Manufacturing and Life Cycle Management Concerns
Privilege Separation and Access Control Issues
Power, Clock, Thermal, and Reset Concerns
Security Primitives and Cryptography Issues
Physical Access Issues and Concerns
Memory and Storage Issues
Debug and Test Problems
Cross-Cutting Problems
Security Flow Issues
Integration Issues

Improper Access Control Applied to Mirrored or Aliased Memory Regions
Hardware Logic with Insecure De-Synchronization between Control and Power-On of Untrusted Execution Core Before Enabling Fabric Access
Unprotected Confidential Information on Device is Accessible by OSAT
Improper Scrubbing of Sensitive Data from Decommissioned Device
Improper Handling of Overlap Between Protected Memory Ranges
Sensitive Information Uncleared Before Debug/Power State Transition
Cryptographic Operations are run Before Supporting Units are Ready
Exposure of Sensitive System Information Due to Uncleared Debug
Improperly Preserved Integrity of Hardware Configuration State During Public Key Re-Use for Signing both Debug and Production Code
Security-Sensitive Hardware Controls with Missing Lock Bit Protection
Improper Access Control for Volatile Memory Containing Boot Code
Improper Isolation of Shared Resources in Network On Chip (NoC)
CPU Hardware Not Configured to Support Exclusivity of Write and On-Chip Debug and Test Interface With Improper Access Control
Missing Support for Security Features in On-chip Fabrics or Buses
Improper Protection against Electromagnetic Fault Injection (EM-FI)
Improper Setting of Bus Controlling Capability in Fabric End-point
Improperly Preserved Integrity of Hardware Configuration State During Security-Sensitive Hardware Controls with Missing Lock Bit Protection

Exposure of Sensitive Information during Transient Execution
Use of a Cryptographic Primitive with a Risky Implementation
Improper Write Handling in Limited-write Non-Volatile Memories
Use of Predictable Algorithm in Random Number Generator
Hardware Internal or Debug Modes Allow Override of Locks
Improperly Preserved Integrity of Hardware Configuration State During Security-Sensitive Hardware Controls with Missing Lock Bit Protection
Non-Transparent Sharing of Microarchitectural Resources
Improper Lock Behavior After Power State Transition
Improperly Preserved Integrity of Hardware Configuration State During Security-Sensitive Hardware Controls with Missing Lock Bit Protection
Improperly Preserved Integrity of Hardware Configuration State During Security-Sensitive Hardware Controls with Missing Lock Bit Protection

Unintended Proxy or Intermediary ('Confused Deputy')
Inclusion of Undocumented Features or Chicken Bits
Expected Behavior Violation
Reliance on Component That is Not Updateable
Improper Management of Sensitive Trace Data
Security Version Number Mutable to Older Versions
Reliance on Insufficiently Trustworthy Component

Assumed-Immutable Data is Stored in Writable Memory
Mutable Attestation or Measurement Reporting Data
Security Version Number Mutable to Older Versions
Improper Protection Against Voltage and Clock Glitches
Incorrect Selection of Fuse Values
Firmware Not Updateable
Incorrect Default Permissions
Expected Behavior Violation

Integrated Circuit (IC) Imaging Techniques
Protected and Unprotected Ranges
Representations of Shared State
Data Channels
Environments
Data Agents
Vendors (SOC)

Exposure of Sensitive Information caused by Incorrect Data Forwarding
Exposure of Sensitive Information caused by Shared Microarchitectural Structures during Transient Execution
Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
Improper Restriction of Security Token Assignment
Improper Zeroization of Hardware Register
Predictor State that Influences Transient Execution
Incorrect Comparison Logic Granularity
Incorrect Selection of Fuse Values
Incorrect Default Permissions
Expected Behavior Violation

Incorrect Default Permissions
Expected Behavior Violation

Expected Behavior Violation