2024 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION JAPAN

Security Annotation for Electronic Design Integration

Akio Mitsuhashi, EE Tech Focus

EE Tech Focus

accellera SYSTEMS INITIATIVE

Agenda

- IEEE P3164 Background and Introduction
- Problem Statement
- Asset Identification

IEEE P3164
Background and Introduction

Cyber Attack Trend

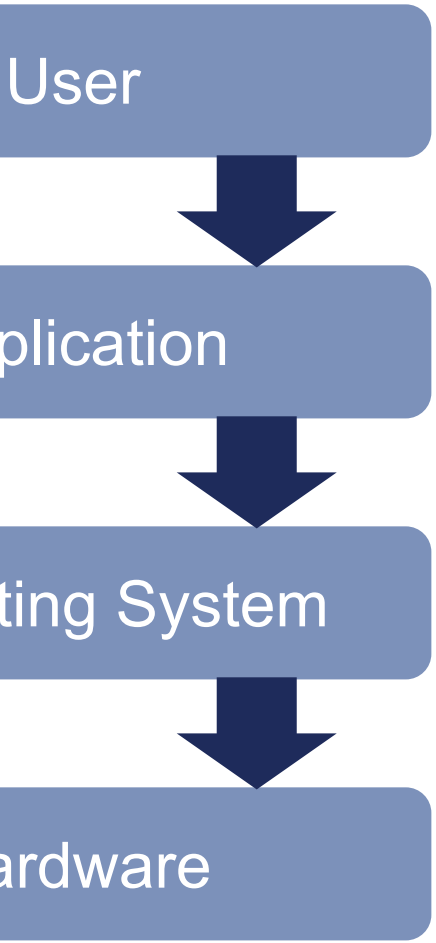
Impact

1～100

10,000～100,000

～100,000,000

～100,000,000

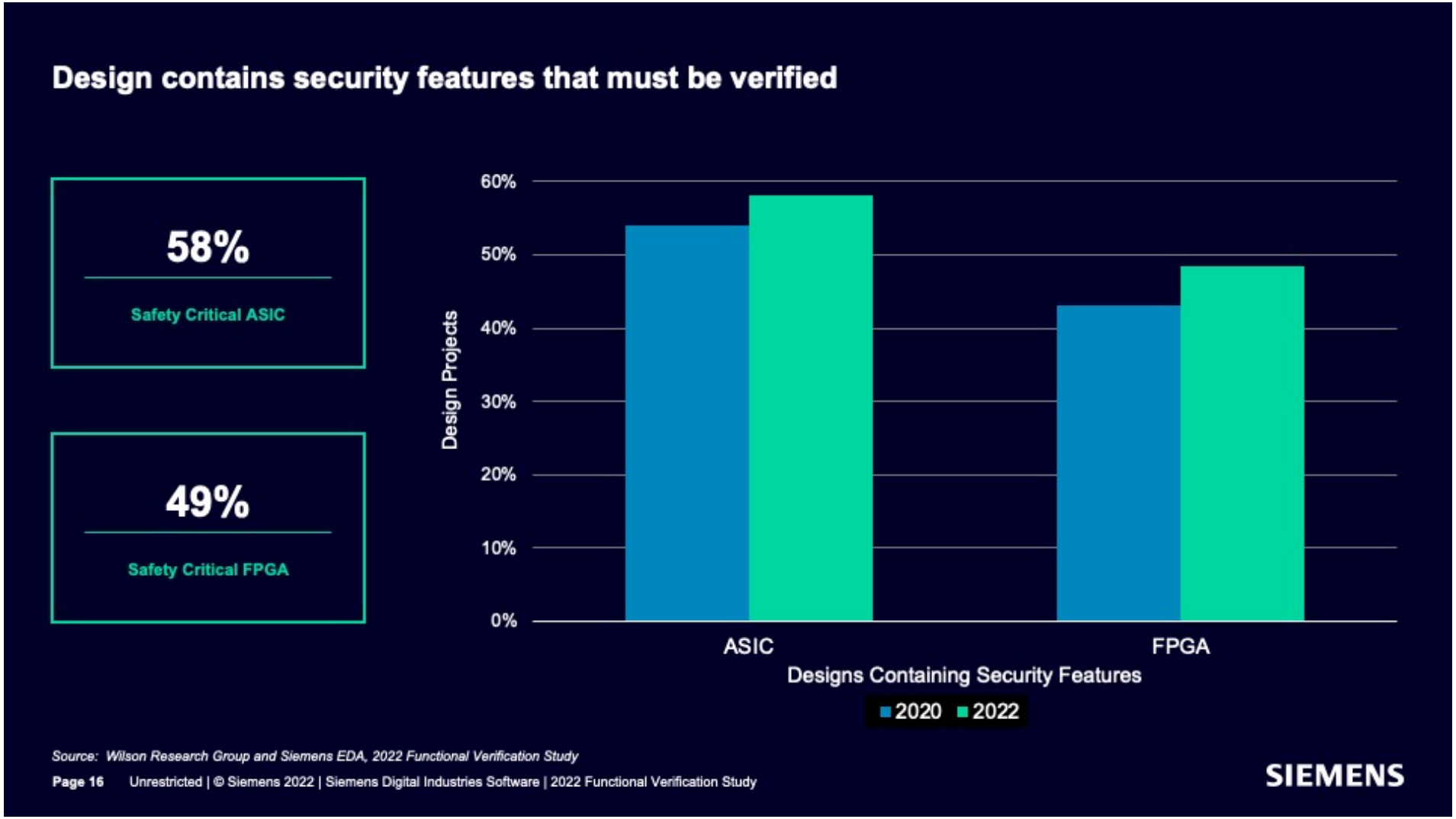


Procide Services

Root Of Trust

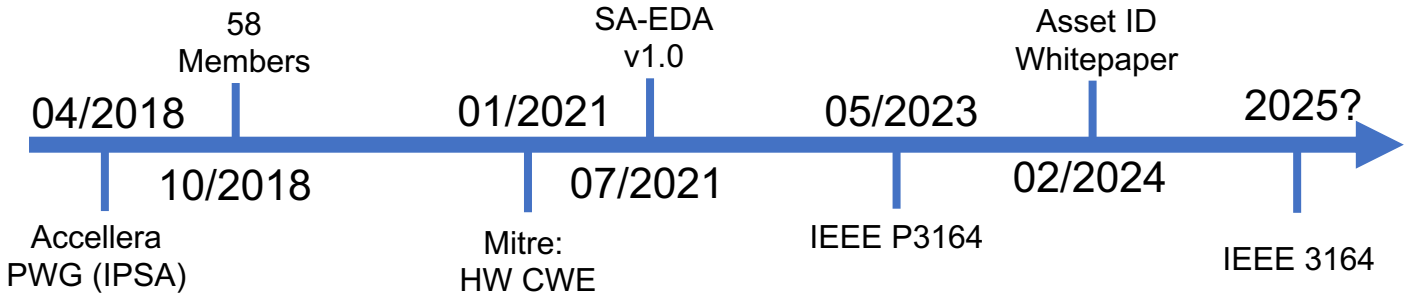
Source: "Understanding Integrated Circuit Security Threats" at MITsdm

