2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

IP Security Assurance Workshop

Mike Borza, Synopsys Inc.
Ambar Sarkar, NVIDIA Corporation
Adam Sherer, Cadence Design Systems Inc.
Brent Sherman (in spirit), Intel Corporation

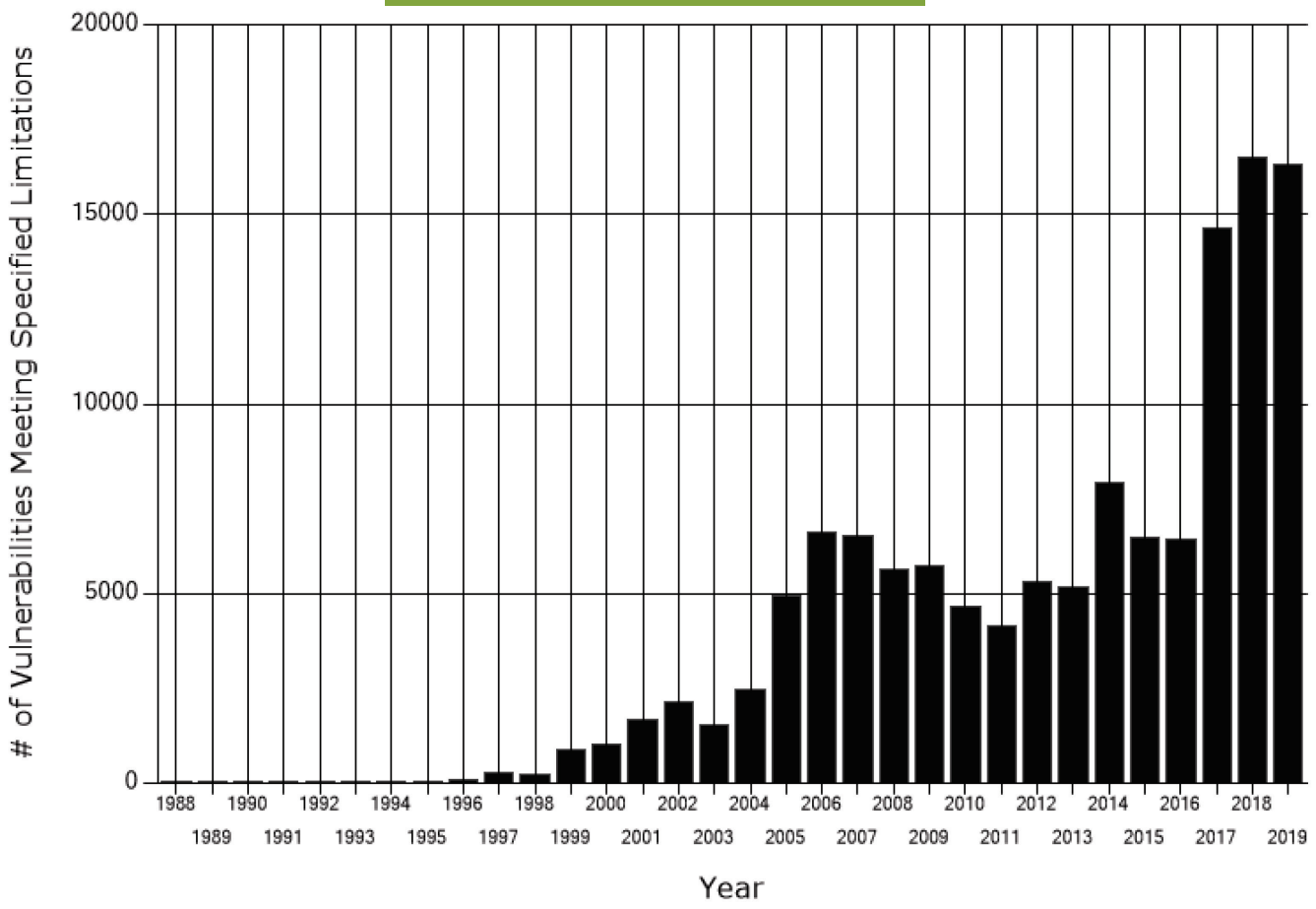
accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Security Risk is Growing

- $1.5 Trillion cyber crime economy[1]
- +11% in security breaches 2019[2]
- $1-200 Hacking tools/kits[3]
- Ransomware attack every ~14s[4]

CVE Growth[5]



1. https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/
2. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
3. https://fortune.com/2017/10/25/cybercrime-spyware-marketplace/
4. https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/
5. https://nvd.nist.gov/vuln/search

accellera SYSTEMS INITIATIVE

Everything is Connected…

- Peer-to-Peer, Device-to-Cloud, Cloud-to-Cloud, ...
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Security: multiple dependencies and assumptions
  - Functional and Assurance
- Break the chain and it falls apart
  - Denial of Service (Permanent vs. Persistent)
  - Escalation of privilege
  - Information leakage
  - Code execution

Security Risk with IPs

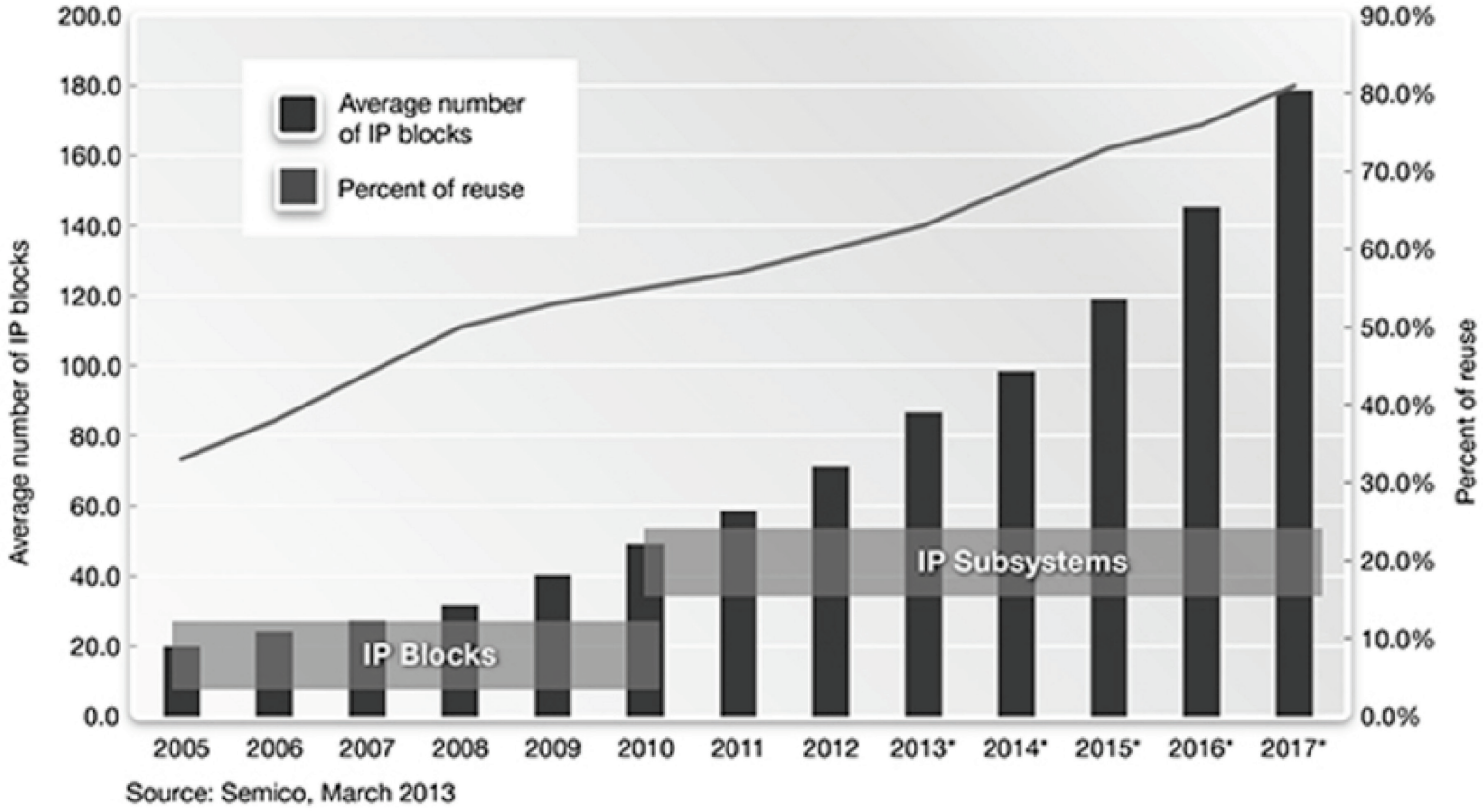
Increasing demands for:

