2022 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

An Overview of Security Annotation for Electronic Design Integration (SA-EDI) Standard

Sohrab Aftabjahani, PhD, SIM, SAM
Senior Staff Security Researcher, Product Security Expert
Intel Corporation

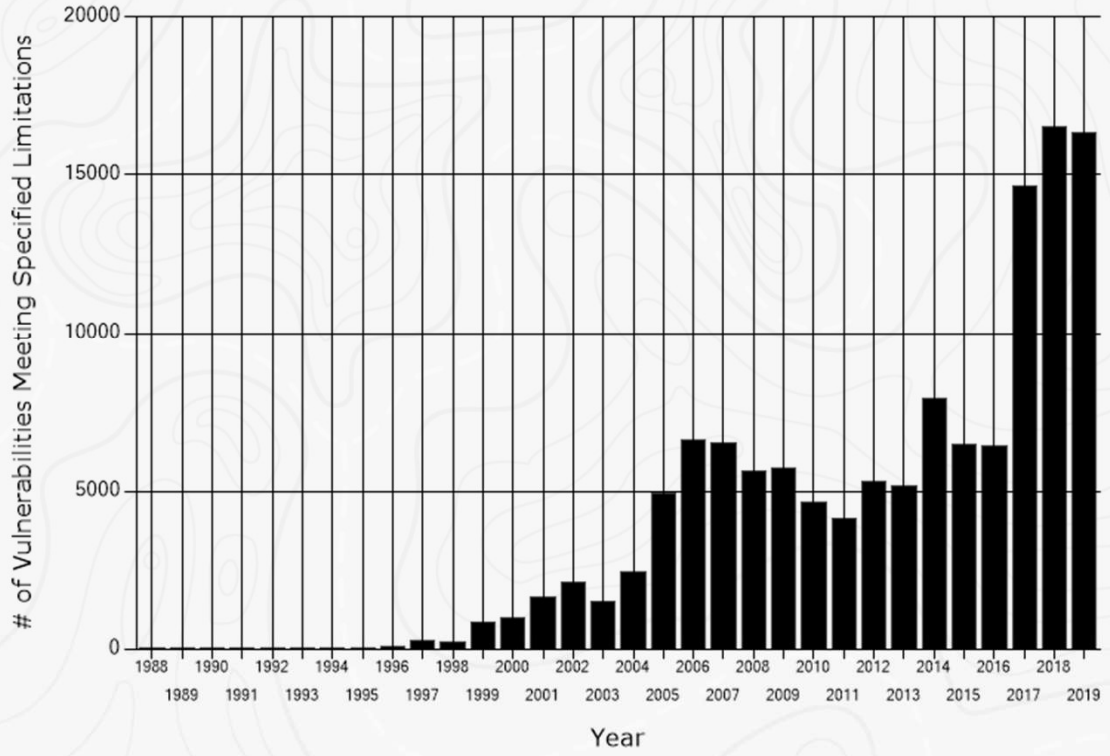
Representing Accellera IPSA WG
With valuable contributions of the IPSA WG

accellera SYSTEMS INITIATIVE

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

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

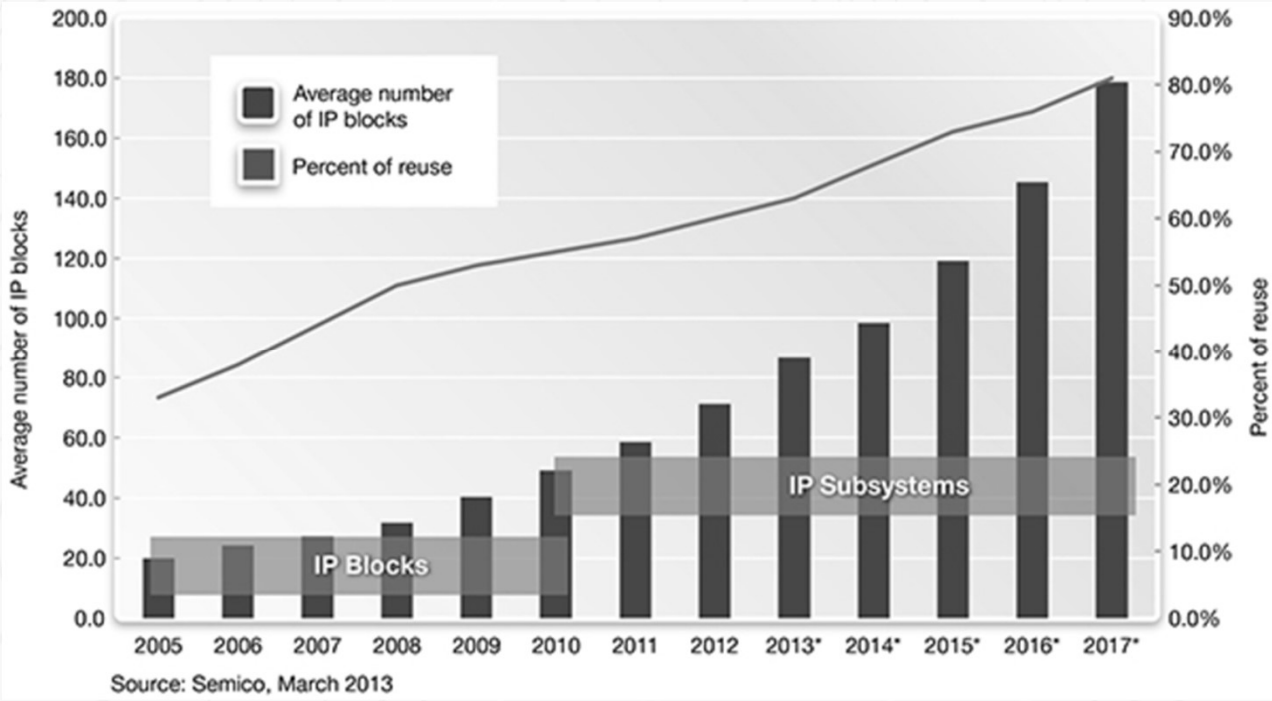
Increasing demands for:

- 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

Existing Work

- Some ISO efforts address security or impact security – but none cover security assurance for COTS IP

ISO#	Title
15408	Common Criteria
20243	Open Trusted Technology Provider Standard (O-TTPS)
26262	Functional Safety (Auto)
21434	Cybersecurity for Automotive
27001	Information Security Management System (ISMS)
27034	Application Security

  - ISO 27034 is the closest, but does not address hardware and the standard has stalled
  - ISO 21434 does address hardware components, however, does not dive at the IP level

Industry Technical Paper

- Intel led an effort to author an industry technical paper, published April'17
  - Co-authored with Qualcomm, Cadence, & Synopsys

- Good starting point however has limitations:
  - Fixed – difficult to support growth
  - Small sample group (4 companies)
  - Does not address accuracy, completeness, or quality of the collateral

J Hardw Syst Secur (2017) 1:38–55
DOI 10.1007/s41635-017-0002-5

CrossMark

Security Assurance Guidance for Third-Party IP

Brent Sherman[1] · Mike Borza[2] · Brian Rosenberg[3] · Charles Qi[4]

Received: 14 November 2016 / Accepted: 20 March 2017 / Published online: 7 April 2017

Abstract System OEMs are increasingly adopting the motto "Trust but verify" when it comes to their supply chains. After several public incidents in which trusted vendors unknowingly provided vulnerable components, OEMs are requesting evidence of security assurance before integrating components into their products. It can be problematic for semiconductor vendors to provide such evidence since their products often contain 3rd party components that are typically treated as black boxes. Moreover, asking 3rd party vendors to provide such evidence for their components is equally problematic due to the many integration unknowns and a lack of applicable literature on security assurance for standalone technologies. We address these issues by defining a security process and relationship between semiconductor vendors and trusted 3rd party component providers and a practical methodology to produce standardized quality security assurance evidence. We provide example applications of the methodology using several open source components.