Wilson Research Study - 2022



Accellera SA-EDI Standard

- Released July 2021
  - 21 authors, 11 companies
- Properties:
  - Uses JSON data modeling
    - Required fields helps consistency
    - Expansion supported for proprietary information
  - Binds the data objets to the RTL
    - Automatable and verifiable
  - Outside the design
    - Can be applied to existing IP
  - Low Overhead
    - Only 4 data object types



Problem Statement

Why was SA-EDI Needed ?

- No standard mechanism to bind security assurance (SA) collateral to an IP
  - Missing verification of SA
- Unable to perform any data mining (e.g. common threts, security objectives, etc)
- Lacking consistent quality in SA collateral
  - Different IP providers produce different collateral/formats (e.g. doc, ppt, pdf, xls, etc.)

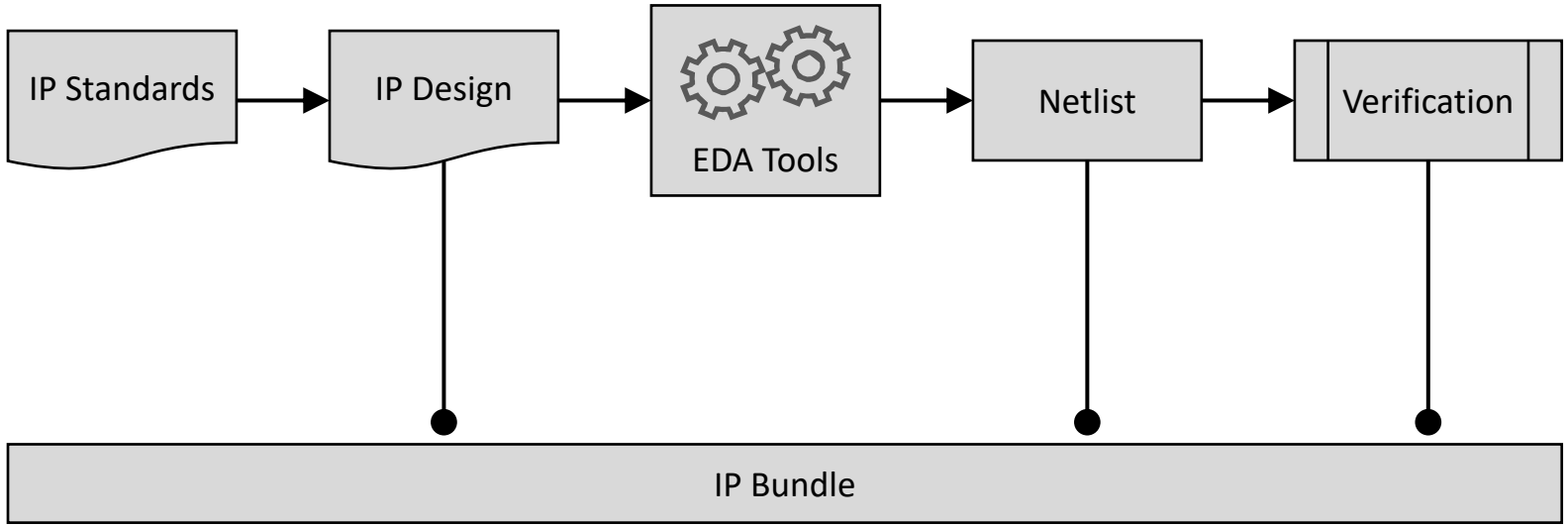
Shared Responsibility

- IP Provider ensures functional and implementation correctness
  - Expectations from integrator: No bugs (functional or security) in IP will be discovered once the IP has been delivered - not always true

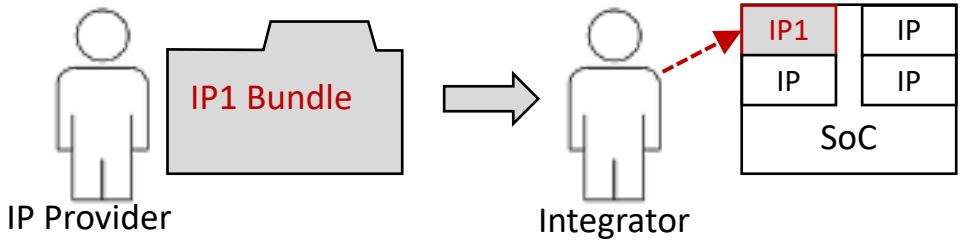
- Integrator endures configuration and connection are correct
  - Expectations from IP provider: Integrator will follow integration guidelines to ensure IP propert functionality - mostly true

What about security ??