- IP Subsystems
- Reuse
- Third-party IP

Unfortunately lead to…

Security concerns:

- Complexity = Increase risk
- Reuse = Increase exposure
- Third-party = Increase unknowns (black-box)

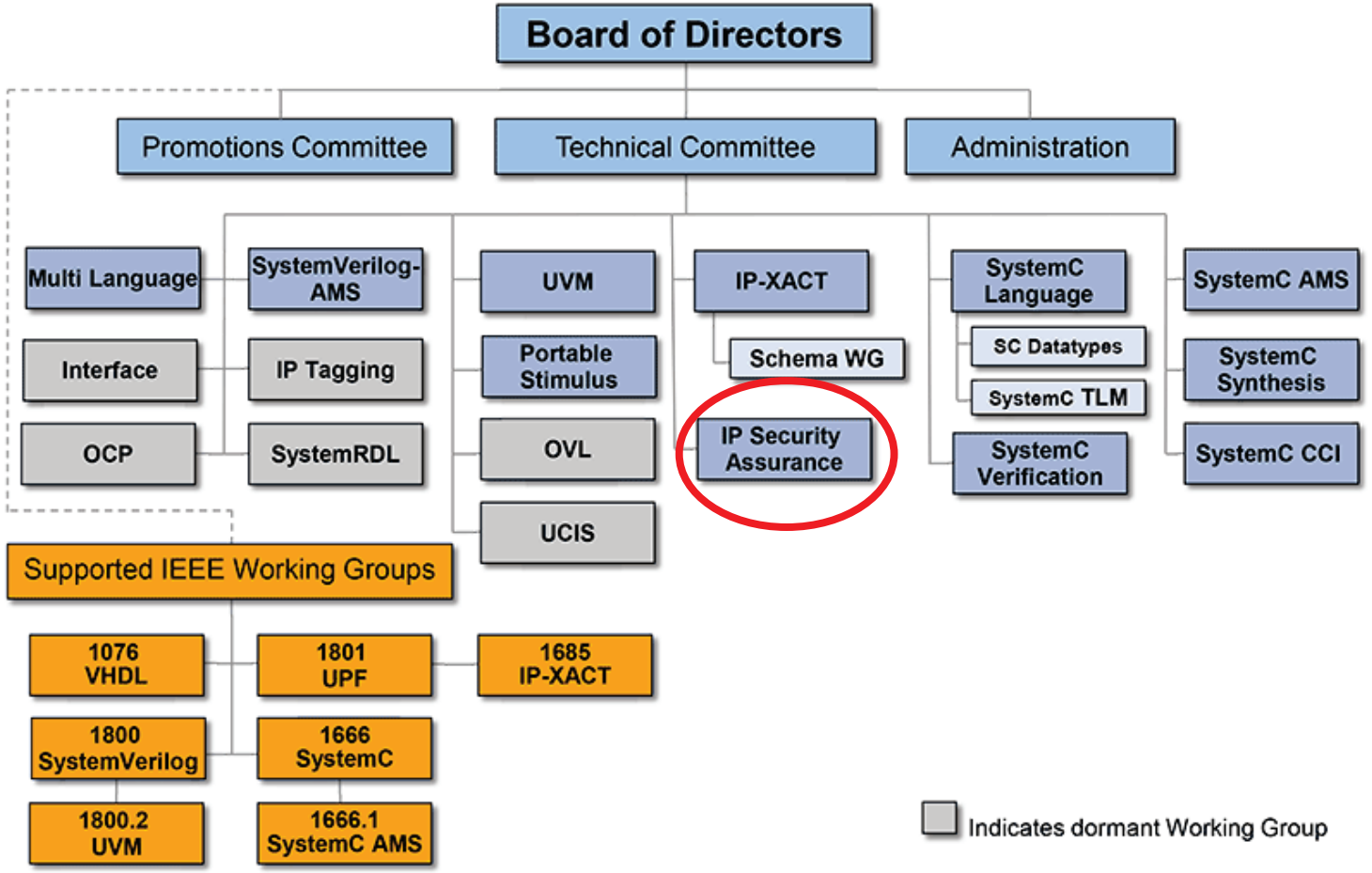


https://www.synopsys.com/designware-ip/technical-bulletin/accelerate-time-to-market.html

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Accellera

- Accellera is an independent, not-for profit organization dedicated to create, support, promote, and advance system-level design, modeling, and verification standards for use by the worldwide electronics industry
- Mission is to provide a platform in which the industry can collaborate to innovate and deliver global standards that improve design and verification productivity for electronics products.



https://www.accellera.org/

accellera SYSTEMS INITIATIVE

Accellera: IP Security Assurance Workgroup

- Formed: Oct'18
- Members: 61
- Companies: 21

AMD	Intel	NXP Semiconductors	Tortuga Logic
Analog Devices	Leidos	OneSpin Solutions	VeriSilicon
ARM	Marvell	Qualcomm	Xilinx
Cadence Design Systems	Mentor Graphics	SiFive	
Cisco	Methodics	Synopsys	
Cypress Semiconductor	NVIDIA	Texas Instruments	

- University: 1
  - University of Maryland

Source: Internal Accellera data

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

IPSA WG Agenda

Scope	Security concerns with integrating hardware IP into embedded systems (e.g., SoC)
Concern	What exactly is being integrated? What are the risks? How to verify the completeness, accuracy, and overall quality of a supplier's security assurance collateral?
Focus	Existing standards that pertain to IP specification, design, verification, and integration where security risk is a concern Known security concerns that have been identified by either industry experience or security researchers
Stakeholders	IP Providers EDA Vendors IP Integrators
Out of Scope	Establishing trust between stakeholders Establishing trust in the supply-chain (e.g., Trojan Horse detection)