Keywords Threat model · Security assurance · Security development lifecycle · Commercial Off-the-Shelf (COTS) · IP development

✉ Brent Sherman
brent.m.sherman@intel.com

[1] Intel Corporation, Hillsboro, OR, USA

[2] Synopsys, Inc., Kanata, Ontario, Canada

[3] Qualcomm Technologies, Inc., San Diego, CA, USA

[4] Cadence Design System, Inc., Santa Clara, CA, USA

Springer

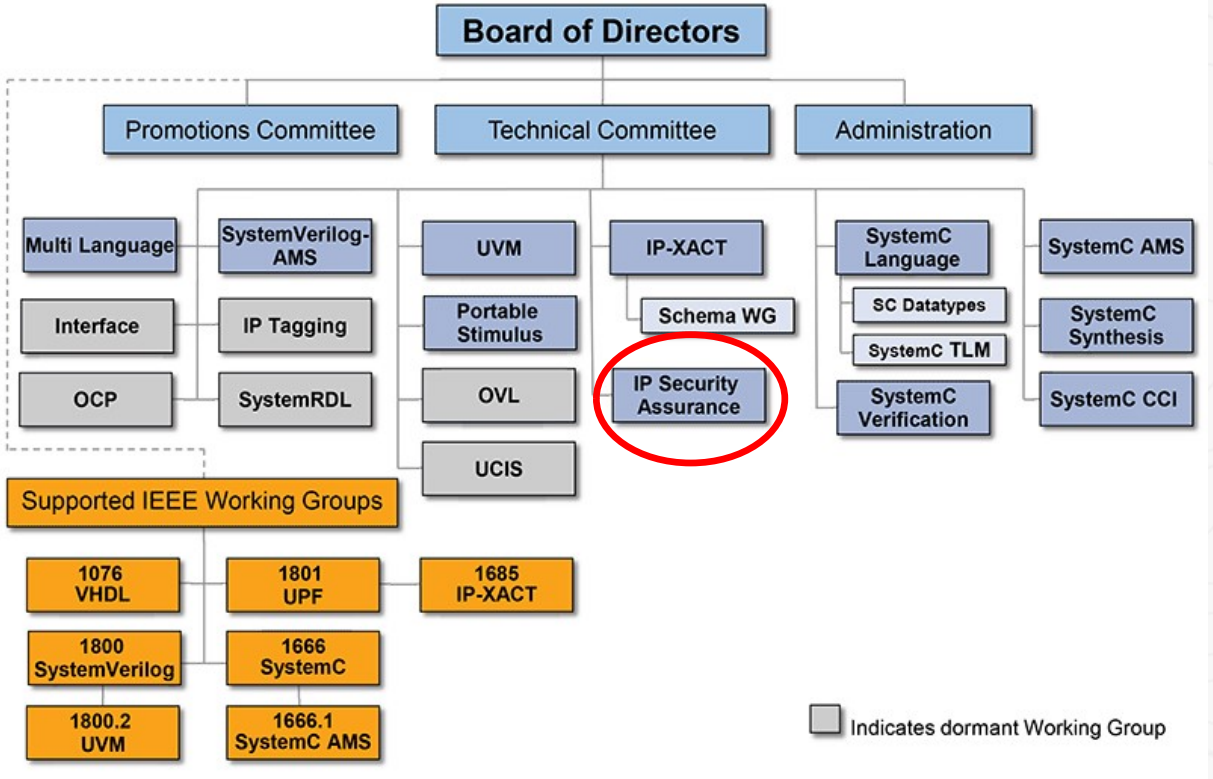
1 Introduction

There have been several incidents in which system OEMs have suffered costly security vulnerabilities due to 3rd party components [1–4]. As far as we are aware, all were caused by software components, making the mitigation of these vulnerabilities relatively simple (e.g., patch, disablement, or removal). However, mitigating a similar problem arising from insecure hardware would require an expensive recall. To help manage security risk, OEMs are requesting hardware vendors to provide evidence of security assurance to increase confidence in a component's quality. In general, semiconductor vendors will be able to accommodate these requests, since they know the data flows, use cases, interdependencies, etc. of their silicon, all of which are needed to perform security assessments using existing methodologies [5–8]. However, if the vendor has integrated 3rd Party Intellectual Property (3PIP, IP), their knowledge alone would typically not be sufficient to produce quality security assurance evidence. Most semiconductor vendors view 3PIP as black box technology that hooks into their silicon and "just works." Furthermore, 3PIP is often provided only as a netlist, which limits what security evaluation a semiconductor vendor (now functioning as an Integrator) can perform. An Integrator can perform security design checking [18] and/or formal verification; however, these can be time consuming and still not address all integration security concerns. Therefore, Integrators depend on trusted IP providers to produce security assurance collateral for their technologies. However, existing security assurance methodologies require system level information in order to complete. Unfortunately, this information is rarely available to IP providers, mainly because 3PIP is designed, developed, and productized well before Integrators define their product requirements. It is not uncommon for Commercial

Link

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.
- Timeline:
  Dec'17 – Pitched to Accellera BoD
  Mar'18 – PWG Announced Press Release
  Oct'18 – WG Kicked off



https://www.accellera.org/

Accellera: IP Security Assurance Workgroup

The initial scope for the Working Group is to define an automatable systematic approach that can be consistently supported across multiple target implementations. The WG will focus on existing standards that pertain to IP specification, design, verification and integration where security risk is a concern, as well as known security concerns that have been identified by either industry experience or security researchers.

- Members: 60
- Companies: 18

AMD	Marvell	Qualcomm
Analog Devices	Mentor Graphics	SiFive
ARM	Methodics	Synopsys
Cadence Design Systems	NVIDIA	Texas Instruments
Infineon Technologies	NXP Semiconductors	Tortuga Logic
Intel	OneSpin Solutions	Xilinix

- University: 1
  - University of Maryland
- Workgroup meets Biweekly (Tuesday)

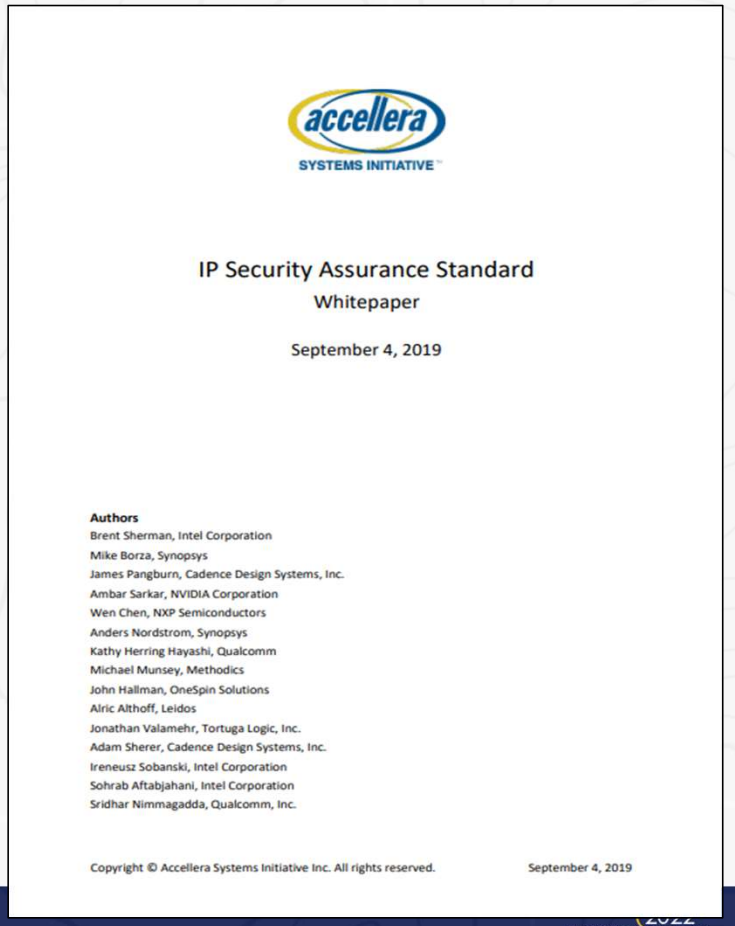
Source: Internal Accellera data

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)

