<td>PL Domain (PLD)</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>Battery Domain (BD)</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
</tr>
</tbody>
</table>
Part 3 of 4:
Warm Restart …
Warm Restart Manager

> **Use Case**
>   >> Independent PS/PL/APU/RPU sub-system restarts

> **Summary**
>   >> Enables independent sub-system restarts
>     - PMU is always alive and has access to control registers
>   >> IPI/WDT error triggers restart
>   >> PMU idles down peripherals and DMAs
>   >> Asserts reset to subsystem
>   >> Loads images
>     - Offloaded to resident FSBL in the case of full PS Restart
>   >> Releases resets

... Restart is typically used to recover from error states ...
… Warm Restart is similar to Boot, other processors unaffected …

Warm Restart Dependencies …
Part 4 of 4: Functional Safety …
Safety/Reliability

> **TMR Processors in PMU**
  >> Triple Modular Redundancy Voting Logic

> **Physical Diversity (R5 / PMU / CSU)**
  Synthesized to different frequency targets
  >> Different net lists
  >> Different areas
  >> Different layouts
  >> Different routing

> **ECC**
  >> ECC for PMU & CSU RAMs

> **Memory interleaving to avoid multi-bit error by SEUs (Single Event Upsets)**
  >> 8:1 interleaving reduces probability of multi-bit error to nil

> **Independent memories for Data and ECC**
  >> Separate address latches
  >> Reduces probability of address latch corruption resulting in bad data
  - Ex. Bad address for ECC data will result in “random” ECC for correct data

> **“Early” Separation of Clocks and Resets to Individual Cores**

... Redundancy for reliability...
Functional Safety Software Test Library (STL)

- Complements hardware safety features by increasing Diagnostic Coverage

- APIs execute periodically for coverage of random hardware failures
  - E.g., Register checking, Interconnect checking, Memory scrubbing etc.

- APIs execute on user demand for latent failure coverage
  - Ex: XMPU (Xilinx Memory Protection Unit), SysMon, error injection, etc.
  - Executes from: R5 and PMU

- Software Test Library Coverage
  - R5 Caches, TCMs & OCM
  - PMU RAM
  - Low Power Domain Interconnect/Switch
  - Peripherals: Ethernet, CAN & UART
  - System Monitor
  - LPD General Interrupt Controller
  - LPD DMA
  - LPD Watchdog Timer
  - Error injection into LPD memories & R5 lockstep
  - XMPU (Xilinx Memory Protection Unit), XPPU (Xilinx Peripheral Protection Unit)
  - LPD reset/clock controller, LPD TTC, PMU TMR (Triple Modular Redundancy)

... Periodic test where there is no hardware redundancy ...
The Trifecta of Embedded References

- SW: Software Developer's Guide (SDG = ug1137)
- Xilinx-specific: Embedded Design Tutorial (EDT = ug1209)

... Of the many documents... Best three to start with...
How to Estimate Power: Xilinx Power Estimator

- Xilinx Power Estimator (XPE)
  - Spreadsheet to model PS Power, etc.
  - Helps with power tradeoffs during the evaluation phase of your low power mode.
  - Fill out XPE, then discuss your design with a Xilinx FAE
  - Suggests Power Management Methodology

Download at https://www.xilinx.com/products/technology/power/xpe.html
EEMI: How Do We Control a Power Island

... PMU turns off any island when it is not in use ...
EEMI: How Do We Suspend a Processor

PMU communicates / performs requests to suspend...
Additional Security Features

- Key Revocation – Public Key Authentication
- Encrypt/Decrypt Algorithm Enhancement
- Key Agility
- Permanent Decryptor Disable
- Tamper Logging
- DPA Resistance
- Obfuscated Key Loading
- Key Readback Protections
- User Access to Crypto Functions
- Other Items…