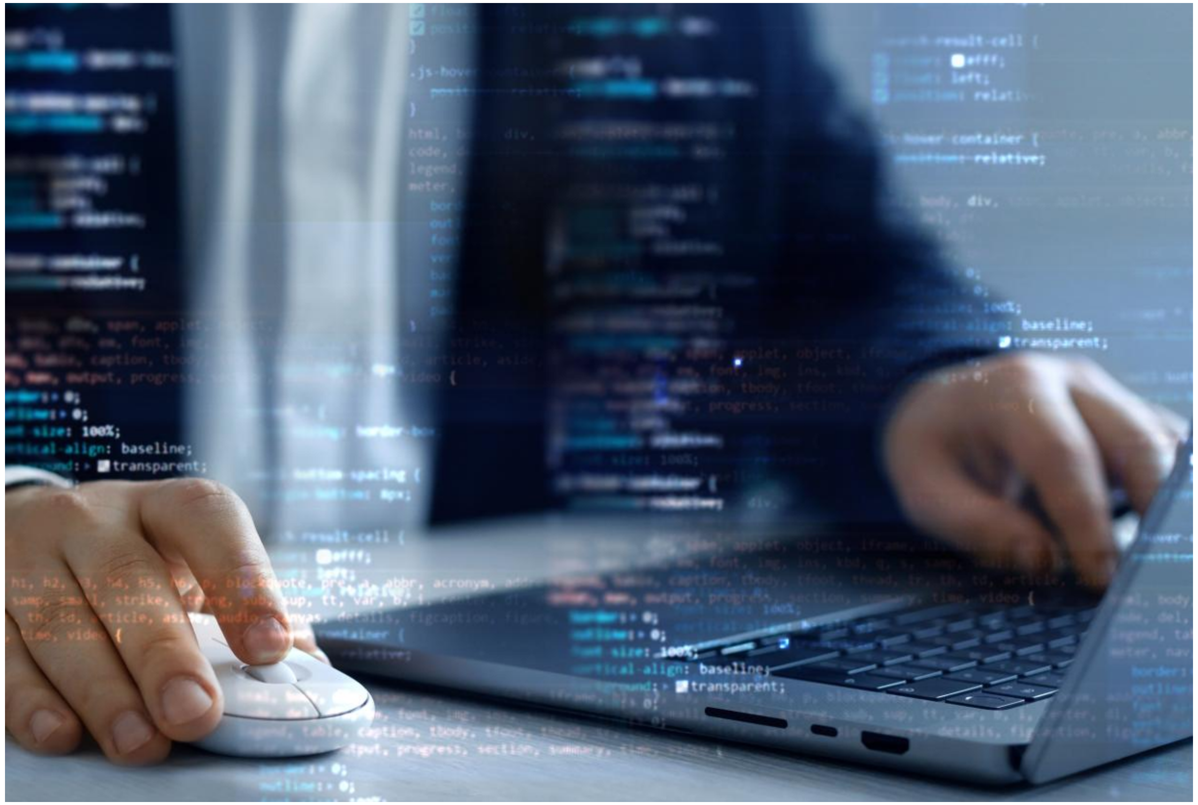
Configuration Flow for AMD Spartan™ UltraScale+™ Devices

AMD
together we advance_

Configuration Process

Configuration Fundamentals

FPGA configuration defines device functionality by loading a bitstream or Programmable Device Image (PDI) into volatile internal memory



Configuration is done after every power-up, requiring data storage in non-volatile memory like flash

FPGAs are highly flexible, allowing multiple in-system reprogramming via serial or parallel data paths, including JTAG

Uses full or partial bitstreams for reconfiguration

Supports self-configuration from external non-volatile memory or programming by external devices

[Public]

AMD Spartan™ UltraScale+™ FPGAs: Configuration Overview

Advanced configuration logic with dedicated platform management controller (PMC)

- **PMC** manages device boot, configuration, and security

AMD Spartan™ UltraScale+™ FPGA is configured using a programmable device image (PDI) file

- **PDI** replaces the legacy bitstream format from earlier FPGA families

After power-up, the PMC's BootROM firmware initiates configuration by loading the PDI via special configuration pins

Dedicated Platform Management Controller (PMC)