White paper: 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

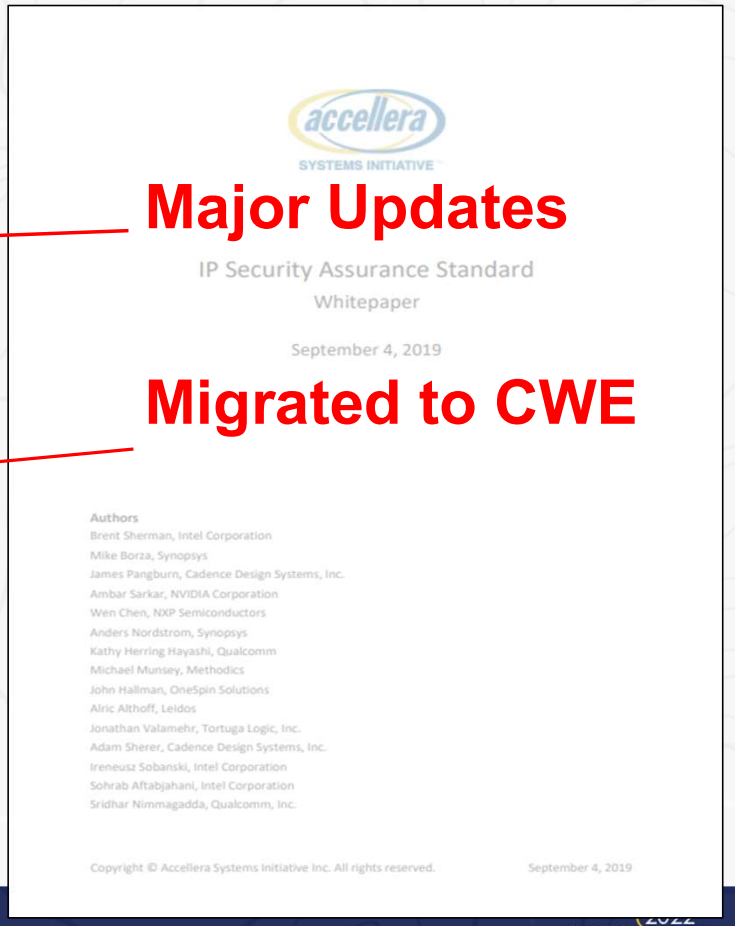
Authors

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.

September 4, 2019

White paper: 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



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
  - **Now expanded into hardware weaknesses (95 in v4.3)**
- The CWE Compatibility Program recognizes products or services that leverage CWE

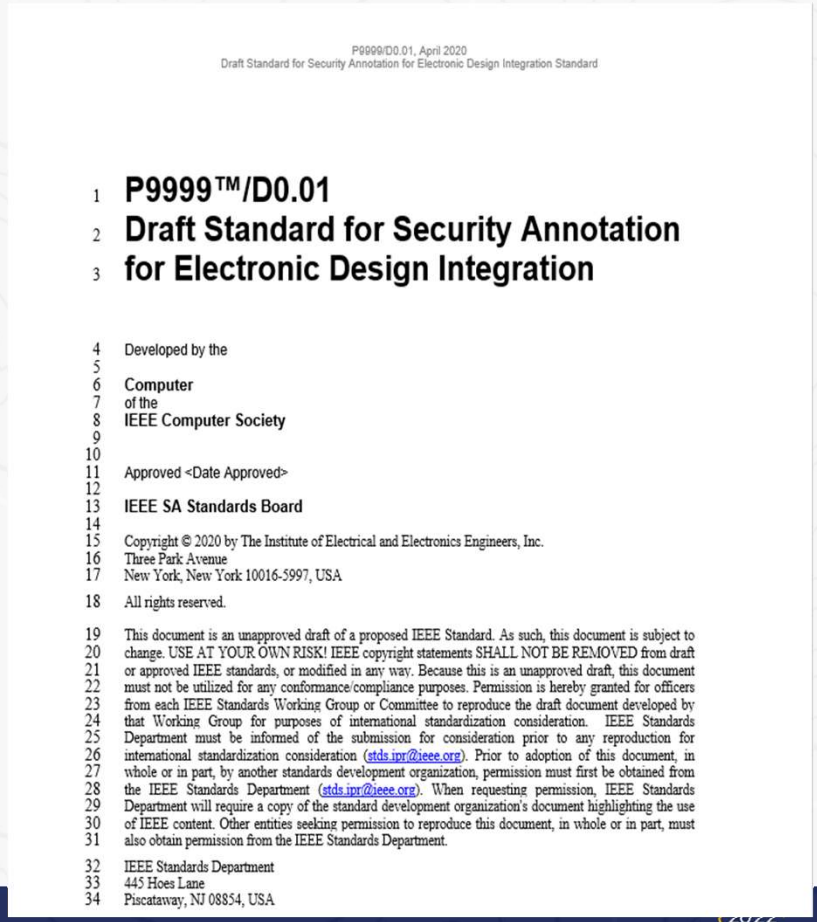
With industry partners, CWE expanded into enumerating hardware weaknesses and is seeking further collaborators and contributors to help grow the effort.

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

MITRE

Introducing: SA-EDI Standard

- IEEE format
  - IEEE standard is the end goal
- Draft complete (45pp)
- Accellera Public Release
  - July 2021, 21 authors, 11 companies
  - Available online through Accellera:
  [Security Annotation for Electronic Design Integration Standard]
- EDA's Companies' PoC/Demo @ DAC'21
  - Tortuga Logic ™
  - Methodics ™


P9999/D0.01, April 2020
Draft Standard for Security Annotation for Electronic Design Integration Standard

P9999™/D0.01
Draft Standard for Security Annotation for Electronic Design Integration