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Thank You

Please Continue with Part 2

Thank you to our Accellera Global Sponsors

cadence®

Mentor® A Siemens Business

SYNOPSYS®

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

IP Security Assurance Workshop

Part 2:
METHODOLOGY & WORKFLOW

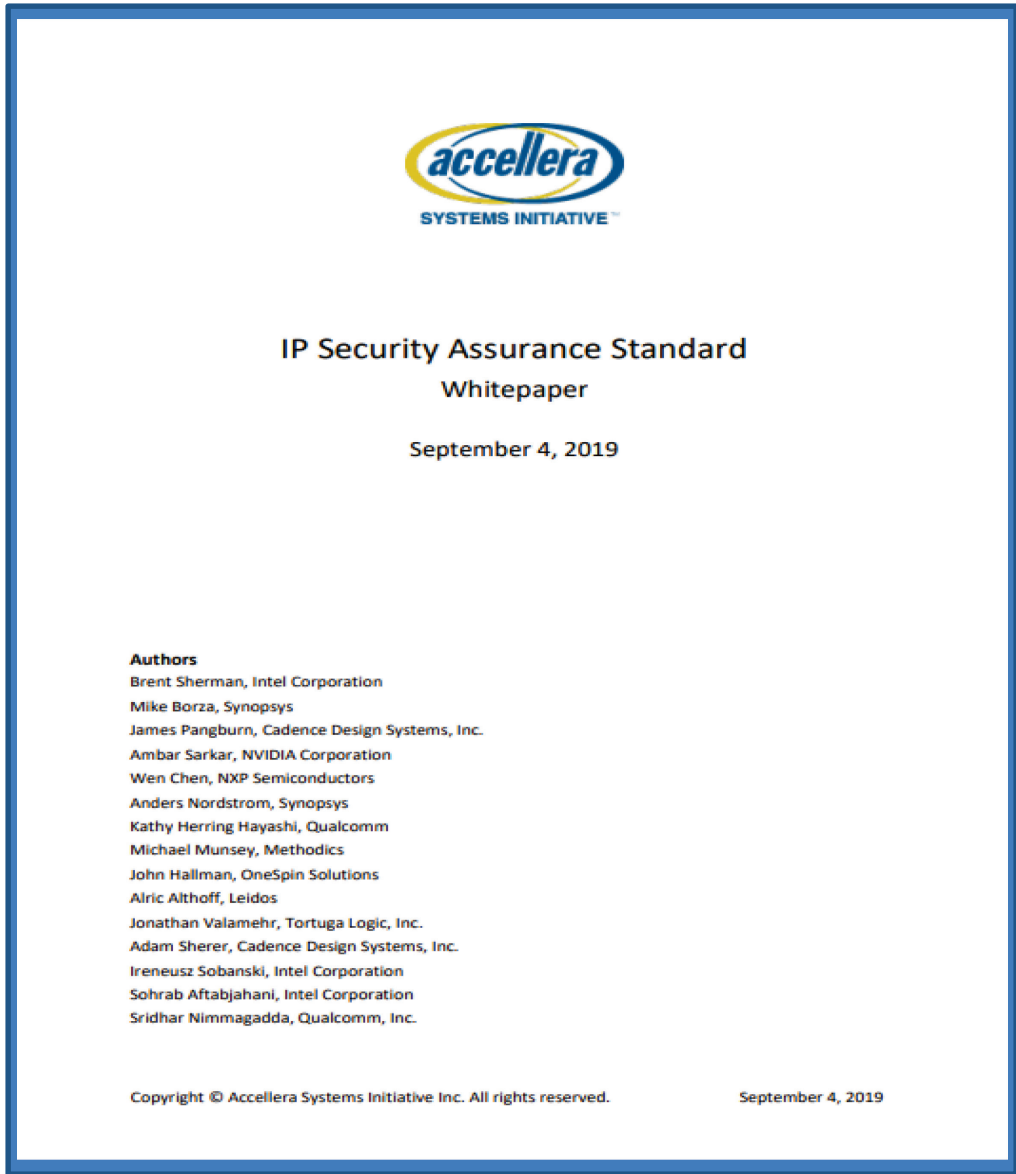
Ambar Sarkar, NVIDIA Corporation

accellera SYSTEMS INITIATIVE

Whitepaper: IPSA Proposal

- Released: Sept 4th 2019
  - https://www.accellera.org/images/activities/working-groups/ipsa-wg/Whitepaper_IPSA_Sept_4_2019.pdf

  - **Methodology:**
    - The overall concept and workflow along with the individual components, dependencies, and assumptions
  - **Common IP Security Concern Enumeration (CIPSCE):**
    - A knowledge base that lists potential IP security concerns in a similar manner as Common Weakness Enumeration (CWE)
  - **OpenCores Examples:**
    - Highlights how the methodology applies to real open source cores
  - **Summary and Outlook:**
    - Captures the next steps required for public release of the standard and roadmap



accellera SYSTEMS INITIATIVE

IP Security Assurance Standard

Whitepaper

September 4, 2019

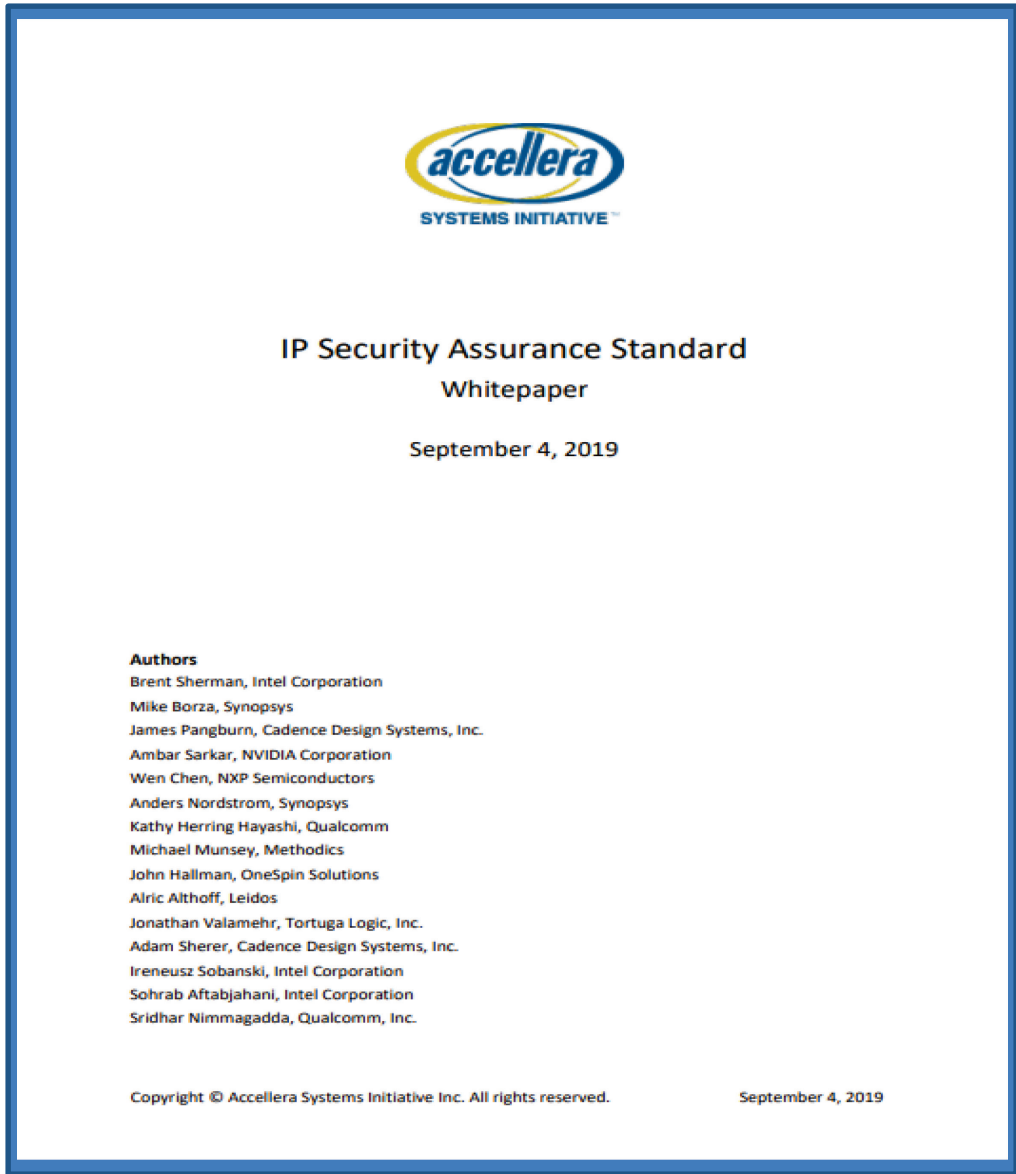
Authors
Brent Sherman, Intel Corporation
Mike Borza, Synopsys
James Pangburn, Cadence Design Systems, Inc.
Ambar Sarkar, NVIDIA Corporation
Wen Chen, NXP Semiconductors
Anders Nordstrom, Synopsys
Kathy Herring Hayashi, Qualcomm
Michael Munsey, Methodics
John Hallman, OneSpin Solutions
Alric Althoff, Leidos
Jonathan Valamehr, Tortuga Logic, Inc.
Adam Sherer, Cadence Design Systems, Inc.
Ireneusz Sobanski, Intel Corporation
Sohrab Aftabjahani, Intel Corporation
Sridhar Nimmagadda, Qualcomm, Inc.