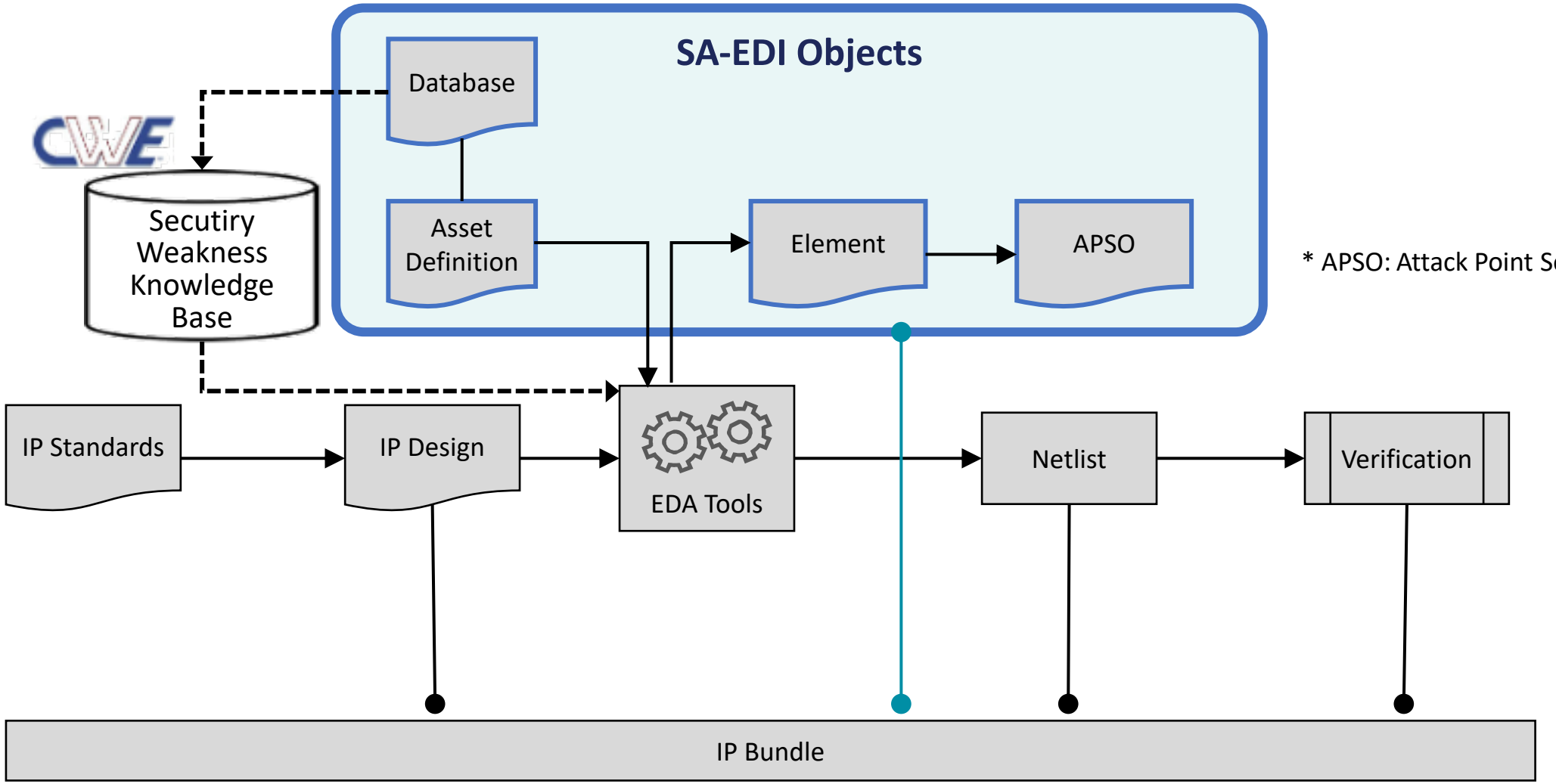
Today’s Typical IP design flow



6:42



SA-EDI Data Objects Describe Security Properties of IP



* APSO: Attack Point Security Objective

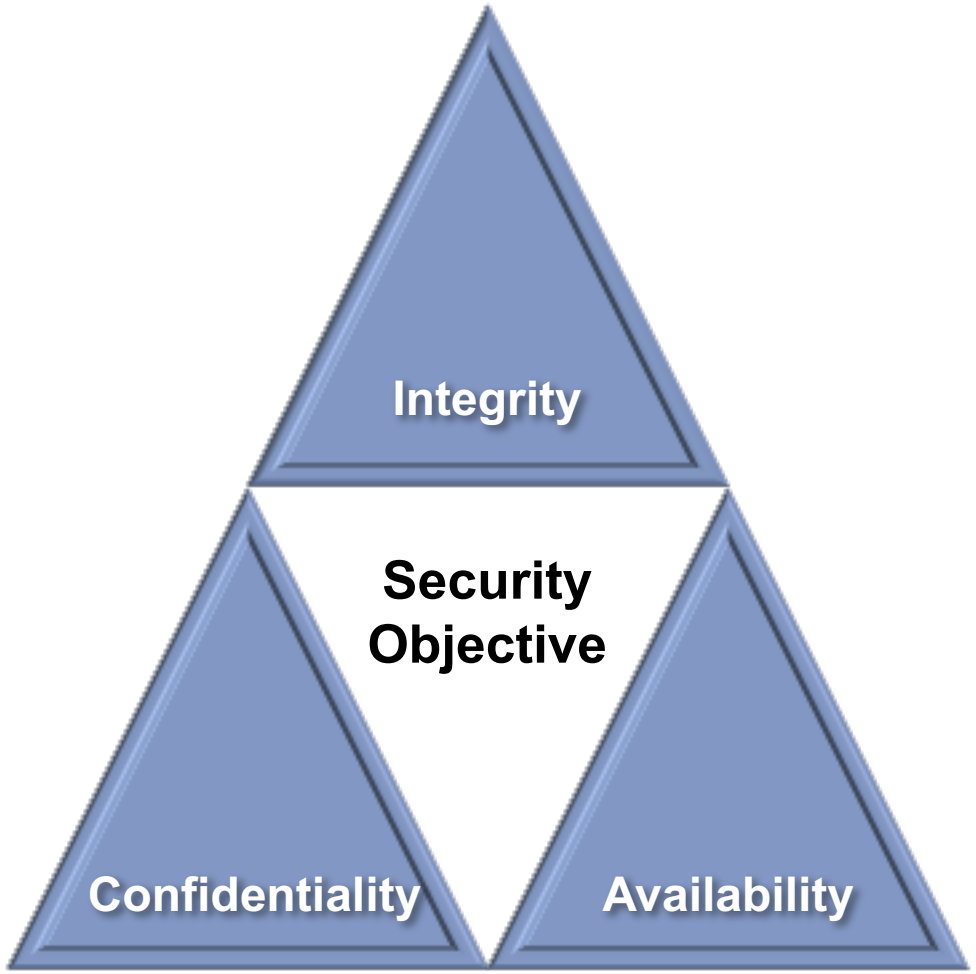
Common Weakness Enumeration

- CWE is a formal list of known vulnerabilities
  - Provides a common language for security vulnerabilities in architecture, design and code
  - Standard metrics for software security tools targeting these vulnerabilities
  - Common standard basis for threat identification, mitigation and prevention measures
  - Started specifically for software vulnerabilities (now over 800)
  - Through industry collaboration, CWE extended its scope to hardware vulnerabilities, releasing 31 hardware design vulnerabilities for the first time in the major release
  - Launch of the CWE Compatibility Program to recognise products and services that utilise CWE.