Developed by the

Computer
of the
IEEE Computer Society

Approved <Date Approved>

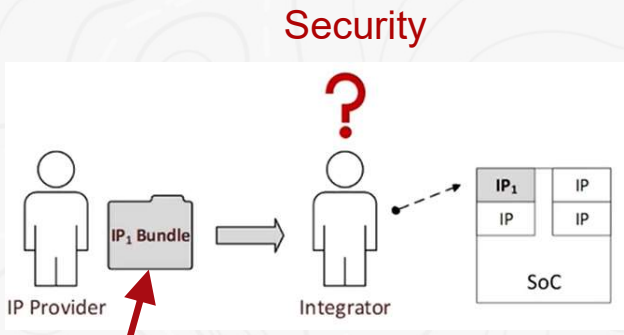
IEEE SA Standards Board

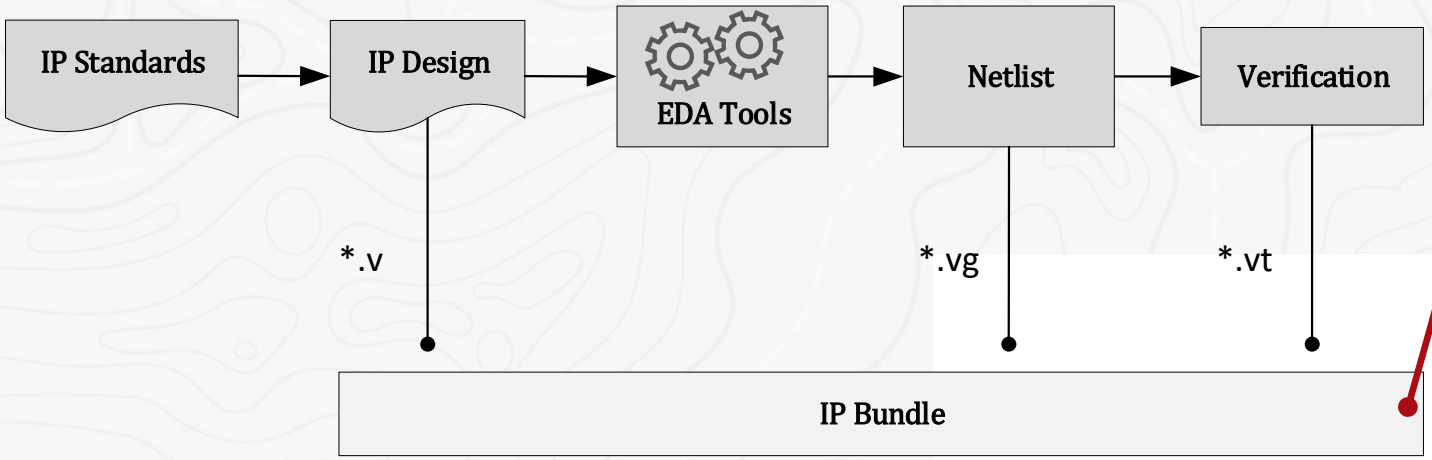
IEEE Standards Department
445 Hoes Lane
Piscataway, NJ 08854, USA

SA-EDI Standard

- Objectives:
  - Improve trustworthiness of IPs and IP providers
  - Assist IP integrators in understanding and reducing security risk
  - Accelerate tool development to enable scalable security assurance
- Properties:
  - Uses JSON data modeling
    - Required fields help consistency
    - Expansion supported for proprietary information
  - Binds the data objects to the RTL
    - Automatable and verifiable
  - Outside the design so can be applied to existing IP
  - Low overhead
    - Only 4 data object types

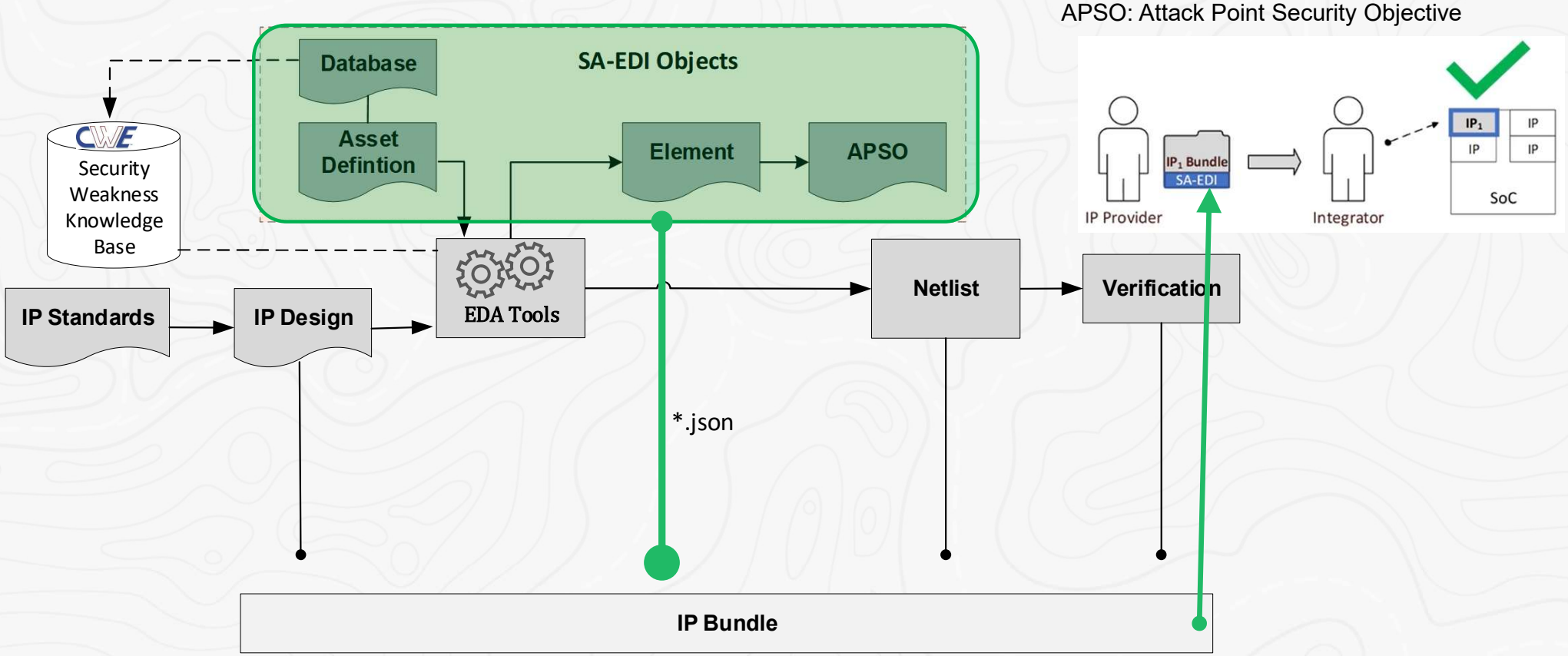
Today's IP Design Flow





Security annotations are not part of the IP bundle to be used/verified by integrators ☹