Acts as a Secure Configuration Engine, Orchestrating Power-up, PDI Loading, and Critical Security Functions

PMC Includes

- Configuration controller for running BootROM firmware
- I/O interfaces for config mode protocols
- Security module for cryptographic functions
- Configuration control unit (CCU) for programmable logic data

BootROM Responsibilities

- Samples configuration mode
- Sets up the registers for selected mode
- Validates PDI boot header
- Load and initiate Platform Loader Manager (PLM)

PLM Responsibilities

- Performs boot and config activities
- Program mode-specific registers and advanced settings
- Loads PDI (secure/non-secure)
- Supports full/partial reconfiguration

Enables comprehensive system health monitoring, and provides integrated power domain control, ultimately ensuring enhanced reliability, security, and flexibility for advanced applications

Configuration Sequence – Three Key Phases

Phase 1

Power-Up and Reset (**PMC Hardware**)

- PMC detects valid power
- PROGRAM_B release initiates configuration
- Mode pins (M[2:0]) are sampled to determine the configuration interface
- Cryptographic hash checks are performed to ensure integrity

Phase 2

Initialization and PLM Load (**BootROM**)

- Validates the PDI structure
- Reads configuration mode settings from the mode register
- Loads the PLM firmware into PMC RAM
- If the primary image is invalid, a fallback mechanism searches for a backup image

Phase 3

PDI Image Processing and Configuration (**PLM**)

- Parses and processes PDI
- Executes full or partial configuration into PL
- PL starts up
- Asserts the DONE pin to signal successful configuration and readiness

Configuration Interfaces

Mode selected via M[2:0] pins

M[2:0] pin values must be stable before PROGRAM_B initiates the configuration process upon deassertion

PMC samples M[2:0] during Phase 1 power-up

Selected mode captured at power-up, maintained through initialization

AMD Spartan™ UltraScale+™ FPGAs have five configuration modes

S.No.	Configuration Mode	M[2:0]	Description
1	**JTAG**	101	Used for direct programming and debugging via a JTAG cable
2	**Master SPI_24**	001	FPGA self-configures from an external SPI NOR flash, acting as master to read its configuration, and supports 24-bit (up to 128 Mb) or 32-bit (greater than 128 Mb) addressing
	Master SPI_32	010	
3	**Master OSPI**	011	Uses an external Octal SPI 8-bit wide bus for faster configuration
4	**Slave SelectMAP**	110	External processor configures FPGA in parallel (8/16/32-bit)
5	**Slave Serial**	111	External source sends configuration serially, one bit at a time

Configuration Mode - Design Considerations

Choosing the optimal configuration mode is crucial for efficient system design. Configuration modes can impact:

- **Pin Allocation**
- **I/O Bank Voltage Requirements**
- **System Costs**

Recommended Design Flow and Configuration Factors

01

Determine the optimal configuration mode early in the design cycle based on system characteristics

02

Utilize JTAG as an additional mode specifically for debugging

03

Plan for multi-function pins used during configuration to prevent conflicts

04

Ensure quality signal integrity for key signals during PCB layout

05

Consider all aspects of the configuration sequence to reduce configuration time, including power-up time

06

Generate the configuration PDI using the latest AMD tools, targeting the correct device version

For more information refer to Design Consideration and PCB Design section

Differences between AMD UltraScale™/UltraScale+™ & Spartan™ UltraScale+

Feature / Aspect	AMD UltraScale™/ UltraScale+ FPGAs	Spartan™ UltraScale+™ FPGAs
• **Primary Configuration Manager**	Dedicated configuration engine	Platform Management Controller (PMC)
• **Configuration Format**	Bitstream (.bit)	Programmable Device Image (.PDI)
• **Standard Modes**	JTAG, Master/Slave Serial, Master/Slave SelectMAP, and PCIe (variants)	JTAG, Master SPI (x1, x2, x4), Master OSPI, Slave Serial, Slave SelectMAP, and PCIe (variants)
• **Fallback Mechanism**	Jumps to address 0x00000000 where the golden image is stored	BootROM automatically jumps to the next 32 KB address and attempts to search for the signature
• **Security**	Optional encryption/authentication (often manual/external control)	Built-in secure boot capabilities, hardware root of trust, and automated PDI validation via PMC
• **Reconfiguration**	Typically, via ICAP or PCAP; may require manual setup	PMC-managed dynamic reconfiguration (simpler setup)
• **Application Suitability**	General-purpose FPGA applications	More suitable for modern, secure, and flexible applications due to enhanced management and security features at the edge