SA-EDI Data Objects

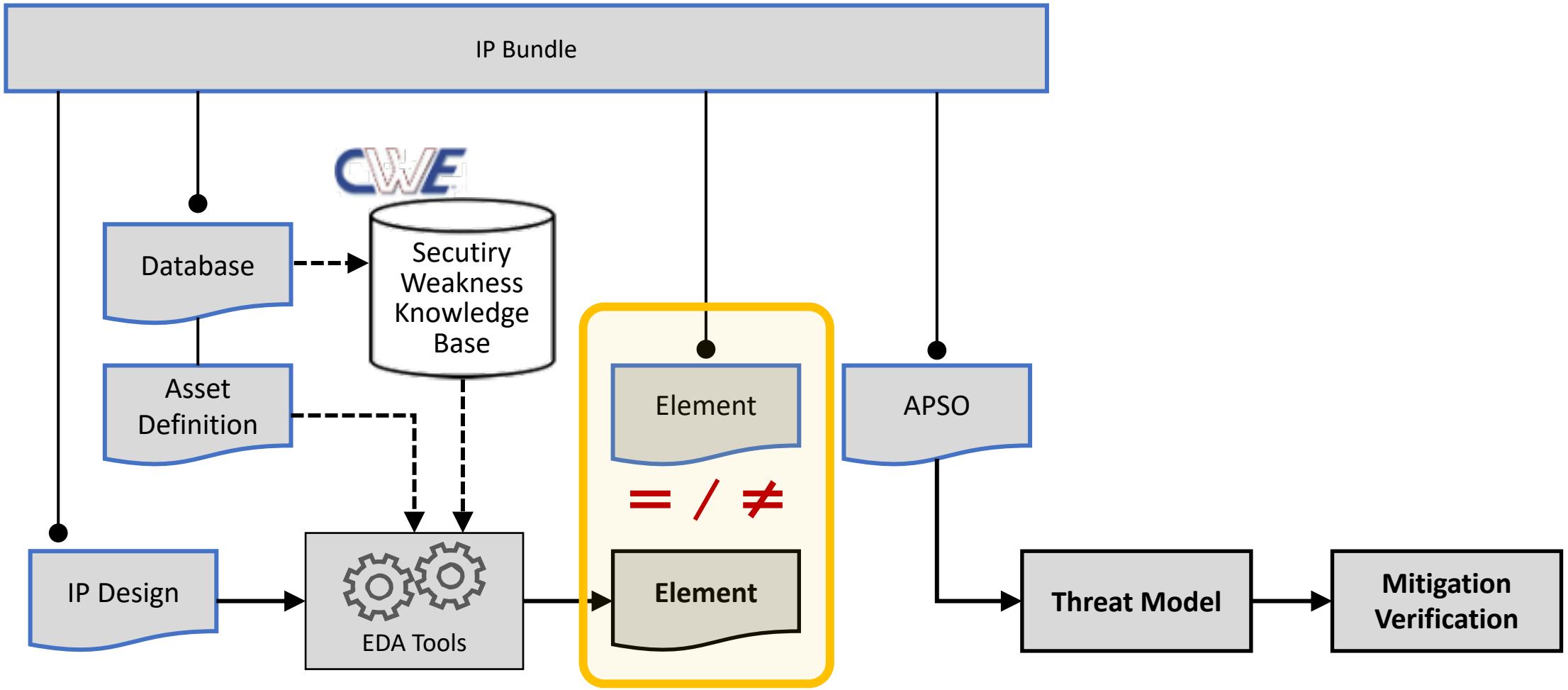
- Database
  - Key attributes for defining security vulnerabilities (CWE)
- Asset Definition
  - Fundamental object that defines an asset within IP
  - Asset = something that has value or importance to be protected
- Element
  - Specifies input/output ports and configuration parameters that can affect or observe an asset
- APSO - Attack Points Security Objective
  - Security goals and attack points assigned to an asset
  - Security Objectives = Confidentiality / Integrity / Availability
  - Specifies conditions that may violate security objectives

Security Objectives



- Confidentiality
  - Making assets that need to be protected unavailable and private to unauthorized processes or entities
- Integrity
  - Protecting the accuracy and completeness of assets that need to be protected
- Availability
  - The property of being accessible when requested by authorized processes or entities