Future's IP Flow w/ SA-EDI Data Objects

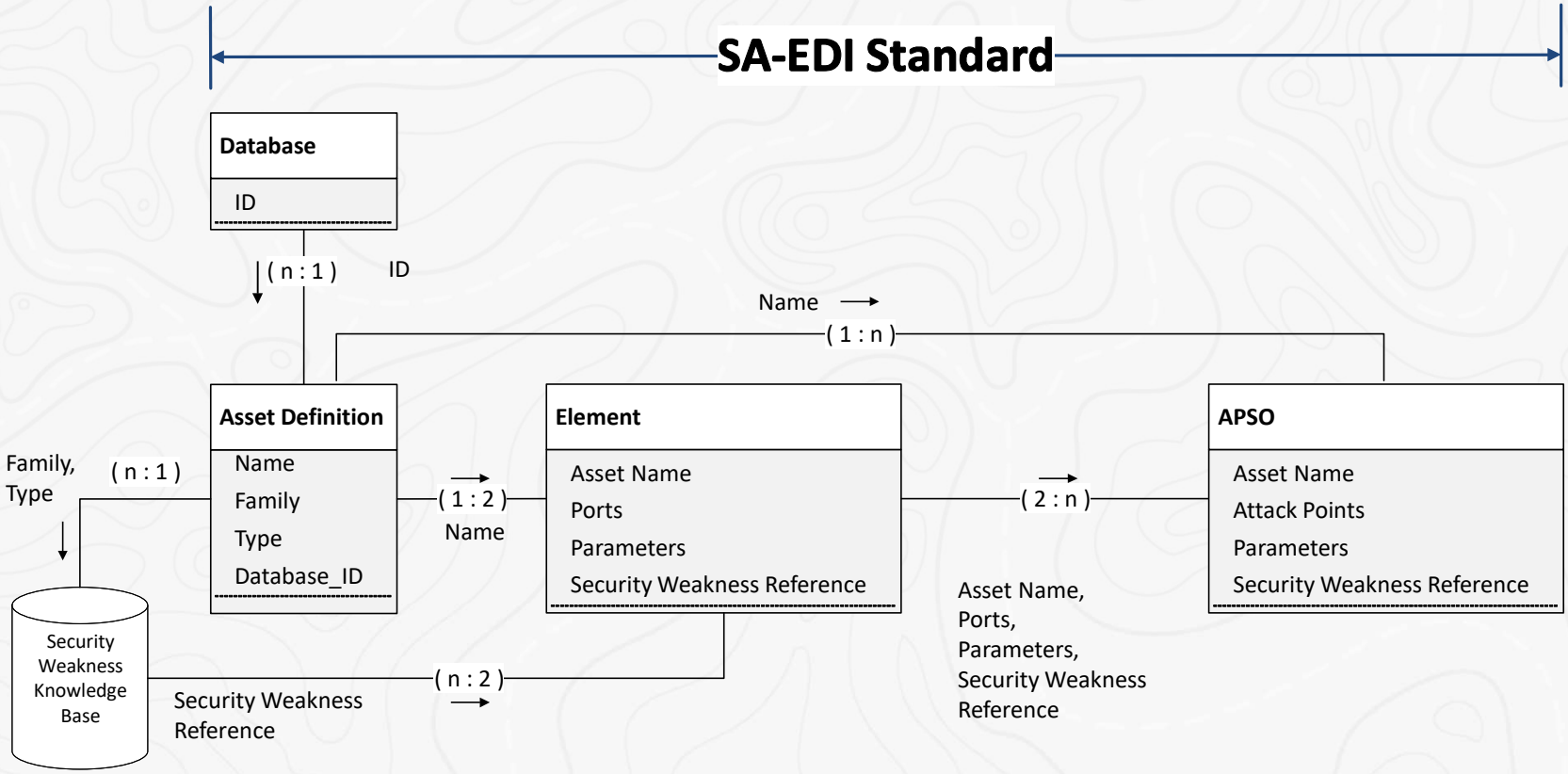


Security annotations are added to the IP bundle to be used/verified by integrators ☺

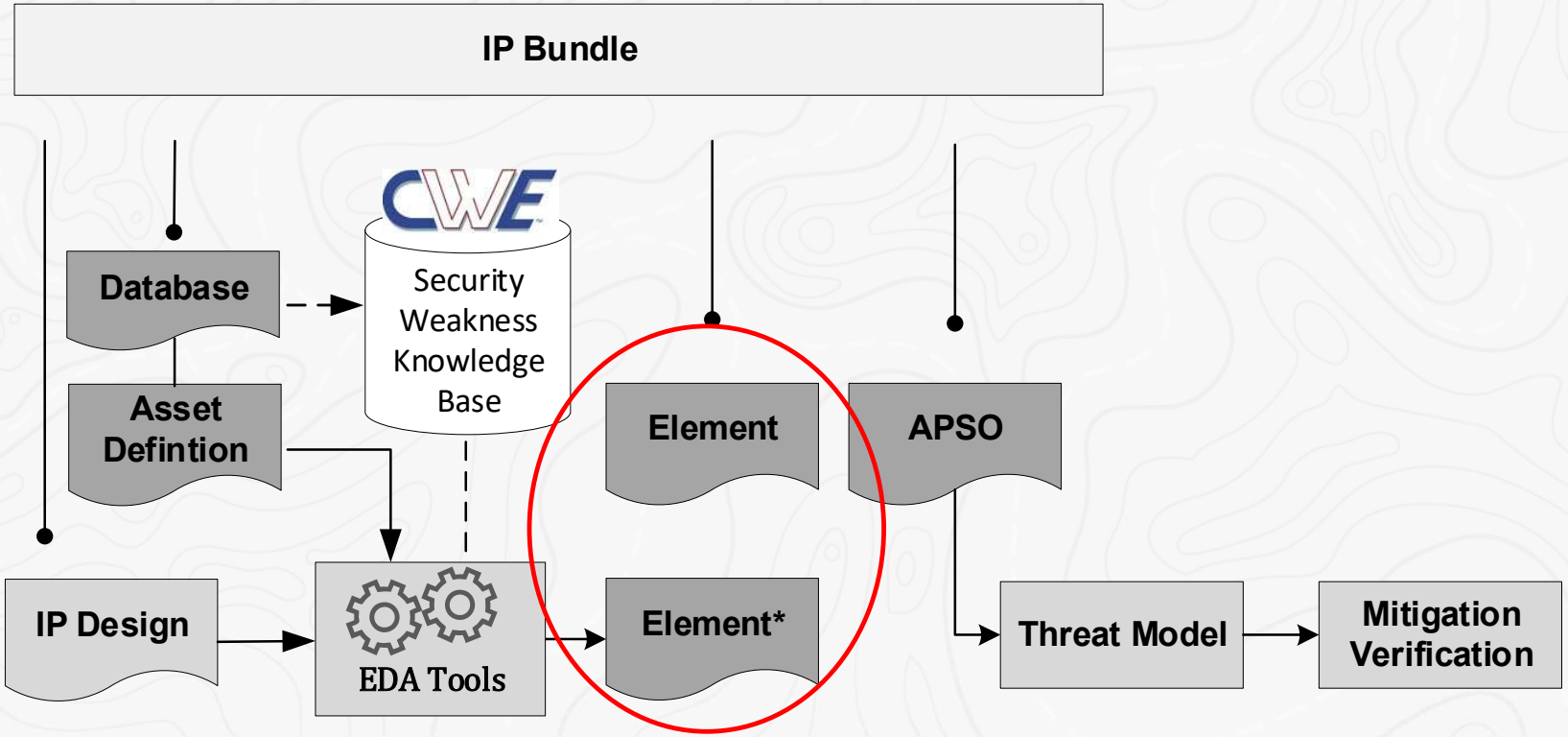
SA-EDI Data Objects

- Database (Manual)
  - Key attributes defining a security weakness database (e.g., CWE)
- Asset Definition (Manual)
  - Root object that identifies assets in the IP
    - Asset = anything of value/importance (e.g., security objective)
- Element (Generated)
  - Identifies input/output ports and configuration parameters that can influence and/or observe the asset
- APSO - Attack Points Security Objective (Manual)
  - Assigns a security objective and attack points (Elements) to an asset
    - Confidentiality, Integrity, Availability
  - Identifies conditions that might violate the security objective