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Whitepaper: IPSA Proposal

Many changes happened since the release (e.g., feedback, developments, etc.). Want to focus on the following:

- **Methodology:**
  - The overall concept and workflow along with the individual components, dependencies, and assumptions
- **Common IP Security Concern Enumeration (CIPSCE):**
  - A knowledge base that lists potential IP security concerns in a similar manner as Common Weakness Enumeration (CWE)
- **OpenCores Examples:**
  - Highlights how the methodology applies to real open source cores
- **Summary and Outlook:**
  - Captures the next steps required for public release of the standard and roadmap



accellera SYSTEMS INITIATIVE

IP Security Assurance Standard

Whitepaper

September 4, 2019

Authors

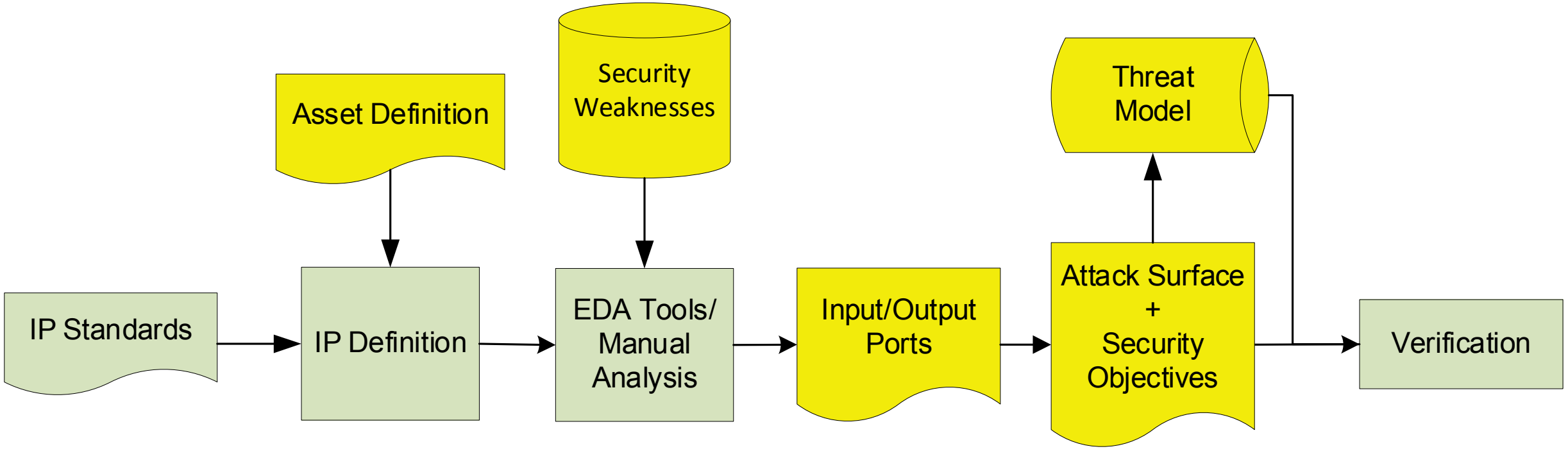
Brent Sherman, Intel Corporation
Mike Borza, Synopsys
James Pangburn, Cadence Design Systems, Inc.
Ambar Sarkar, NVIDIA Corporation
Wen Chen, NXP Semiconductors
Anders Nordstrom, Synopsys
Kathy Herring Hayashi, Qualcomm
Michael Munsey, Methodics
John Hallman, OneSpin Solutions
Alric Althoff, Leidos
Jonathan Valamehr, Tortuga Logic, Inc.
Adam Sherer, Cadence Design Systems, Inc.
Ireneusz Sobanski, Intel Corporation
Sohrab Aftabjahani, Intel Corporation
Sridhar Nimmagadda, Qualcomm, Inc.

accellera SYSTEMS INITIATIVE

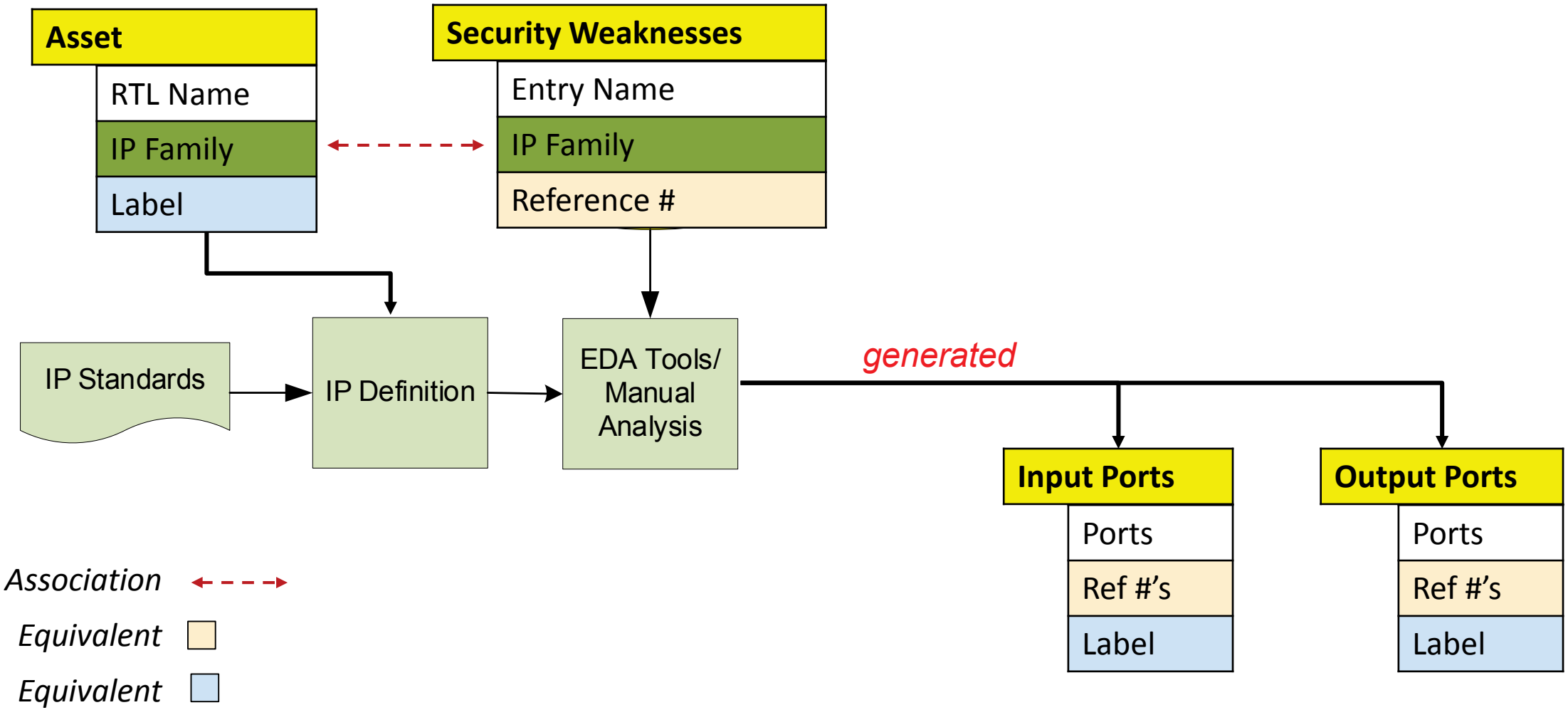
Definition of Terms

Term	Definition
RTL (Register-transfer Level)	A design abstraction that models a digital circuit.
IP (Intellectual Property)	The RTL or other design representation that is the subject of this discussion.
Asset	Anything of value or importance that is used, produced, or protected within the IP.
Threat (Attack)	Anything that can potentially adversely affect an asset.
Concern (Consequence)	The potential harm that a threat poses to an asset. This can also be considered a weakness.
Attack Surface	The set of access points to which threats can be applied.

