1059 - Peripherals, On-chip Fabric, and Interface/I/O Problems
1311 - Improper Translation of Security Attributes by Fabric Bridge
1312 - Missing Protection for Mismatched Regions in On-Chip Fabric Firewall
1315 - Improper Setting of Bus Controlling Capability in Fabric Endpoint
1316 - Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges
1317 - Improper Access Control in Fabric Bridge
1331 - Improper Isolation of Shared Resources in Network On-Chip (NoC)
1197 - Integration Issues
1278 - Hardware Child Block Incorrectly Connected to Parent System
1201 - Core and Compute Issues
1052 - CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations
1281 - Sequence of Processor Instructions Leads to Unexpected Behavior
1240 - Improper Write Handling in Limited-write Non-Volatile Memories
1051 - Mirrored Regions with Different Values
1050 - Memory and Storage Issues
1247 - Improper Access Control Applied to Mirrored or Aliased Memory Regions
1082 - Assumed-Immutable Data is Stored in Writable Memory
226 - Sensitive Information in Resource Not Removed Before Reuse
1240 - Information Exposure through Microarchitectural State after Transient Execution
1039 - Improper Zeroization of Hardware Register
1196 - Security Flow Issues
1196 - DMA Devices Enabled Too Early in Boot Phase
1193 - Power-On of Untrusted Execution Core Before Enabling Fabric Access Control
1384 - Hardware Logic with Insecure De-Synchronization between Control and Data Channels
1274 - Improper Access Control for Volatile Memory Containing Boot Code
1193 - Mutable Attestation or Measurement Reporting Data
1310 - Missing Ability to Patch ROM Code
1326 - Missing Immutable Root of Trust in Hardware
1328 - Security Version Number Mutable to Older Versions
1199 - General Circuit and Logic Design Concerns
1245 - Improper Finite State Machines (FSMs) in Hardware Logic
1250 - Improper Preservation of Consistency Between Independent Representations of Shared State
1332 - Incorrect Selection of Fuse Values
1334 - Incorrect Comparison Logic Granularity
1298 - Hardware Logic Contains Race Conditions
1339 - Failure to Disable Reserved Bits
1221 - Incorrect Register Defaults or Module Parameters
1223 - Race Condition for Write-Once Attributes
1224 - Improper Restriction of Write-Once Bit Fields
1231 - Improper Prevention of Lock Bit Modification
1233 - Security-Sensitive Hardware Controls with Missing Lock Bit Protection
1234 - Hardware Internal or Debug Modes Allow Override of Locks
1273 - Sensitive Information Uncleared Before Debug/Power State Transition
1291 - Public-Key Re-Use for Signing both Debug and Production Code
1081 - Improper Handling of Single-Event Upsets
1295 - Debug Messages Revealing Unnecessary Information
1084 - Incorrect Chaining or Granularity of Debug Components
1313 - Hardware Allows Activation of Test or Debug Logic at Runtime
1037 - Debug and Test Problems
1053 - Improper Management of Sensitive Trace Data
219 - Cleartext Transmission of Sensitive Information
1191 - On-Chip Debug and Test Interface With Improper Access Control
1243 - Sensitive Non-Volatile Information Not Protected During Debug
1244 - Internal Asset Exposed to Unsafe Debug Access Level or State
1258 - Exposure of Sensitive System Information Due to Unclosed Debug Information
1319 - Improper Protection against Electromagnetic Fault Injection (EM FI)
1384 - Improper Handling of Physical or Environmental Conditions
1178 - Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques
1389 - Physical Access Issues and Concerns
1191 - Improper Handling of Hardware Behavior in Exceptionally Cold Environments
1232 - Improper Lock Behavior After Power State Transition
1320 - Improper Handling of Faults that Lead to Instruction Skips
1247 - Improper Protection Against Voltage and Clock Glitches
1300 - Improper Protection of Physical Side Channels
203 - Observable Discrepancy
1035 - Security Primitives and Cryptography Issues
1348 - Comparison Logic is Vulnerable to Power Side-Channel Attacks
1240 - Use of a Cryptographic Primitive with a Risky Implementation
1241 - Use of Predictable Algorithm in Random Number Generator
1279 - Cryptographic Operations are run Before Supporting Units are Ready
325 - Missing Cryptographic Step
1326 - Improper Protection for Outbound Error Messages and Alert Signals
1206 - Power, Clock, Thermal, and Reset Concerns
1338 - Improper Protections Against Hardware Overheating
1334 - Improper Restriction of Software Interfaces to Hardware Features
1248 - Semiconductor Defects in Hardware Logic with Security-Sensitive Implications
1271 - Uninitialized Value on Reset for Registers Holding Security Settings
1304 - Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation
640 - Expected Behavior Violation
1053 - Missing Documentation for Design
1214 - Missing Write Protection for Parametric Data Values
1263 - Improper Physical Access Control
1277 - Firmware Not Updateable
1039 - Cross-Cutting Problems
1301 - Insufficient or Incomplete Data Removal within Hardware Component
1330 - Remanent Data Readable after Memory Erase
1329 - Reliance on Component That is Not Updateable
1357 - Reliance on Insufficiently Trustworthy Component
1092 - Improper Access Control for Register Interface
1267 - Policy Uses Obsolete Encoding
1298 - Policy Privileges are not Assigned Consistently Between Control and Data Agents
1290 - Access Control Check Implemented After Asset is Accessed
1384 - Insecure Security Identifier Mechanism
1052 - Incorrect Conversion of Security Identifiers
1059 - Improper Restriction of Security Token Assignment
1270 - Generation of Incorrect Security Tokens
1340 - Incorrect Decoding of Security Identifiers
1218 - Missing Support for Security Features in On-chip Fabrics or Buses
1324 - Unauthorized Error Injection Can Degrade Hardware Redundancy
1198 - Privilege Separation and Access Control Issues
276 - Incorrect Default Permissions
441 - Unintended Proxy or Intermediary ("Confused Deputy")
1394 - Missing Protection Mechanism for Alternate Hardware Interface
1302 - Missing Security Identifier
1303 - Non-Transparent Sharing of Microarchitectural Resources
1189 - Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
1193 - System-on-Chip (SoC) Using Components without Unique, Immutable Identifiers
1203 - Insufficient Granularity of Access Control
1228 - Insufficient Granularity of Address Regions Protected by Register Locks
1242 - Inclusion of Undocumented Features or Chicken Bits
1360 - Improper Handling of Overlap Between Protected Memory Ranges
1059 - Insufficient Technical Documentation
1196 - Manufacturing and Life Cycle Management Concerns
1387 - Unprotected Confidential Information on Device is Accessible by OSAT Vendors
1386 - Improper Scrubbing of Sensitive Data from Decommissioned Device
1369 - Product Released in Non-Release Configuration
1373 - Device Unlock Credential Sharing