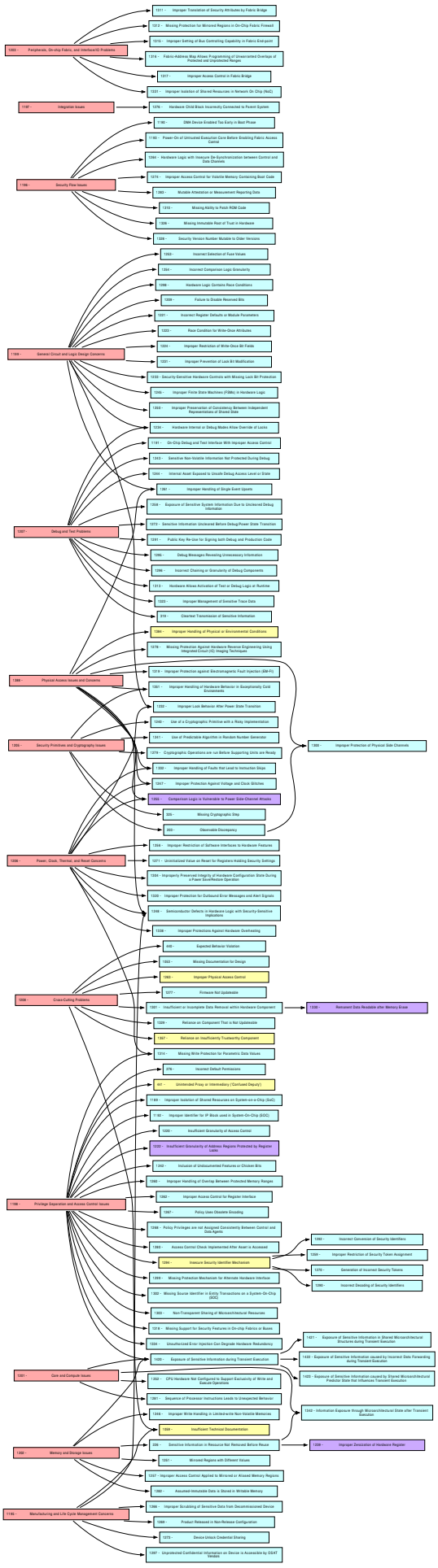
1003 - Peripherals, On-chip Fabric, and Interface/IO Problems
1317 - Improper Translation of Security Attributes by Fabric Bridge
1312 - Missing Protection for Mirrored Regions in On-Chip Fabric Firewall
1315 - Improper Setting of Bus Controlling Capability in Fabric End-point
1318 - Fabric-Address Map 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)
1187 - Integration Issues
1276 - Hardware Child Block Incorrectly Connected to Parent System
1199 - Security Flow Issues
1186 - DMA Device Enabled Too Early in Boot Phase
1193 - Power-On of Untrusted Execution Core Before Enabling Fabric Access Control
1244 - Hardware Logic with Insecure De-Synchronization between Control and Data Channels
1274 - Improper Access Control for Volatile Memory Containing Boot Code
1283 - Mutable Attestation or Measurement Reporting Data
1319 - Missing Ability to Patch ROM Code
1326 - Missing Immutable Root of Trust in Hardware
1329 - Security Version Number Mutable to Older Versions
1198 - General Circuit and Logic Design Concerns
1250 - Incorrect Selection of Fuse Values
1284 - Incorrect Comparison Logic Granularity
1298 - Hardware Logic Contains Race Conditions
1299 - Failure to Disable Reserved Bits
1221 - Incorrect Register Defaults or Module Parameters
1232 - Race Condition for Write-Once Attributes
1234 - Improper Restriction of Write-Once Bit Fields
1231 - Improper Prevention of Lock Bit Modification
1195 - Security-Sensitive Hardware Controls with Missing Lock Bit Protection
1245 - Improper Finite State Machines (FSMs) in Hardware Logic
1253 - Improper Preservation of Consistency Between Independent Representations of Shared State
1256 - Hardware Internal or Debug Modes Allow Override of Locks
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
1397 - Improper Handling of Single-Event Upsets
1258 - Exposure of Sensitive System Information Due to Uncleared Debug Information
1272 - Sensitive Information Uncleared Before Debug/Power State Transition
1191 - Public Key Re-use for Signing both Debug and Production Code
1295 - Debug Messages Revealing Unnecessary Information
1296 - Incorrect Chaining or Granularity of Debug Components
1313 - Hardware Allows Activation of Test or Debug-Logic at Runtime
1323 - Improper Management of Sensitive Trace Data
319 - Cleartext Transmission of Sensitive Information
1384 - Improper Handling of Physical or Environmental Conditions
1278 - Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques
1399 - Physical Access Issues and Controls
1314 - Improper Protection against Electromagnetic Fault Injection (EM-FI)
1391 - Improper Handling of Hardware Behavior in Exceptionally Cold Environments
1222 - Improper Lock Behavior After Power State Transition
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
1332 - Improper Handling of Faults that Lead to Instruction Skips
1247 - Improper Protection Against Voltage and Clock Glitches
1300 - Improper Protection of Physical Side Channels
1254 - Comparison Logic is Vulnerable to Power Side-Channel Attacks
305 - Missing Cryptographic Step
203 - Observable Discrepancy
1205 - Security Primitives and Cryptography Issues
1206 - Power, Clock, Thermal, and Reset Concerns
1304 - Improper Restriction of Software Interfaces to Hardware Features
1271 - Uninitialized Value on Reset for Registers Holding Security Settings