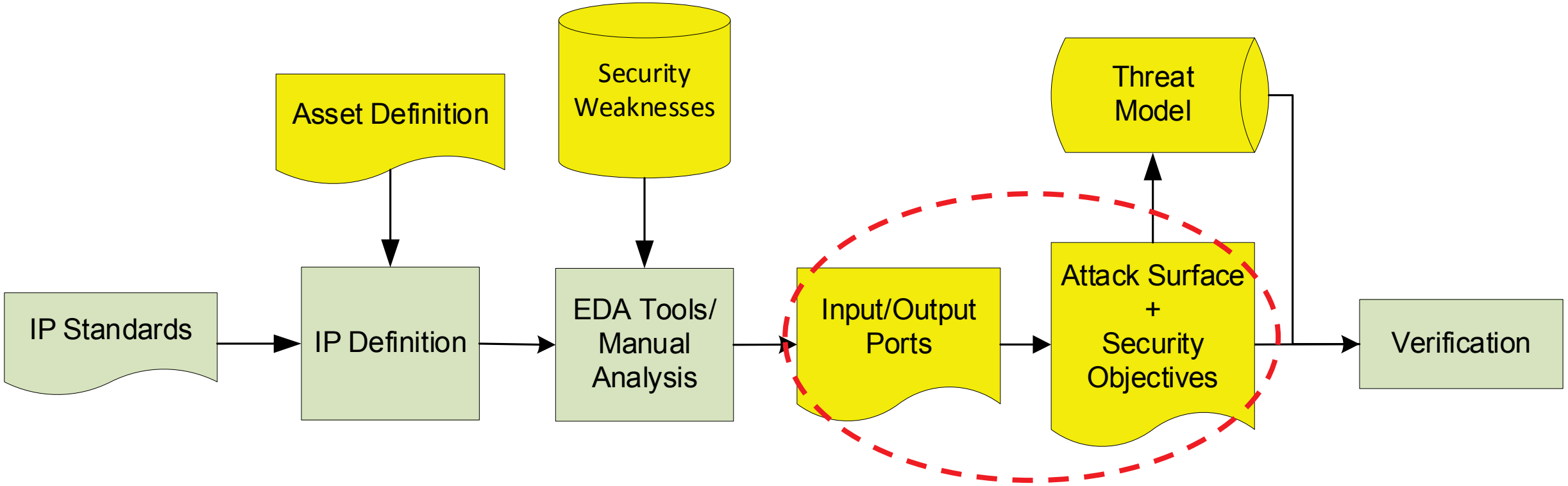
Conceptual Workflow



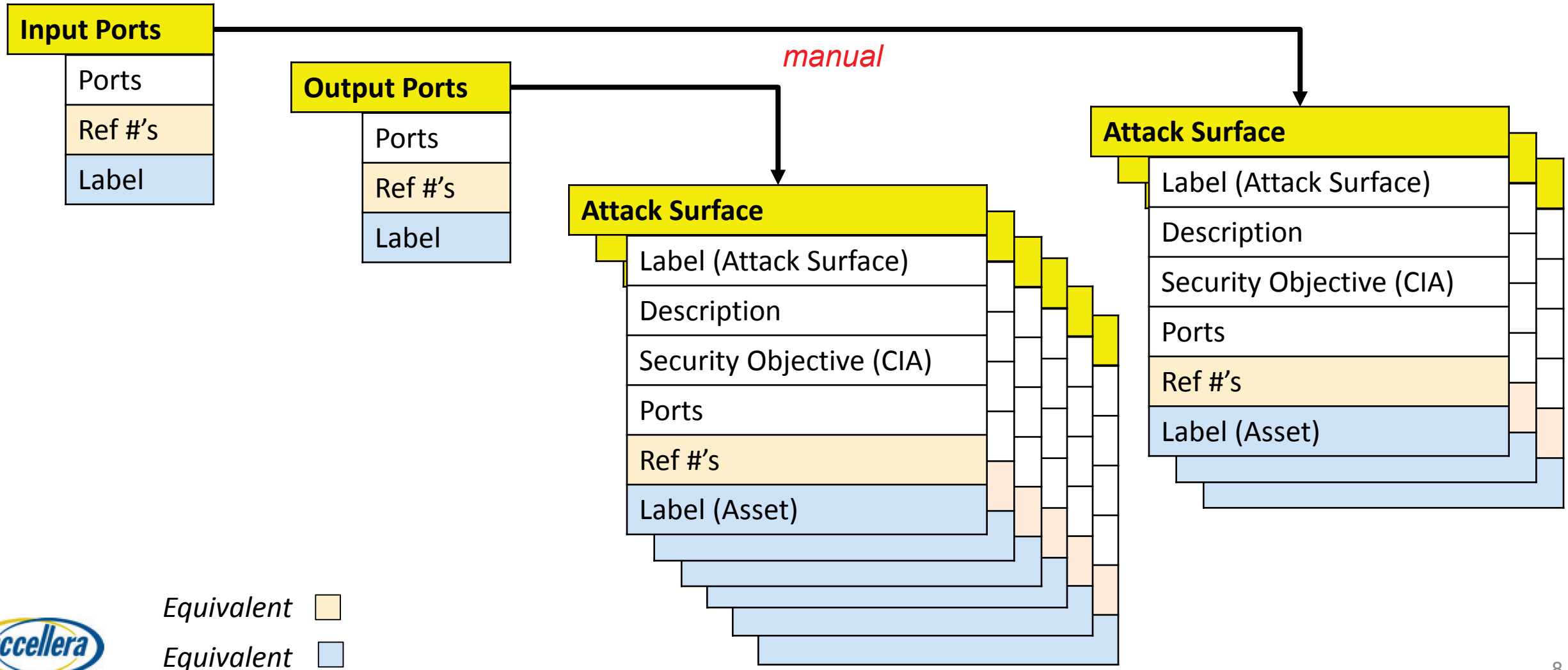
IP Provider: #1 - Identify Assets and Generate