Data Object Associations



IP Bundle: Integrator



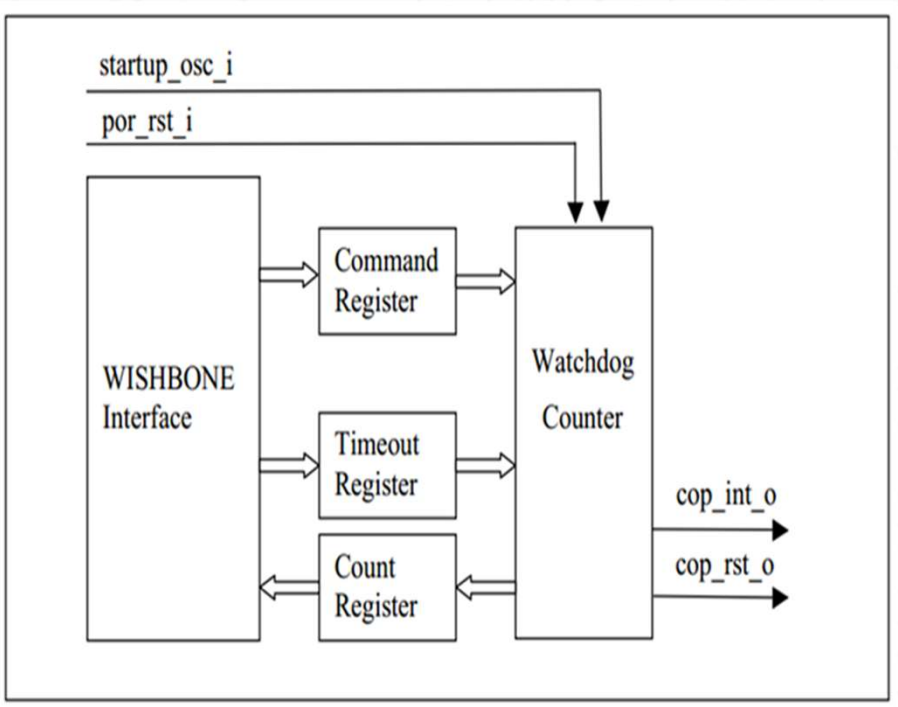
IP Integrator: Verifies; Threat Model

1. Verify the existence of the SA data objects
2. Using RTL source and Asset Definition object, re-generates the Element object(s) (E*)
3. Compares E* with the Element object(s) in the IP Bundle (E)
   - E* == E then SA collateral matches RTL. Use IP.
   - E* != E then stop; RTL/SA collateral out of sync.
4. Decide which APSO objects are in scope of the SoC/IC
   - Becomes part of the product's threat model
5. Identify additional APSO objects for integration
   - Becomes part of the product's threat model
6. Perform verification on the threat model

Example: OpenCore COP - Watchdog

- Simple watchdog IP
- Configured through Wishbone Interface
- Write-protection lock
- Non-standard debug signals

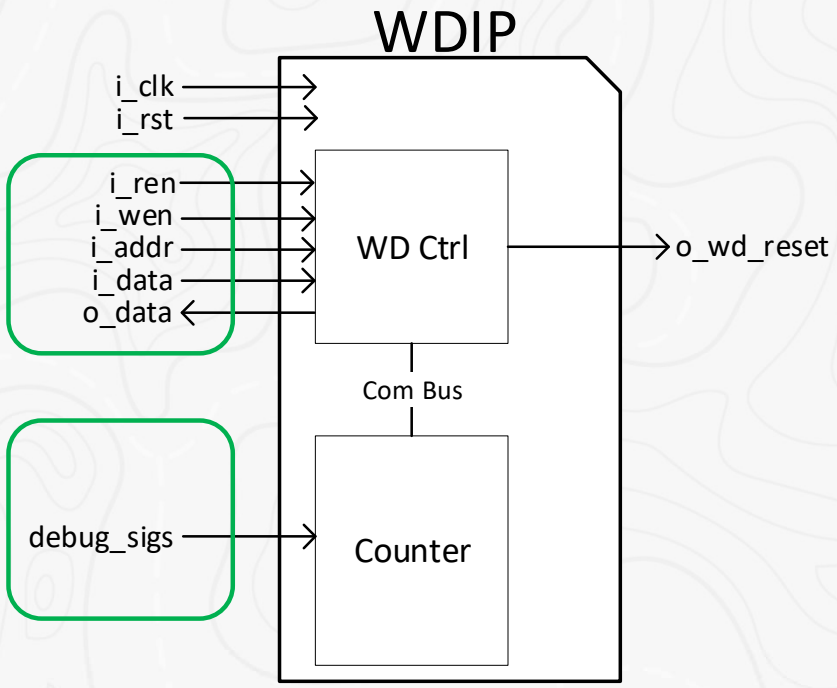
- Asset: 16bit Counter in module cop_count
  - output reg [15:0] cop_counter



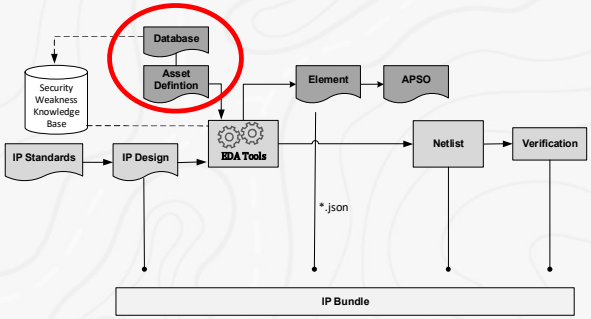
OpenCores. COP. Retrieved from http://opencores.org/websvn,listing?repname=cop&path=%2Fcop%2F&rev=0

Example: Watchdog Timer

- Simple timer – two interfaces:
  - 8-bit bus to access registers
  - Debug signals (overrides registers)
    - 8 wires/buses total
- WD Crtl – RTL to configure and control the timer
- Counter – RTL that is the timer



Step #1: Identify the Asset(s) and Knowledge Base

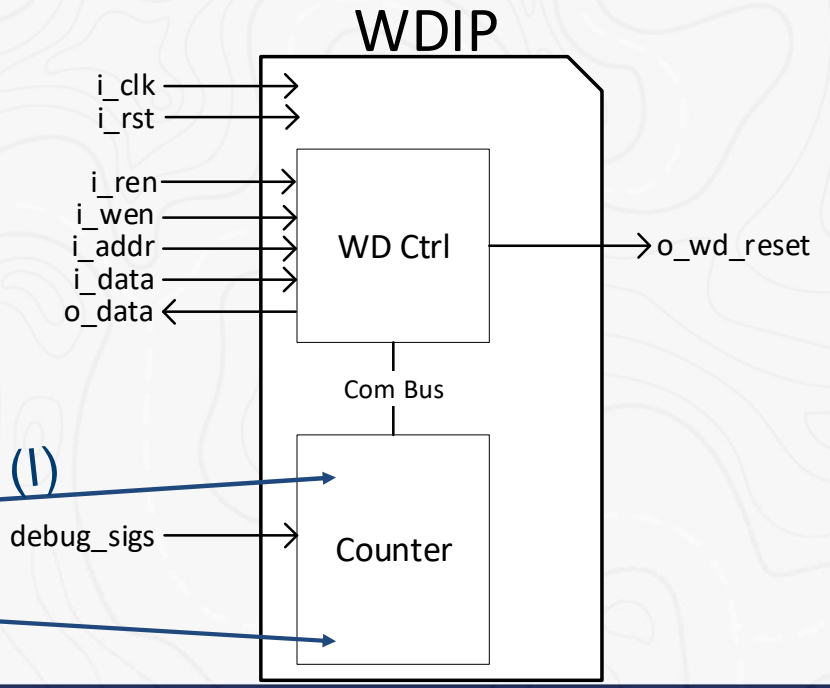


- What's critical to proper functionality?
- Does the IP have any security objectives (CIA)?