1394 - Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation
1320 - Improper Protection for Outbound Error Messages and Alert Signals
1398 - Semiconductor Defects in Hardware Logic with Security-Sensitive Implications
1338 - Improper Protections Against Hardware Overheating
402 - Expected Behavior Violation
1053 - Missing Documentation for Design
1400 - Improper Physical Access Control
1277 - Firmware Not Updatable
1008 - Crypto Quality Problems
1301 - Insufficient or Incomplete Data Removal within Hardware Component
1330 - Recovered Data Readable after Memory Erase
1329 - Reliance on Component That is Not Updateable
1307 - Reliance on Insufficiently Trustworthy Component
1314 - Missing Write Protection for Parametric Data Values
276 - Incorrect Default Permissions
441 - Unintended Proxy or Intermediary ('Confused Deputy')
1189 - Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
1192 - Improper Identifier for IP Block used in System-On-Chip (SOC)
1205 - Insufficient Granularity of Access Control
1022 - Insufficient Granularity of Address Regions Protected by Register Locks
1402 - Inclusion of Undocumented Features or Chicken Bits
1386 - Improper Handling of Overlap Between Protected Memory Ranges
1190 - Privilege Escalation and Access Control Issues
1282 - Improper Access Control for Register Interface
1267 - Policy Uses Obsolete Encoding
1246 - Policy Privileges are not Assigned Consistently Between Control and Data Agents
1260 - Access Control Check Implemented After Asset is Accessed
1294 - Insecure Security Identifier Mechanism
1262 - Incorrect Conversion of Security Identifiers
1289 - Improper Restriction of Security Token Assignment
1270 - Generation of Incorrect Security Tokens
1290 - Incorrect Decoding of Security Identifiers
1303 - Missing Protection Mechanism for Alternate Hardware Interface
1350 - Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC)
1303 - Non-Transparent Sharing of Microarchitectural Resources
1318 - Missing Support for Security Features in On-chip Fabrics or Buses
1334 - Unauthorized Error Injection Can Degrade Hardware Redundancy
1420 - Exposure of Sensitive Information during Transient Execution
1421 - Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
1422 - Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution
1423 - Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution
1342 - Information Exposure through Microarchitectural State after Transient Execution
1351 - Core and Compute Issues
1352 - CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations
1261 - Sequence of Processor Instructions Leads to Unexpected Behavior
1416 - Improper Write Handling in Limited-write Non-Volatile Memories
1359 - Insufficient Technical Documentation
1358 - Improper Zeroization of Hardware Register
1290 - Memory and Storage Issues
299 - Sensitive Information in Resource Not Removed Before Reuse
1251 - Mirrored Regions with Different Values
1337 - Improper Access Control Applied to Mirrored or Aliased Memory Regions
1282 - Assumed-Immutable Data is Stored in Writable Memory
1386 - Improper Scrubbing of Sensitive Data from Decommissioned Device
1145 - Manufacturing and Life Cycle Management Concerns
1389 - Product Released in Non-Release Configuration
1273 - Device Unique Credential Sharing
1297 - Unprotected Confidential Information on Device is Accessible by OSAT Vendors