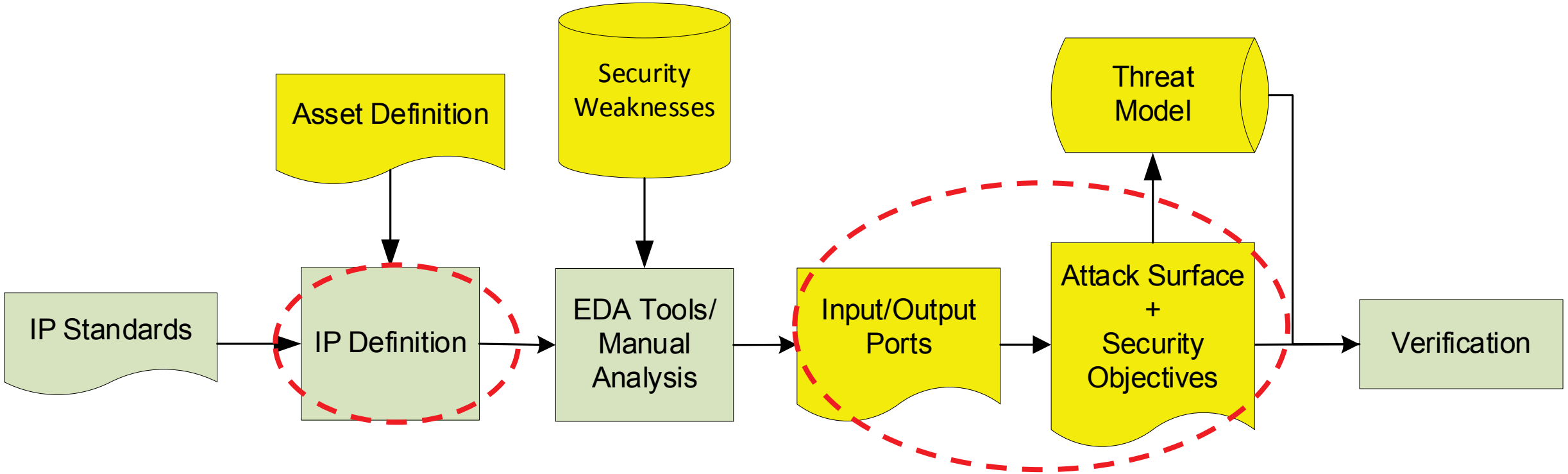
Conceptual Workflow



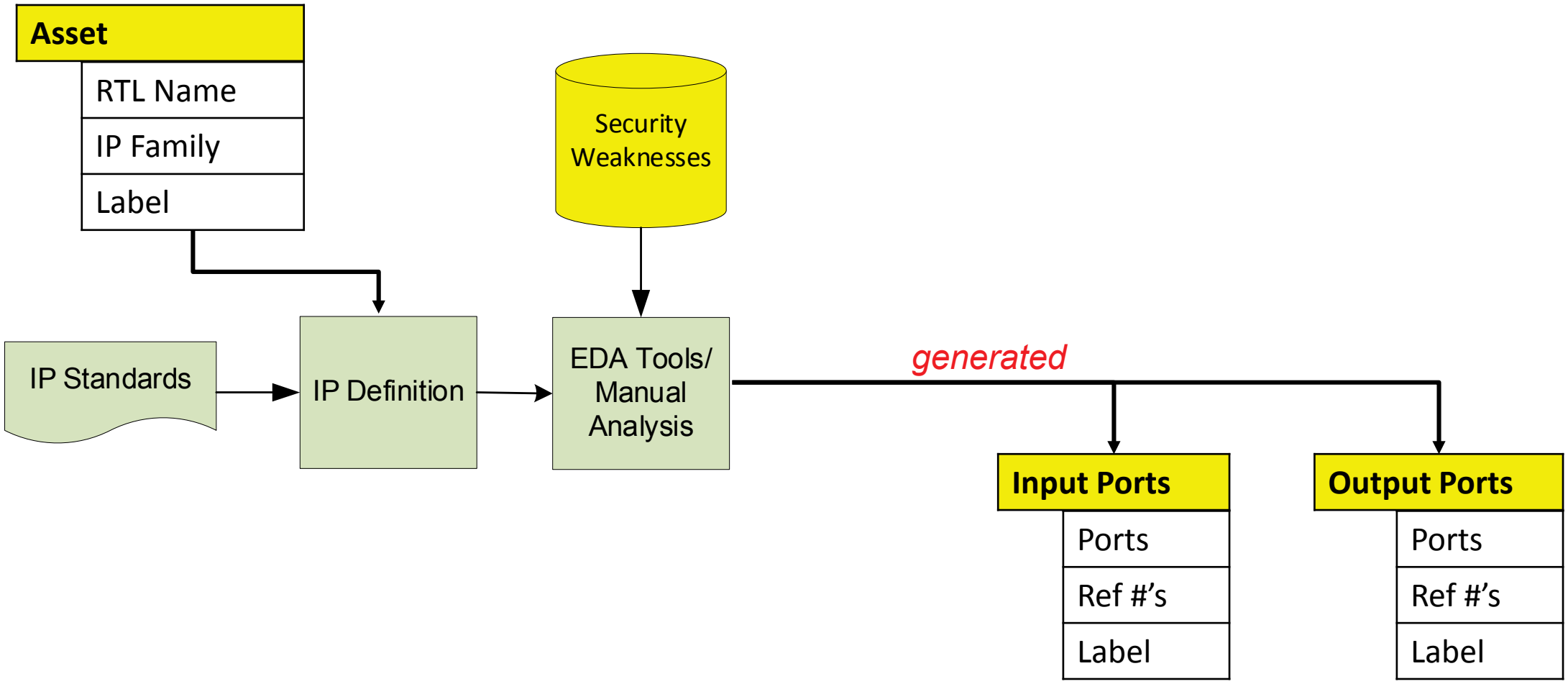
IP Provider: #2 - Assign Security Objectives