AMD

Programmable Device Image (PDI)

Programmable Device Image (PDI) Overview

Modern configuration format for newer AMD Spartan™ UltraScale+™ FPGAs and Versal devices, replacing traditional bitstreams

Unlike monolithic bitstreams, PDI is a containerized format supporting multiple partitions (config data, firmware, metadata, and security headers)

Bitstream

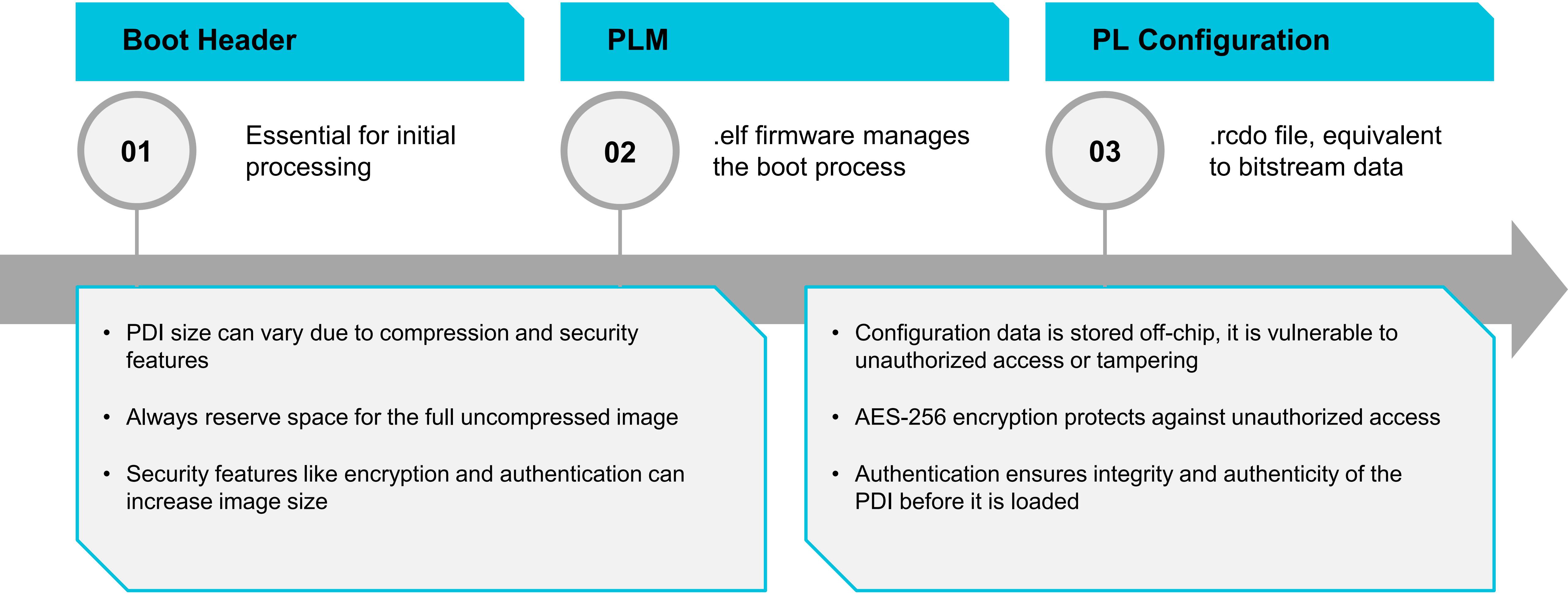
- Is directly loaded into logic
- Lacks advanced boot/security

Programmable Device Image (PDI)

- Is processed by the PMC for multi-phase boot, including:
  - Validation
  - Decryption
  - Fallback
- PDI format is inherently more robust, secure, and flexible

PDI Format

AMD Spartan™ UltraScale+™ FPGAs use a PDI format for boot and configuration. A typical PDI includes:



Boot Header

01 Essential for initial processing

PLM

02 .elf firmware manages the boot process

PL Configuration

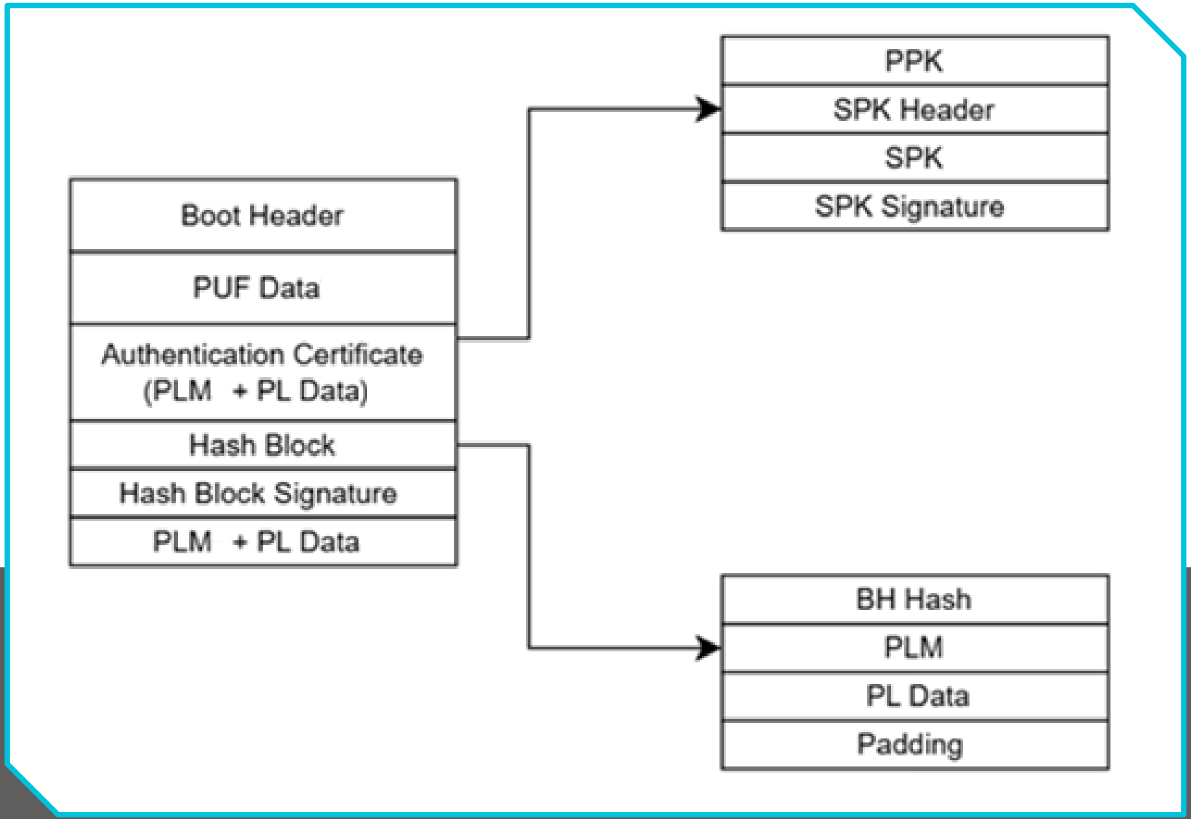
03 .rcdo file, equivalent to bitstream data

- PDI size can vary due to compression and security features
- Always reserve space for the full uncompressed image
- Security features like encryption and authentication can increase image size

- Configuration data is stored off-chip, it is vulnerable to unauthorized access or tampering
- AES-256 encryption protects against unauthorized access
- Authentication ensures integrity and authenticity of the PDI before it is loaded

[Public]

PDI Format



- Boot header
- PLM (.elf)

- PL configuration (.rcdo)
- Hash block for integrity checks

- PUF helper data (unique per device)

- Public keys (SPK/PPK)
- Stored in a separate PDI

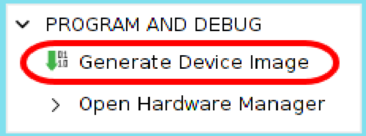
Generating the PDI in AMD Spartan™ UltraScale+™ FPAGs

AMD Vivado™ Project Mode

To produce a complete PDI in the run directory:

GUI Mode

In the Flow Navigator, click **Generate Device Image**



OR

Tcl Mode

Execute
launch_runs -to_step write_bitstream

Vivado Non-Project Mode

1. Run the ***write_bitstream*** Tcl command → *Generates .bit, .bif, and other bootgen inputs*
2. *In a new terminal window within same directory as .bif file* → Execute
   bootgen -image <bif_file>.bif -arch spartanuplus -o <pdi_name>.pdi

AMD

Debugging and Security

Error Management

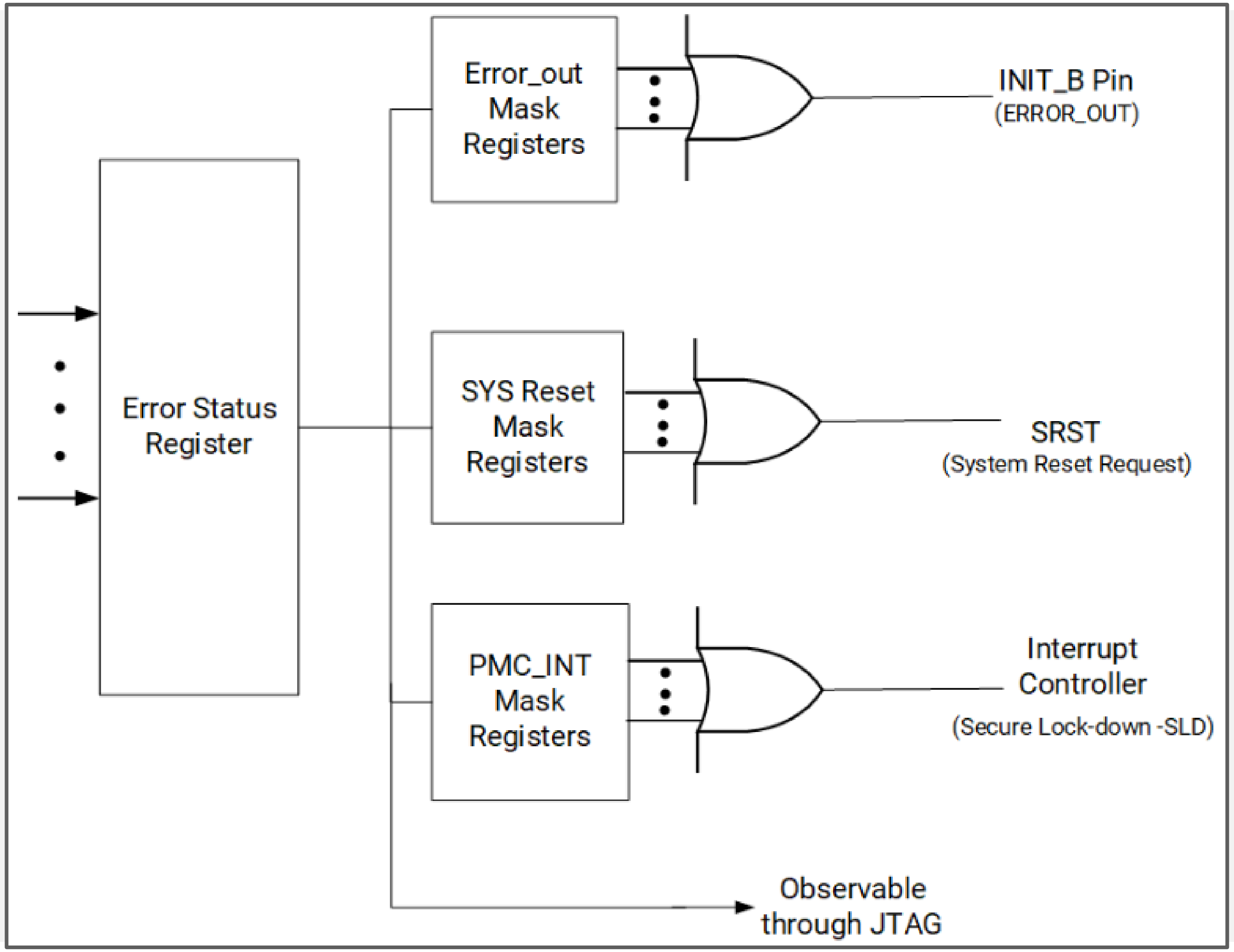
1 Error Aggregation Module (EAM) available that combines specified errors