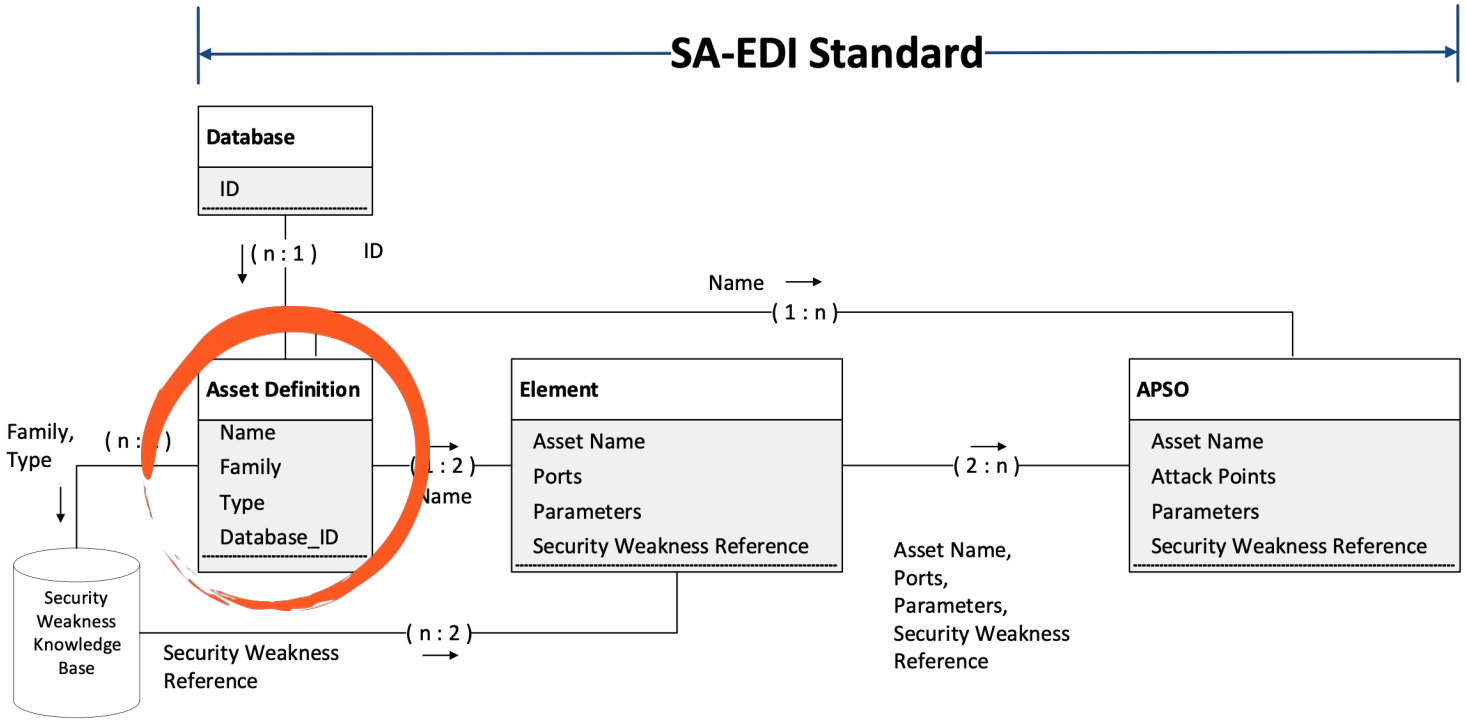
IP Integrator should verify the IP Bundle



Security Asset Identification

What makes something an asset ?

How do I identify assets in my IP ?



Asset :
Anything of value or importance that is used, produced, or protected within the IP

Feedback heard from SA-EDI Users

- *Everything in my IP is important therefore everything is an asset*
  - Creates 100 Asset Definition objects which yields 200 Element objects which yields 400 APSO objects. Humans can not consume 400 JSON objects to create a threat model for their IC.

- *My IP makes no security claims therefore there aren't assets*
  - Information coming into and/or existing the IP could require a security objective once integrated. IP owner needs to assume the IC may have security requirements.

Assets in Detail

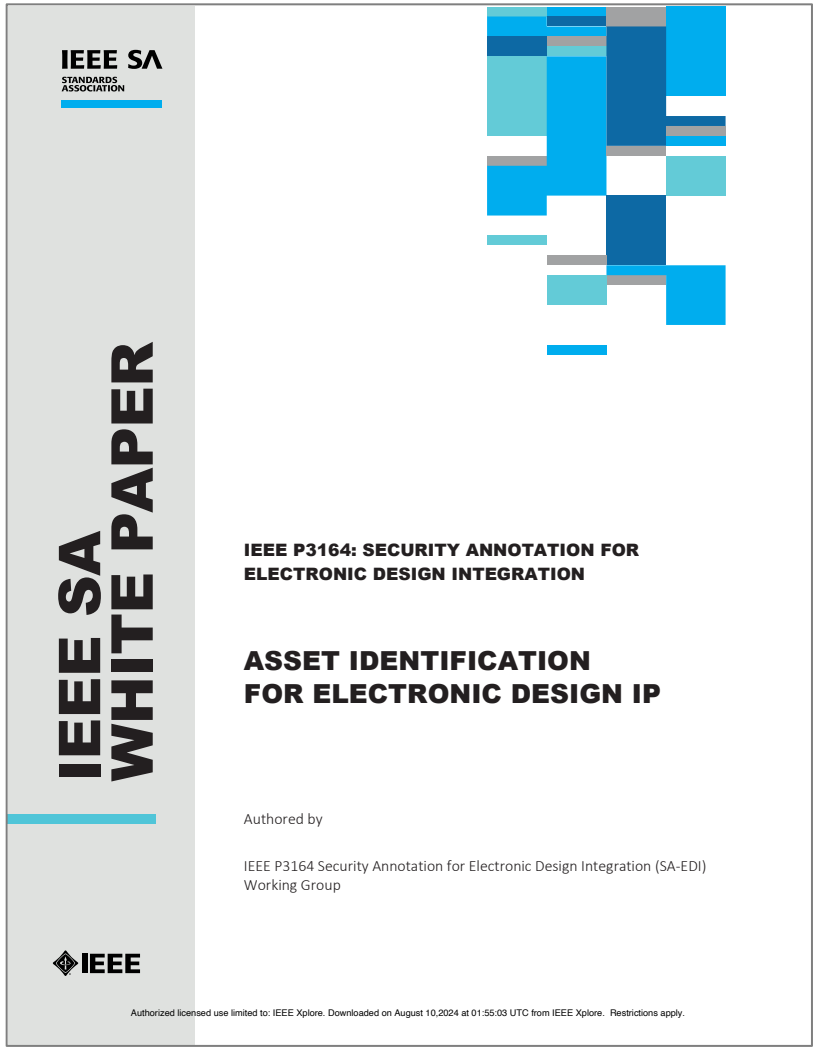
- Definition: Anything of value or importance that is used, produced or protected within the IP

- Anything in an IP:
  - Function (or control of a function)
  - Information

- Value or importance:
  - Monetary value, economical value, operational value, regulatory value
  - To the system integrator, the system user, an adversary
  - Level: asset criticality and sensitivity

Overview Asset Identification Whitepaper

Released on 5 April 2024



The IEEE P3164 Asset Identification Whitepaper

- In P3164 working group discussions, a need to provide guidance for asset idenfitication was recognized, resulting in the Asset Identification Whitepaper
- Two methodologies: CSA and PIO
  - Conceptual and Structural Analysis (CSA): using high-level assets to identify structural assets in the RTL
  - Point of Influence and Observation (PIO): using high-level assets and points of observation/influence to identiry structural assets in the RTL
- Some notes about these methods
  - They are not mutually exclusive
  - Not the only ways to idenfityb assets
  - Both are subjective and not absolute

CSA Introduction

- Conceptual Asset: a high-level asset associated to the use-case flows of data in an IP which involves a security objective (CIA)
  - E.g. an encryption key requires confidentiality

- Structural Asset: RTL material that physical supports a conceptual asset
  - E.g. a register, module, signal, etc. that embodies the conceptual asset

- Asset Definition object: created based on the structural assets

* CIA : Confidentiality Integrity Availability

Security Objectives: Chicken and the Egg

- IP developers typically do not know the security objectives of an IC/SoC -IPs are developed to a specification, not a use-case
  - E.g. the same USB controller may be integrated into a phone, server, and military laptop. All three platforms have different security objectives, but it is the same USB

- Question: How to identify conceptual assets without knowing the security objectives?