IP Provider: #3 – Deliver Collateral to Integrator

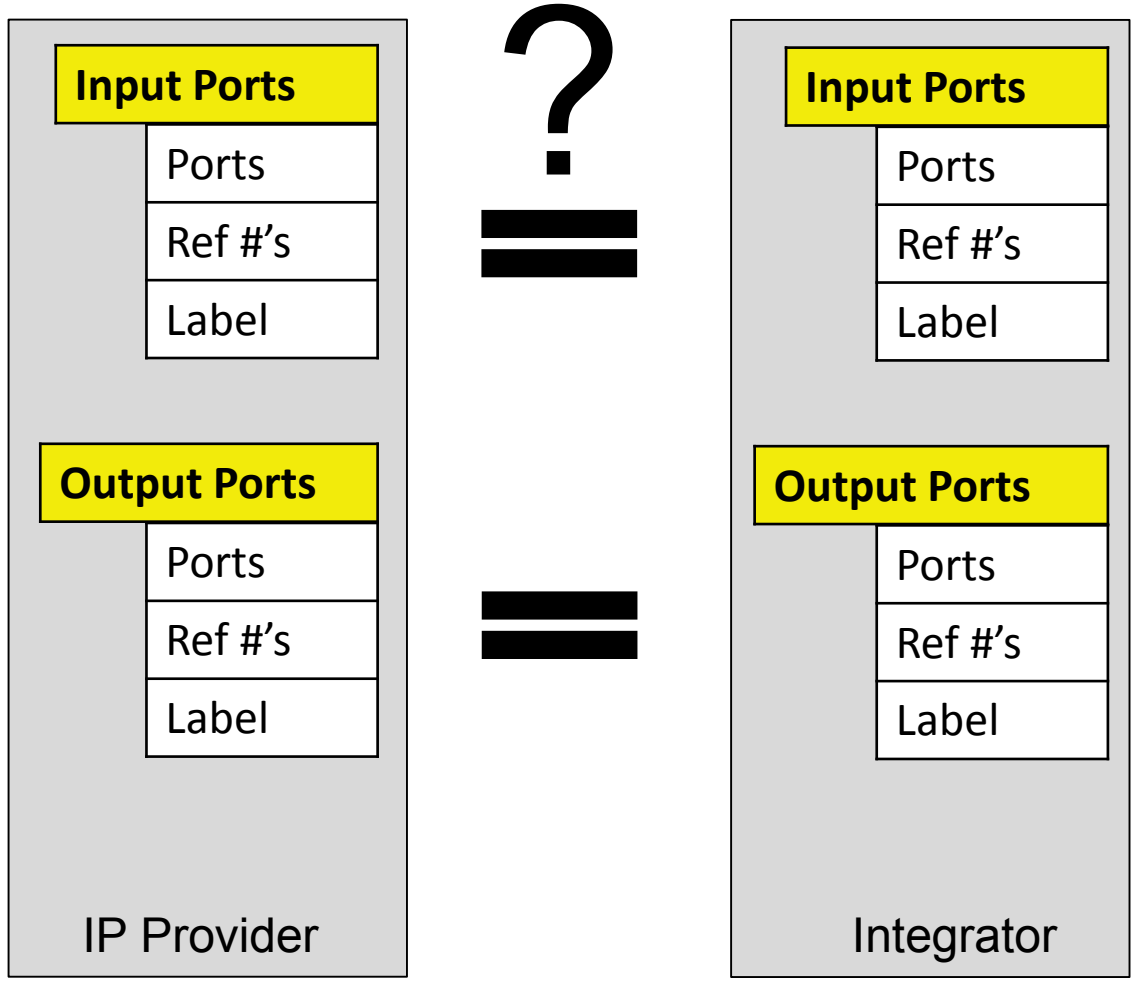


Integrator: #1 – Generate Port Tables

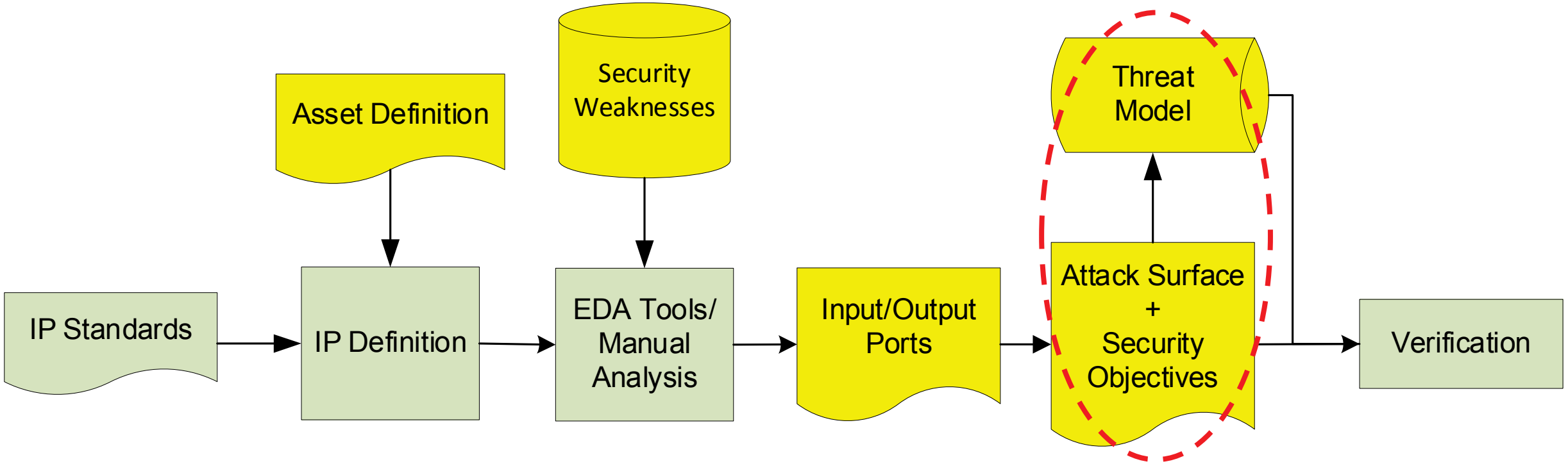


Integrator: #2 – Execute "Trust but Verify"

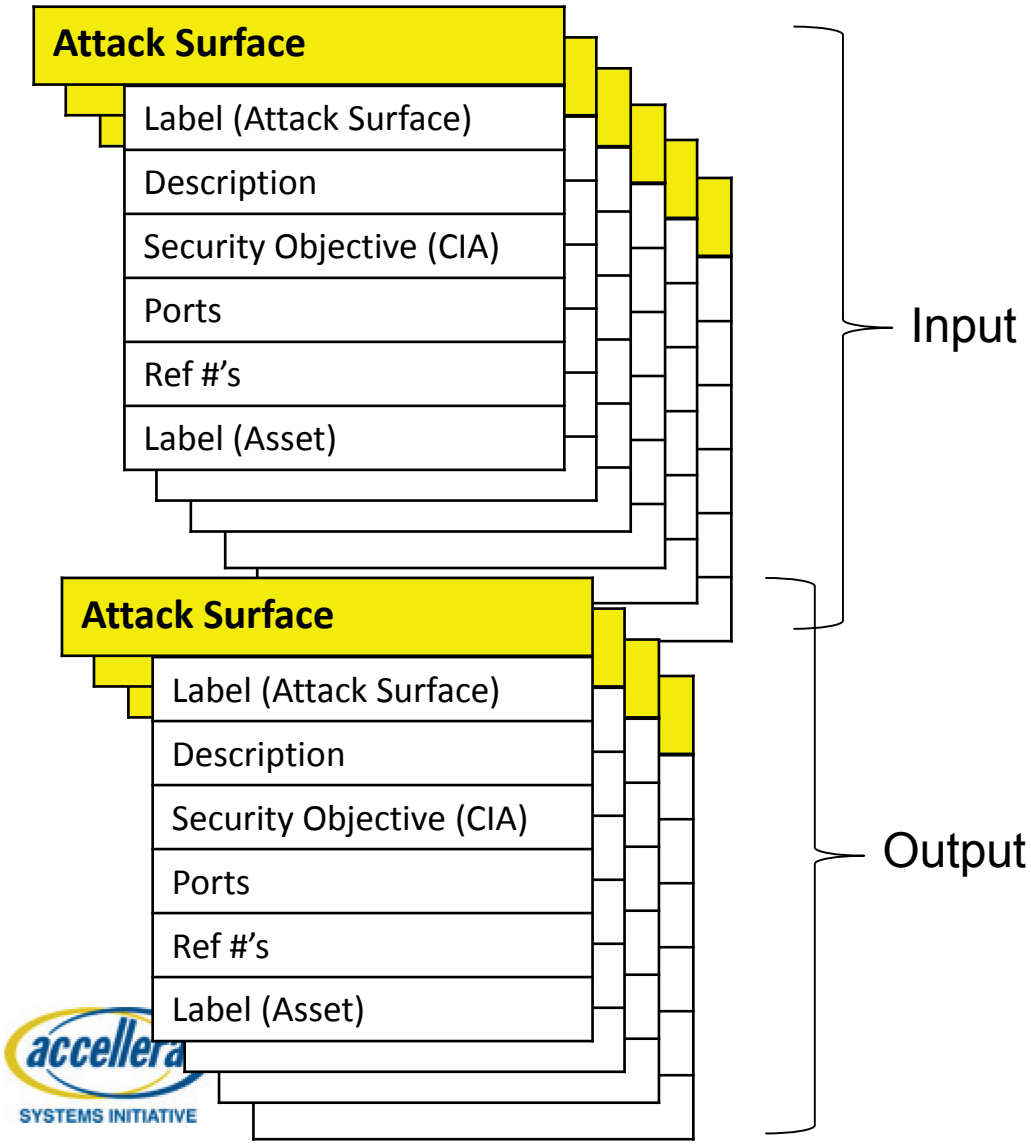
- Compares the Ports generated with the Ports provided by the IP Provider
- If == then RTL matches IPSA collateral and Integrator trusts the IP collateral.
- If != then Integrator should NOT integrate the IP



Conceptual Workflow



Integrator: #3 – Develop Threat Model



1. Select which Security Objectives are in scope for the product

2. For each Security Objective, select which Security Weaknesses are in scope for the product

Integrator: #4 – Expand Threat Model (Optional)

Input Ports
Ports
Ref #'s
Label

Output Ports
Ports
Ref #'s
Label

3. Using the ports, assign additional Security Objectives that may be product specific

4. Manually search the "Security Weaknesses" database for potentially new/missed references

- Final result is the product's Threat Model

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Common Weakness Enumeration

- CWE is a formal list of known weakness types
  - Provides a common language to describe security weaknesses in architecture, design, or code.
  - A standard measuring stick for software security tools targeting these weaknesses.
  - A common baseline standard for identification, mitigation, and prevention efforts
  - Began with a focus on software weaknesses (now 800+) and has published several iterations of the Top 25 Most Critical Software Errors

- **With help from industry collaborators, CWE expanded its scope into hardware weaknesses for the first time with a major new release on February 20, 2020. CWE v4.0 included 31 hardware design weaknesses, and the team is seeking further collaborators and contributors to help grow the effort.**

For more information and to find out how to get involved, please contact cwe@mitre.org

CWE

U.S. DEPARTMENT OF HOMELAND SECURITY

accellera SYSTEMS INITIATIVE

MITRE

IPSA: Summary

#	Requirements	Met?	
1	Low-overhead and non-disruptive	• Defined outside of the design • Simple reference tags (JSON, XML) • Minimum tooling required	✓
2	Flexible and scalable	• Can apply to existing designs • Allows for growth/expansion	✓
3	Auto-generate and verifiable	• EDA tool generation • Verifies RTL matches SA collateral	✓

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Roadmap

- May’20 – Whitepaper updated (Addendum)
- Jun’20 – DAC: Demo with EDA tool and Security Weaknesses database
- Dec’20 – Public review of the candidate standard

accellera SYSTEMS INITIATIVE

Resources

- Contact information:
  - Accellera main page: https://www.accellera.org/
    - IPSA workgroup main page: https://www.accellera.org/activities/working-groups/ip-security-assurance
    - Whitepaper discussion page: https://forums.accellera.org/forum/46-ip-security/
    - Lynn Garibaldi lynn@accellera.org
  - MITRE Corporation
    - CWE Submission: cwe@mitre.org
    - Submission guidelines: http://cwe.mitre.org/community/submissions/guidelines.html

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Thank You

Please Continue with Part 3

Thank you to our Accellera Global Sponsors

cadence®

Mentor® A Siemens Business

SYNOPSYS®

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

IP Security Assurance Workshop

Part 3:
CAPTURING SECURITY CONCERNS KNOWLEDGE IN THE ACCELLERA IPSA STANDARD

Mike Borza, Synopsys Inc.