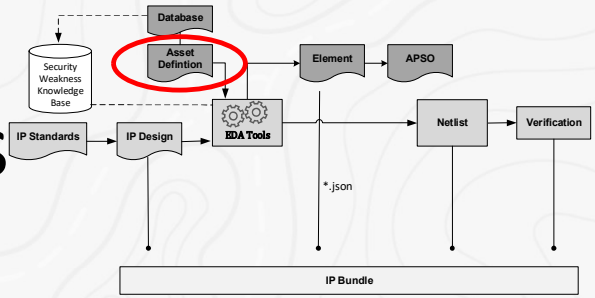
```
module wd_count #(parameter COUNT_SIZE = 16)
(
        output reg [COUNT_SIZE-1:0] wd_timer;
        …
        reg wd_assert_timeout;
)
```

(I)

(I)



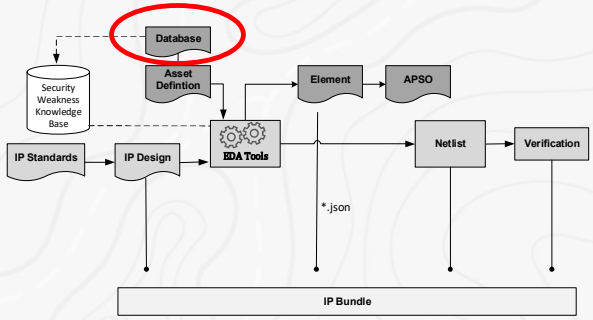
JSON: Asset Definition Objects




```
{
    "Name" : "wd_top.count_block.wd_count.wd_timer",
    "Description" : "Timer count status.  Critical for proper operation",
    "Family" : ["Counter/Timer","Test/Debug"],
    "Type" : ["Control", "Critical"],
    "Database_ID" : ["CWE VIEW: Hardware Design"]
}

{
    "Name" : "wd_top.count_block.wd_count.wd_assert_timeout",
    "Description" : "Reset assertion signal.  Critical for proper operation",
    "Family" : ["Counter/Timer","Test/Debug"],
    "Type" : ["Control", "Critical"],
    "Database_ID" : ["CWE VIEW: Hardware Design"]
}
```

JSON: Database Object

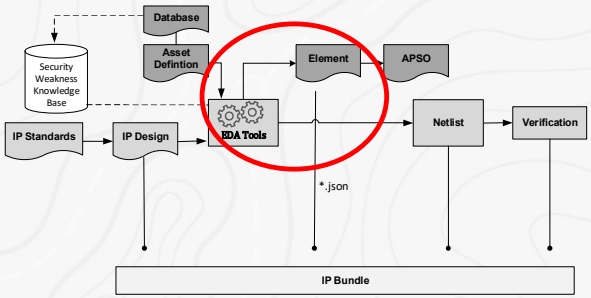



```
{
        "ID" : "CWE VIEW: Hardware Design",
        "Description" : "A community developed list of hardware weakness types",
        "URI" : "https://cwe.mitre.org/data/definitions/1194.html",
        "Version" : "4.3"
}
```

CWE is a formal list of known weakness types: https://cwe.mitre.org/

- Began with a focus on software weaknesses (now 800+) and has published several iterations of the Top 25 Most Critical Software Errors
- Now expanded into hardware weaknesses (95 in v4.3)

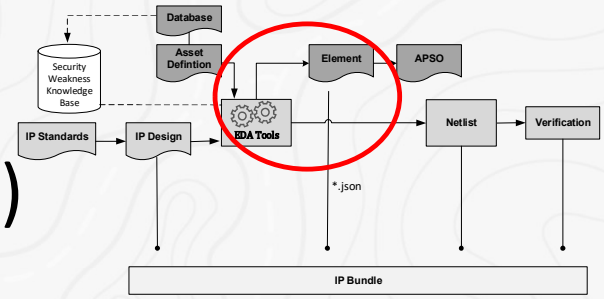
Step #2: Generate Element Objects (wd_timer)




```
{
    "Asset Name" : "wd_top.count_block,wd_count.wd_timer",
    "Direction" : "Input",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Ports" : [
        "wd_top.i_rst",
        "wd_top.i_clk",
        "wd_top.i_ren",
        "wd_top.i_wen",
        "wd_top.i_data",
        "wd_top.i_addr",
        "wd_top.i_dbg_enable",
        "wd_top.i_dbg_clk_en",
        "wd_top.i_dbg_clk",
        "wd_top.i_dbg_pause",
        "wd_top.i_dbg_start",
        "wd_top.i_dbg_service",
        "wd_top.i_dbg_cnt_val" ],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

```
{
    "Asset Name" : "wd_top.count_block.wd_count.wd_timer",
    "Direction" : "Output",
    "Security Weakness Reference":["CWE-1244","CWE-1191","CWE-1234"],
    "Ports" : ["wd_top.o_data"],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

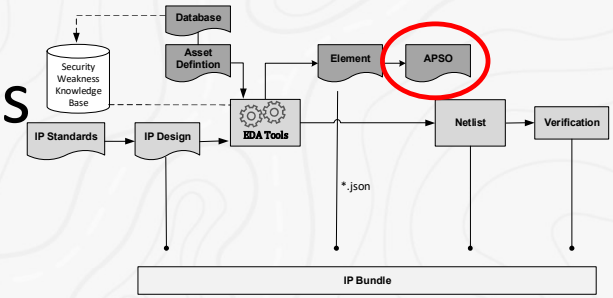
Step #2: Generate Element Objects (wd_assert_timeout)




```
{
    "Asset Name" : "wd_top.count_block,wd_control.wd_assert_timeout",
    "Direction" : "Input",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Ports" : [
        "wd_top.i_rst",
        "wd_top.i_clk",
        "wd_top.i_dbg_enable",
        "wd_top.i_dbg_timeout",
        "wd_top.i_dbg_cnt_val"],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

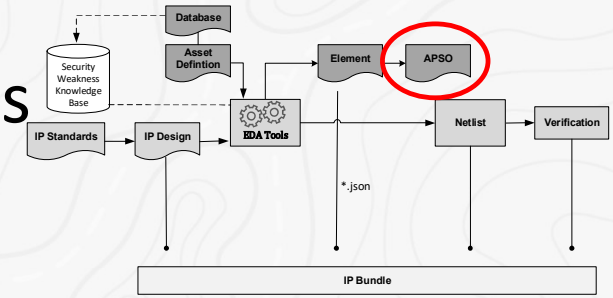
```
{
    "Asset Name" : "wd_top.count_block.wd_control.wd_assert_timeout",
    "Direction" : "Output",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Ports" : ["wd_top.o_wd_reset "]
}
```

Step #3: Create APSO objects (wd_timer)



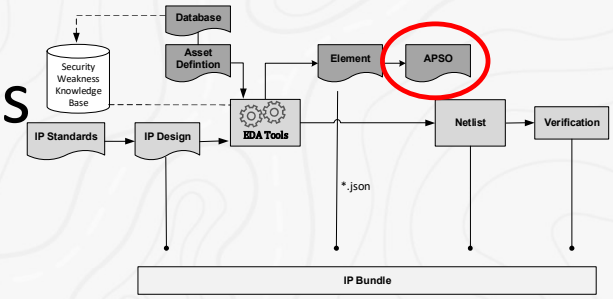

```
{
    "Name" : "SO_1",
    "Asset Name" : "wd_top.count_block.wd_count.wd_timer",
    "Security Objective" : "Integrity",
    "Description" : "If the lock bit is not enabled then the counter can be altered",
    "Condition" : "(wd_top.i_addr = 0x3) && (wd_top.i_data[0] = 0)",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Attack Points" : [
        "wd_top.i_wd_rst",
        "wd_top.i_wd_clk",
        "wd_top.i_enb",
        "wd_top.i_addr",
        "wd_top.i_data"],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