- Answer: Assume the security objectives for targeted applications

Conceptual Assets: Questions

- Answer the following questions:

1. Assume the IP is to be integrated into an IC where confidentiality protections are required. Are there any elements in the IP that can leak or expose material that an Integrator may deem as confidential?
   - Is there any information, either as input or internally generated, that may be considered secret?

2. Assume the IP is to be integrated into an IC where integrity protections are required. Are there any elements in the IP that can modify material an Integrator may deem as sensitive?
   - Are there any state or configuration settings that need to be immutable during certain operations or modes?

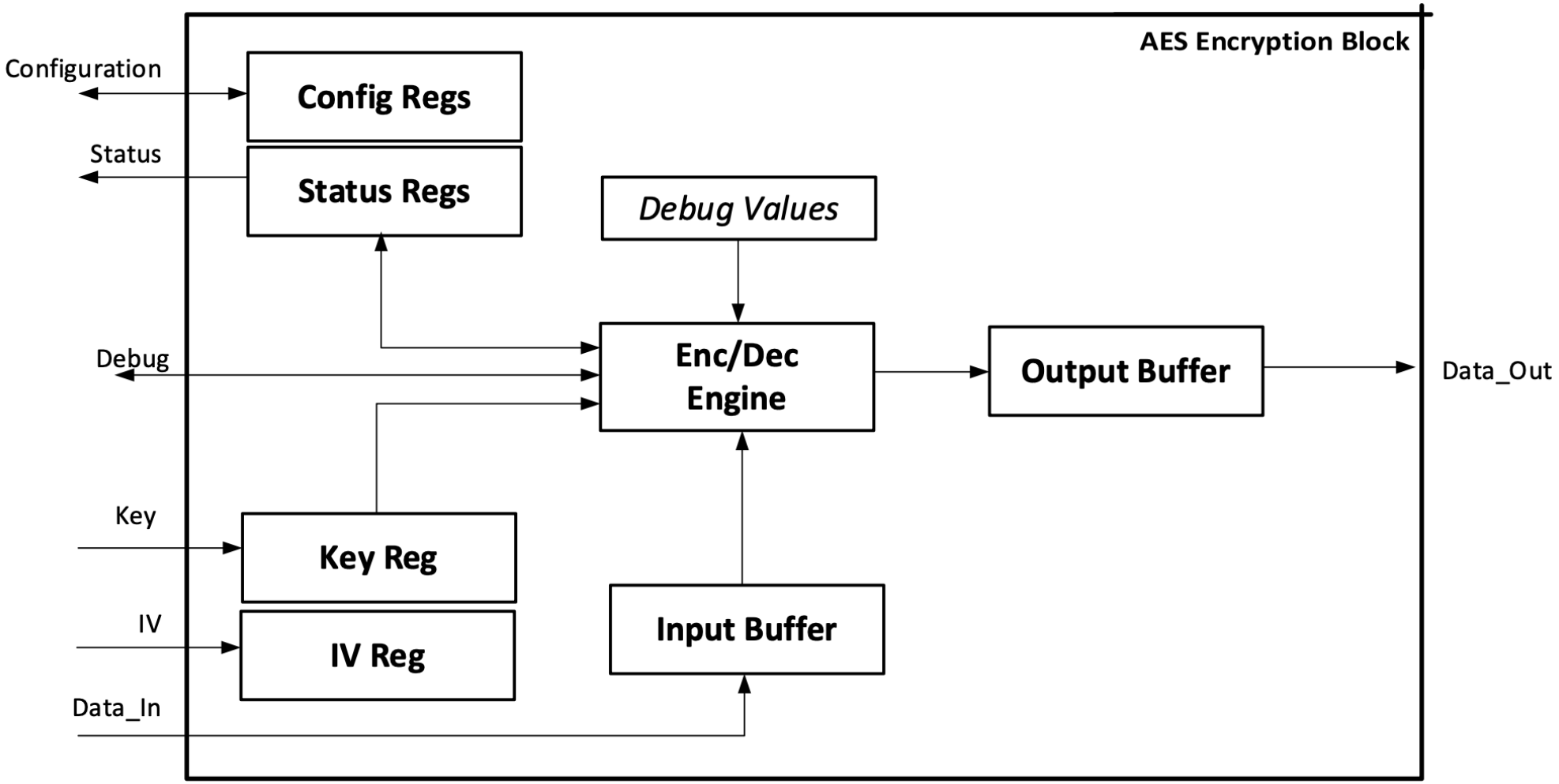
Conceptual Assets: Questions

- Answer the following questions:

3. Are there any elements in the IP that if unavailable, would prohibit the operational behavior of the IP or IC?
   - Are there any elements that could gate an output port or the use of an input port? The focus should be on elements that may be impacted by a denial-of-service attack at the integration level.

4. Are there elements that could be impacted by behaviors at the integration level to undermine the functionality of the IP under normal operation?
   - For example, are there any privileged modes, overrides, bypass, test packet injection, etc. that can make the IP produce incorrect output? The focus should be on elements that may be compromised.

CSA Example: AES Engine



CSA Example: AES Engine

1. Confidentiality. Are there any elements in the IP that can leak or expose material that may need confidentiality?

   - Yes. Since this is a crypto IP, the plaintext data and key value are secrets. Therefore, any block in FIGURE 3 that supports these secrets will be a conceptual asset. These assets are Key Reg, Enc/Dec Engine, Input Buffer, and Output Buffer. Additionally, the Status Regs may leak confidential information since it provides information about the Enc/Dec Engine. Therefore, this block may also be considered a conceptual asset.