2 Allows the users to respond to specified error conditions

3 Three responses for handling the non-masked errors:

- Assert INIT_B pin low
- Issue a system reset (SRST) or
- Issue an interrupt that enters the secure lock-down (SLD) state

4 PLM allows for one option response on each error specified



For more information on bootROM and PLM error codes refer to Error Management section

Configuration Debugging Techniques

Effective debugging during configuration is essential to identify and resolve issues quickly

PDI Options Verification

- Verify PDI properties & flash programming options
- Use `report_property -all [current_design]`
- Review and fix all DRC warnings

Physical Status Pins

- Monitor **INIT_B** for initialization/CRC status
- Check **DONE** for successful config

JTAG Registers

- Access JTAG registers for valuable debug data
- Use registers like IDCODE, JTAG_STATUS, ERROR_STATUS, FW_STATUS

Basic Checks

- Verify PDI (Confirm XLNX signature in boot header)
- Try alternate mode (JTAG) or known-good PDI
- Lower config clock if needed
- Minimize non-default PDI options
- Verify data reception and tool version

State-of-the-art Security Features

Protect Your IP

- **PQC** with NIST-approved algorithms
- **AES-GCM** for secure configuration
- **PUF** for unique device identification and improved physical security

Prevent Tampering

- **Customizable Tamper Responses** incl. permanent penalty to protect the device against misuse
- **DPA** countermeasures for side-channel attacks

Maximize Uptime

- Enhanced **SEU** performance for increased reliability

Offering the advanced security features for AMD Spartan™ UltraScale+™ FPGAs

AMD Spartan™ UltraScale+™ FPGA Security: Pre-configuration

Passive Features	AMD Spartan™ 6	7 Series	AMD UltraScale™/ UltraScale+™	AMD Spartan UltraScale+
Confidentiality w/ AES-256	✓	✓	✓ GCM	✓ GCM
Symmetric Key Authentication		✓	✓ GCM	✓ GCM
Hardened Readback Disable	✓	✓	✓	✓
Public Key (Asymmetric) Authentication			✓	✓
Root of Trust – Replay Protection; Anti-Rollback features			✓ Root of Trust	✓
Differential Power Analysis (DPA) Resistant			✓	✓
Black / Obfuscated Key Load			✓ Obfuscated Key	✓
Post-Quantum Cryptography (PQC)				✓
Primary/Secondary Public Keys				✓
Encrypted Key Storage (PUF)				✓

AMD Spartan™ UltraScale+™ FPGA Security: Post-configuration

Passive Features	AMD Spartan™ 6	7 Series	AMD UltraScale™/ UltraScale+™	AMD Spartan UltraScale+
Single Event Upset (SEU) Checking	✓	✓	✓	✓
JTAG Disable/Monitor (BSCAN)	✓	✓	✓	✓
Unique Identifier (Device DNA)	✓	✓	✓	✓
Unique Identifier (User eFUSE)		✓	✓	✓
On-Chip Temperature/Voltage Monitors		✓	✓	✓
PROGRAM_B Intercept		✓	✓	✓
Tamper Event Logging			✓	✓
Permanent JTAG Disable			✓	✓
Permanent Decryptor Disable			✓	✓
Permanent Tamper Penalty			✓	✓
Physical Unclonable Function (PUF)				✓
True Random Number Generator (TRNG)				✓
User Access to Hard Crypto Engines				✓

Summary

AMD Spartan™ UltraScale+™ FPGAs utilize a new configuration architecture driven by the platform management controller (PMC) and the programmable device image (PDI)

The PDI is the comprehensive programming file, featuring enhanced security and loaded via diverse configuration modes like JTAG, SPI, or SelectMAP

Device configuration follows a distinct three-phase sequence, managed by the PMC's BootROM and platform loader manager (PLM)

For more information on the configuration flow, refer to the Spartan UltraScale+ FPGAs Configuration User Guide (UG860)

DISCLAIMER AND ATTRIBUTIONS

The information contained herein is for informational purposes only and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale. GD-18u.

Certain AMD technologies may require third-party enablement or activation. Supported features may vary by operating system. Please confirm with the system manufacturer for specific features. No technology or product can be completely secure.

AMD