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Overview

- Background motivation for a standard treatment of IP security concerns
- Latest view of capturing Security Concerns knowledge
- Underlying Assumptions: What Information Do We Expect Useful Knowledge Bases to Contain?
- How CIPSCE will be used by CAD tool providers to automate security analysis

accellera SYSTEMS INITIATIVE

Background

- The IPSA Working Group is developing a standard for IP providers to communicate to IP consumers the security properties of their products
  - Inform IP consumers of unmitigated concerns about which they may care
  - Allow objective comparison of the security properties of different products that perform comparable functions

- There is not a widely available catalog of common concerns in hardware IP of which designers should be aware

- Hence, creation of the Known Security Concerns (KSC) subgroup
  - Capture this knowledge in a Common IP Security Concerns Enumeration (CIPSCE)

Background (cont'd)

- Work progressed within the KSC subgroup
  - We developed a prototype CIPSCE database using the Jira tool
  - We also learned that Mitre is extending their Common Weakness Enumeration (CWE) knowledge base from software and systems to incorporate hardware
- Combine forces: distribute the CIPSCE data in the CWE knowledge base
  - Whether and how to do so are still open questions under active consideration
- To accommodate possible alternate Security Concerns knowledge bases in IPSA processes and tools, we relaxed the specifications

IP 'Family' Attribute: Connects IP to CIPSCE

- An IP product's collateral uses an attribute called 'Family' to describe in general terms the functionality of the IP (may be more than one)
- This Family attribute associates CIPSCE entries with the IP

Accelerator	Microcontroller
Analog & Mixed-Signal IP	Power Management
Audio/Video	Processors
Bus/Interface IP	Security
Communications	Storage
Controllers	Test/Debug
Counter/Timer	Transducers
Memories	<user defined>

What Knowledge Needs to be Represented?

- Any Security Concerns knowledge base needs similar information to be useful
- General items, in addition to the Family attribute:
  - Reference Identifier – a unique identifier to refer to an entry
  - Version Identifier – if a source allows multiple versions of a piece of knowledge, it should have an identifier for a specific version
  - Title – a descriptive name that helps to find items of interest
  - Description – a detailed overview of the specific security concern
  - Relationship – reference(s) to related security concern(s) – e.g., the RefID of another concern
  - Examples – descriptive examples that can help others understand a concern

Consequence

- Consequence tells the user what the nature of the concern is
- Confidentiality: ensure only authorized information disclosure
- Integrity: ensure only authorized information modification or destruction
- Availability: ensure information is available when needed
- Adopted NIST FIPS 199 as our standard reference

Applicability

- Applicability is the Family or Families of IP to which this concern corresponds or is relevant
- Use a “wildcard” Applicability class like ‘All’ if any type of IP may be affected
- This is the only attribute we require of a knowledge base to allow automated tools to connect known concerns with particular types of IP products

Modes of Introduction

Lifecycle stages in which the concern may be introduced into a product

- Architecture
- Design
- Implementation
- Integration
- Manufacturing
- Provisioning

Mitigation

Lifecycle stage(s) and measures to be taken to mitigate the concern

- Architecture
- Design
- Implementation
- Integration
- Manufacturing
- Provisioning
- Field or In-service updates

How Do We Envision This Being Used?

- CIPSCE will be useful in its own right as a design reference
- We also expect design tool providers to incorporate the knowledge in automated analysis tools
- CIPSCE data will be imported into the tool, either directly or via a translator for alternate source data
- The IP's collateral includes an IPSA security attributes file that identifies its assets and the concerns for each asset, and whether the concern is mitigated in the IP
- The tool generates an attack surface for the IP, and may probe that attack surface
- As IP is integrated into a complete IC, the tool may probe whether unmitigated concerns remain

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Summing Up

- CIPSCE provides a means to document and disclose security concerns IP providers and consumers should be aware of
- A single attribute, the IP ‘Family,’ is used to relate CIPCSE items to IP products
- It is expected that design tools will be able to use this information to automate security analysis and probe for residual concerns in IP and the products that integrate it

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Thank You

Please Continue with Part 4

Thank you to our Accellera Global Sponsors

cadence®

Mentor® A Siemens Business

SYNOPSYS®

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

IP Security Assurance Workshop

Part 4: SUPPLIERS AND INTEGRATORS' OBLIGATIONS IN CONTEXT OF EMERGING IPSA STANDARD

Adam Sherer, Cadence Design Systems, Inc.

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Notes From The Future

- Thanks to Accellera Safety WG, we have safe flying cars
- Thanks to members of Accellera IPSA, we have secure flying cars
- Thanks to electronics community, IPSA is in broad use
  - IP suppliers (IPS) adopted best practices (obligations) for trusted IP delivery
  - IP integrators (IPI) adopted best practices (obligations) to maintain trusted value

accellera SYSTEMS INITIATIVE

IPS: Coding IPSA Tables

- IPSA tables should be both human and machine readable
  - JavaScript Object Notation (JSON) was chosen by WG
  - JSON has increasing popularity and smaller footprint for easier documentation
  - JSON is human readability

- At least two engineers should code tables
  - Ideally different disciplines (i.e., design and verification/test engineers)
  - Provides a more secure check-and-balance
  - Employ document management system to trace all changes

IPS: Automated Analysis

- Use formal techniques wherever possible
  - Identify attack surfaces from assets
  - Search for unanticipated or unexpected assets
- Trust but verify IPSA tables against the IP
  - Use formal engines that accept machine readable form of tables
  - Automatically gather coverage documenting completeness of analysis

IPS: Encrypt … or Not

- Encrypt IP and tables to lock-down interface
  - Pro: limits integrator's ability to circumvent APIs
  - Con: may require additional documentation/auditing to create trust with integrator
  - Note: requires that IPSA tables are machine readable

- Provide source code for IP and tables
  - Pro: provides integrator with straightforward path to trust but verify
  - Con: enables integrator to alter/modify APIs potentially exposing new attack surfaces

IPS: TCL to Maintain

- Modeled on automotive ISO26262 Tool Confidence Level (TCL) metrics
- Maintain currency of IP and IPSA tables
  - Rerun automated validation with new EDA release
- Maintain security manuals
  - Document intended use of APIs
  - Document known errata – both functional and security – for the IP
- Maintain tools and analysis with current IPSA standard

IPI: Know the IP

- Learn the IP functionality
  - Expert review of all IP documentation – both functional and security
  - Conduct API design review with IP supplier

- Identify potential threats associated with IP in target system
  - Expert assessment by IPI's security engineer

IPI: Trust but Verify

- Verify IP package received
  - Validate receipt of correct IP through checksum, watermark, etc.
- Verify functionality and security
  - Regenerate IPSA collateral to validate it matches received IP package
  - Use formal engines to validate IPSA tables to IP APIs
  - Use automation to validate IP to known threats data base (e.g., Mitre CWE)
- Take action on any anomalies
  - Report errata to IPS
  - Seek new IPS

IPI: On-going Analysis

- Continue to monitor IPS updates
  - Integrate patches prior to fabrication (ASIC) or on-going (FPGA)
- Maintain security analysis throughout product lifecycle
  - Continue to validate integrated IP against threat database(s)
- Follow all guidelines for derivatives and new products
  - Don’t assume what was secure remains secure (back to trust but verify)
- Plan/anticipate for hardware risks as new threats will arise

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Summary

- Security is, and will always be, continuously changing
- Establish a culture of security
  - Reinforces both IP supplier and integrator obligations
  - Provides vigilance and checks for emerging threats
- Stay current
  - Tools (automation) are critical to managing cost and project time

accellera SYSTEMS INITIATIVE

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Thank You

Thank you to our Accellera Global Sponsors

cadence®

Mentor® A Siemens Business

SYNOPSYS®

accellera SYSTEMS INITIATIVE