2. Integrity. Are there any elements in the IP that can modify material an Integrator may deem as sensitive?

   - Yes. When the Enc/Dec Engine is performing an operation, the key, IV, input data, and its configuration should not be modified. Therefore, Key Reg, IV Reg, Input Buffer, and Config Regs are conceptual assets that require integrity.

CSA Example: AES Engine

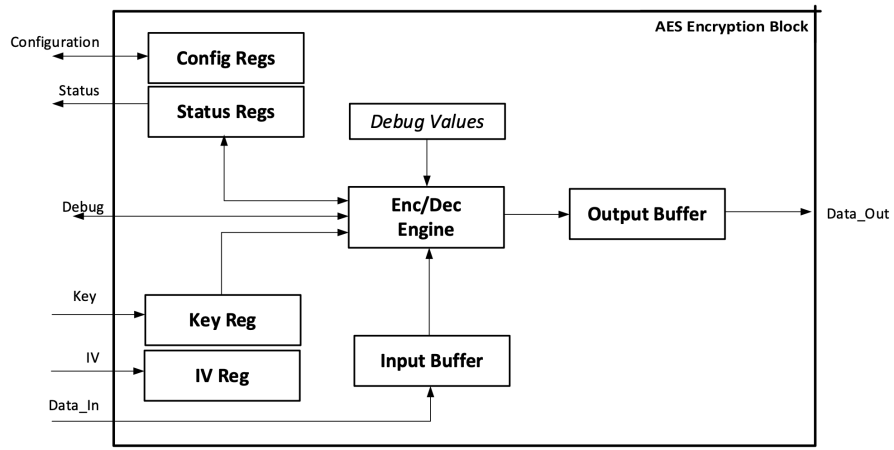
3. Availability. Are there any elements in the IP that can become unavailable, prohibiting operational behavior?

   - Yes. The debug interface allows complete control of the Enc/Dec Engine. Therefore, "Data_Out" can be blocked by this interface and thus making the Enc/Dec Engine a conceptual asset.

4. Undermined expected behavior. Are there elements that could be impacted by behaviors at the integration level to undermine the functionality of the IP under normal operation?

   - Yes. The debug interface allows the IP to encrypt/decrypt using the test key and IV values, which may result in a loss of security strength. Therefore, making the Enc/Dec Engine a conceptual asset.

CSA Example: AES Engine



All blocks in the IP, except the Debug Values block, can be considered as a conceptual asset.

- RTL in each blocks would be the structural assets and require Asset Definition objects,
- Too numerous to list
- Common for security primitives/functions IPs that make security claims (e.g. cryptography).

Options:

1. Entire IP classified as a structural asset with top RTL module as Asset Definition object.
   - Reduce the Asset Definition objects into just one, which simplifies the analysis.
2. Use a modified CSA methodology (detailed in section 4):
   - Analyze the IP from an attack point perspective to identify assets. This approach could help identify assets that are false positives

Both approaches are acceptable and should result in similar APSO objects being created.

Points of Influence and Observation (PIO)

Alternative Approach: Points of Influence and Observation

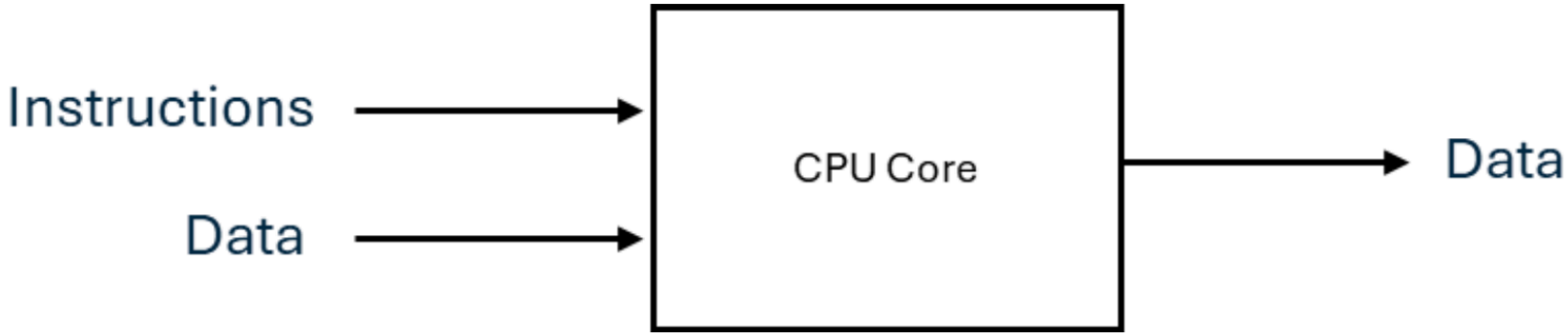
- CSA may be difficult to scale for complex IPs
  - E.g. a CPU core
- CSA may produce false positives or too many structural assets for human comprehension

Points of Influence and Observation (PIO) Methodology

- Focus on inputs and outputs to identify conceptual assets
- Walk through the IP where these conceptual assets can be influenced or observed to identify structural assets:
  1. Does the observation point expose any confidential information about the conceptual asset?
  2. Does the influence point allow any modification of the conceptual asset?
  3. Can the observation and/or influence point prevent the conceptual asset from being available for functional operation?
  4. Does the observation and/or influence point have any special behaviors, e.g. debug mode, that can prevent the conceptual asset from being available for normal operation?

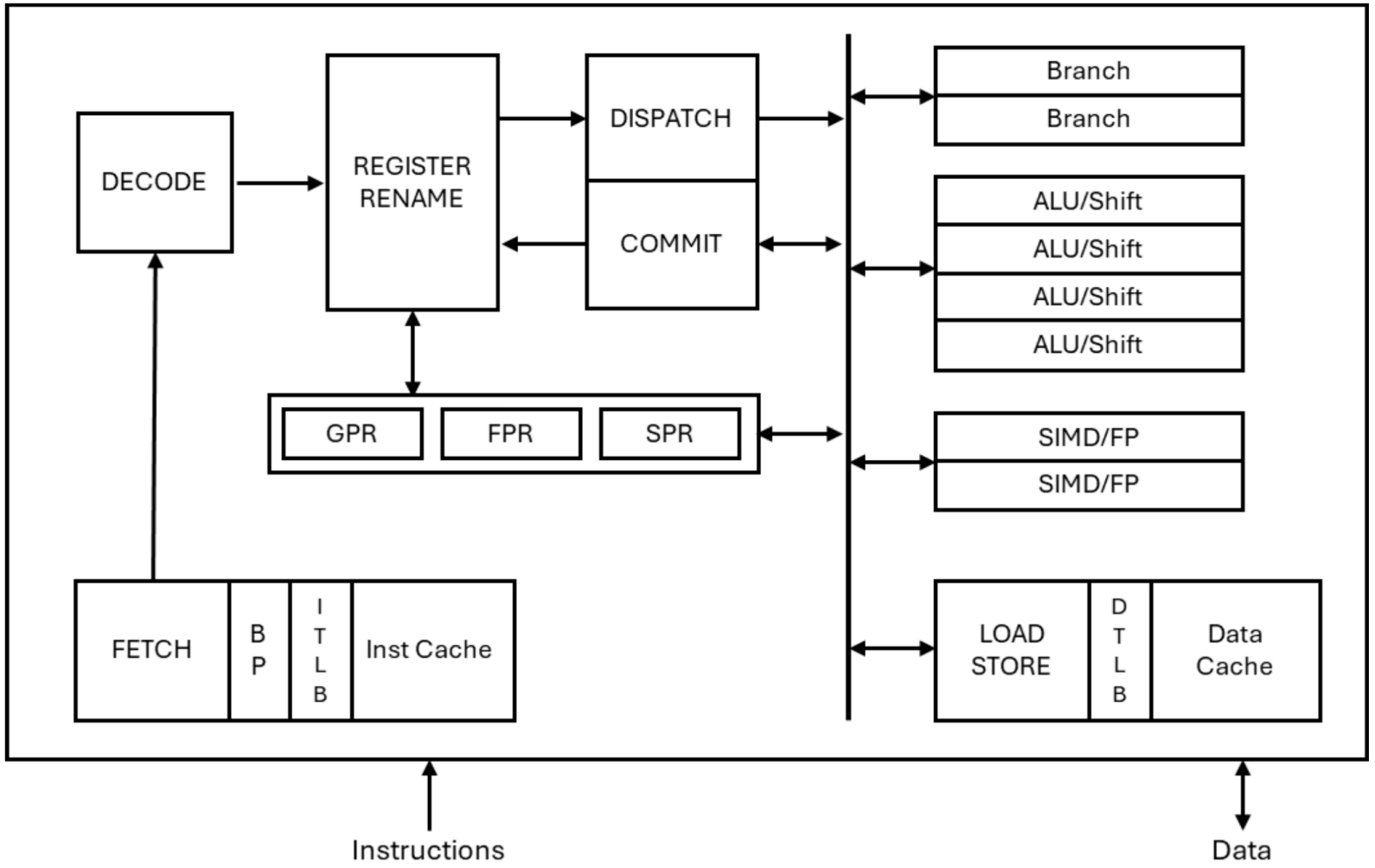
PIO example: CPU Core

- Generic CPU core conceptual assets
  - Instructions
  - Data (input and output)



PIO example: CPU Core

- Registers:
  - General purpose
  - Floating point
  - Special
- Branch predict
- Translation buffer
- Execution units
  - ALU
  - SIMD



PIO example: CPU Core

- Walk through the detailed blocked diagram with focus on Instructions and Data to find the structural assets
  - E.g. DCache (data cache)

1. Confidentiality: Does DCache expose any confidentiality of Data?
   - Yes. Caches are a shared resource that have been known to leak information under certain circumstances.
2. Integrity: Does DCache allow any modification of Data?
   - No the DCache by itself cannot modify data but it can replace when a store operation is requested. However, this is expected behavior and should not result in “Yes” to this question.
3. Availability: Can DCache prevent Data from being available to functional operation?
   - Yes. Thrashing or exhausting the cache can prevent data from being available, in a timely fashion.
4. Undermined expected behavior: Does DCache have any special behaviors that can prevent Data from being available for normal operation?
   - No. There are no features in the Cache that prevents data from being available.

PIO example: CPU Core

- Triggered on questions #1 and #3, therefore structural assets exist in Dcache

- Potential structural assets are the RTL logic for:
  - Replacement policy
  - DCache contents
  - Internal state

PIO example: CPU Core

Conceptual Asset: Instructions			
Observation / Influence Point	Rationale	Structural Asset(s)	Security Objective at Risk
ICache	Caches, if not protected, can be used as covert/side channels to exfiltrate data	ICache replacement policy, ICache contents, and ICache internal state	Confidentiality, availability
BP (Branch Predictor)	BP, if not protected, can be used to influence the flow of control. BP also allows speculative execution, which opens the possibility of exploiting transient execution attacks	Branch prediction history and target addresses	Integrity
ITLB	Caches, if not protected, can be used as covert/side channels to exfiltrate data	Memory mapping, ITLB contents, and ITLB replacement policy	Confidentiality, availability
Conceptual Asset: Data			
GPR, FPR	General-purpose registers are typically shared between multiple processes	Registers	Confidentiality
Functional Units (ALU/Shift, Branch, SIMD, etc.)	The processing time can reveal the data processed if directly Confidentiality dependent on the data itself	Source and data registers	Confidentiality
DCache	Caches, if not protected, can be used as covert/side channels to exfiltrate data	DCache replacement policy, DCache contents, and DCache internal state	Confidentiality, availability
DTLB	Caches, if not protected, can be used as covert/side channels to exfiltrate data	Memory mapping, DTLB contents, and DTLB replacement policy	Confidentiality, availability

Summary

- Two methods to help identify IP assets
  - Conceptual and Structural Analysis (CSA)
  - Points of Influence and Observation (PIO)

- They are not mutually exclusive
- Can be used with other methodologies
- No right or wrong approach

What’s next ?

- Automation
- Additional fields
- Expanded functionality
- Tools

More Information

- Accellera main page :
  - https://www.accellera.org/
- SA-EDI:
  - https://www.accellera.org/downloads/standards/ip-security-assurance
- CWE:
  - https://ccwe.mitre.org
- Submission guidelines:
  - https://cwe.mitre.org/community/submissions/guidelines.html