Step #3: Create APSO objects (wd_timer)



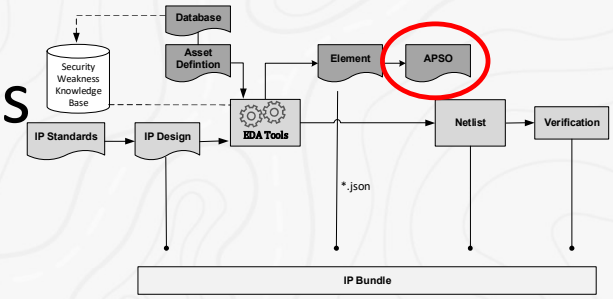

```
{
    "Name" : "SO_2",
    "Asset Name" : "wd_top.count_block.wd_count.wd_timer",
    "Security Objective" : "Integrity",
    "Description" : "Debug signals can alter the counter",
    "Condition" : "wd_top.i_dbg_enable == 1",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Attack Points" : [
        "wd_top.i_dbg_enable",
        "wd_top.i_dbg_clk_en",
        "wd_top.i_dbg_clk",
        "wd_top.i_dbg_pause",
        "wd_top.i_dbg_start",
        "wd_top.i_dbg_cnt_val"],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

Step #3: Create APSO objects (wd_assert_timeout)



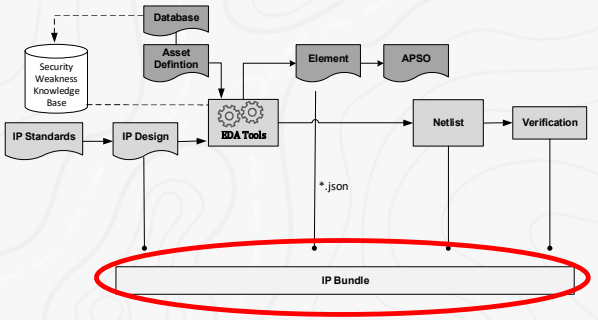

```
{
    "Name" : "SO_3",
    "Asset Name" : "wd_top.count_block.wd_count.wd_assert_timeout",
    "Security Objective" : "Integrity",
    "Description" : "Debug can assert a timeout at any time",
    "Condition" : "wd_top.i_dbg_enable == 1",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Attack Points" : [
        "wd_top.i_dbg_enable",
        "wd_top.i_dbg_timeout"],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

Step #3: Create APSO objects (wd_assert_timeout)



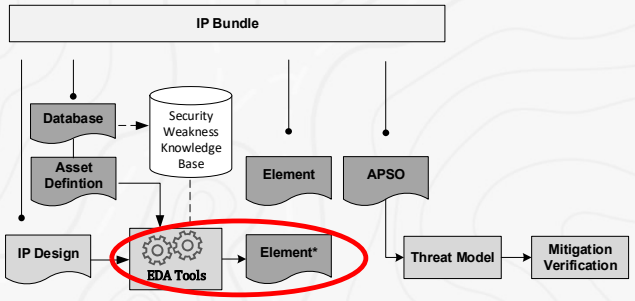

```
{
    "Name" : "SO_4",
    "Asset Name" : "wd_top.count_block.wd_count.wd_assert_timeout",
    "Security Objective" : "Integrity",
    "Description" : "Debug can assert a timeout by setting count value to 0",
    "Condition" : "wd_top.i_dbg_enable == 1",
    "Security Weakness Reference" : ["CWE-1244","CWE-1191","CWE-1234"],
    "Attack Points" : [
        "wd_top.i_dbg_enable",
        "wd_top.i_dbg_cnt_val"],
    "Parameters" : ["wd_top.COUNT_SIZE"]
}
```

Step #4: Create IP Bundle



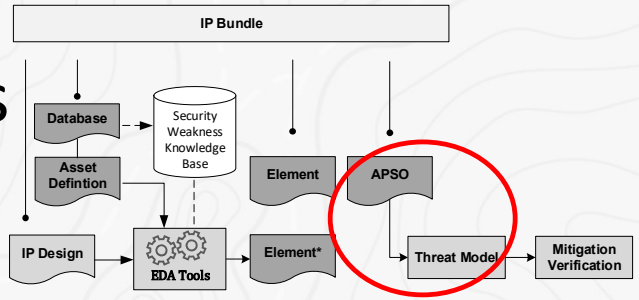
- IP Bundle contains:
  - 2 Asset Definition objects
  - 1 Database object
  - 4 Element objects
  - 4 APSO objects
  - RTL, netlist, etc.

Step #5: Integrator: Verify



1. Generates their own Element* objects from the provided Database and Asset Definition objects and RTL in the IP bundle
2. Compares Element* to Element in the IP bundle
   - If equal then continue
   - If not equal then stop (RTL does not align with the SA-EDI objects)

Step #6: Integrator Defines Threat Model

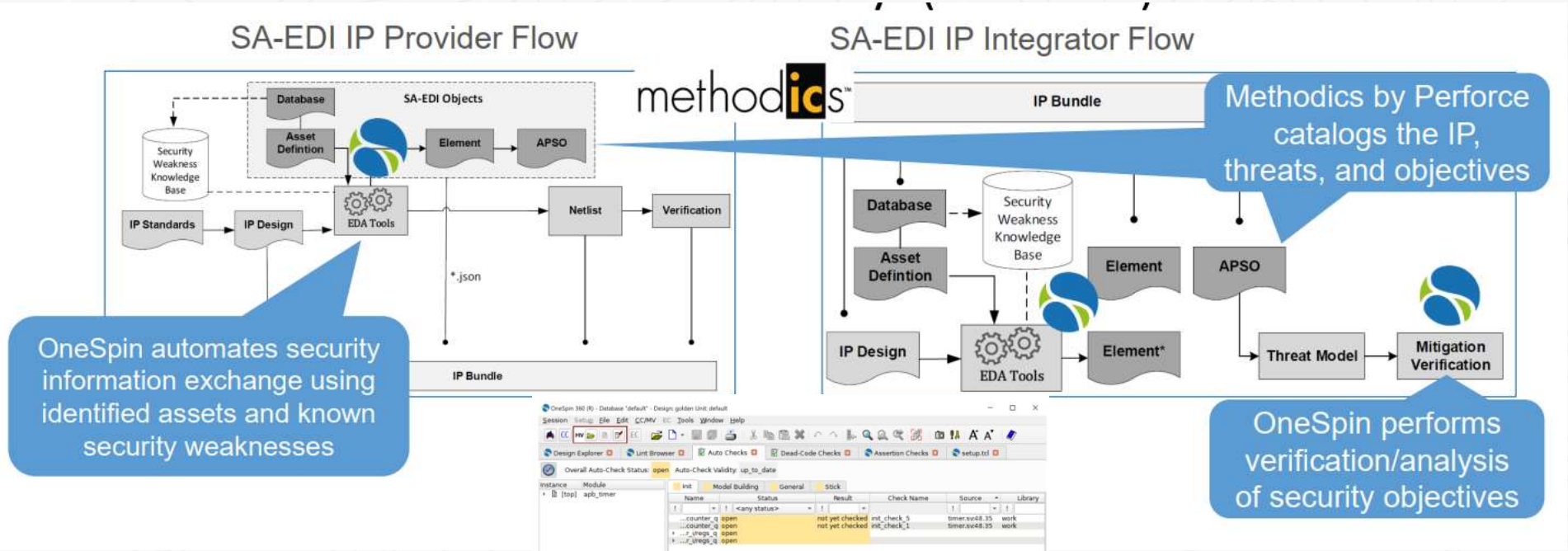


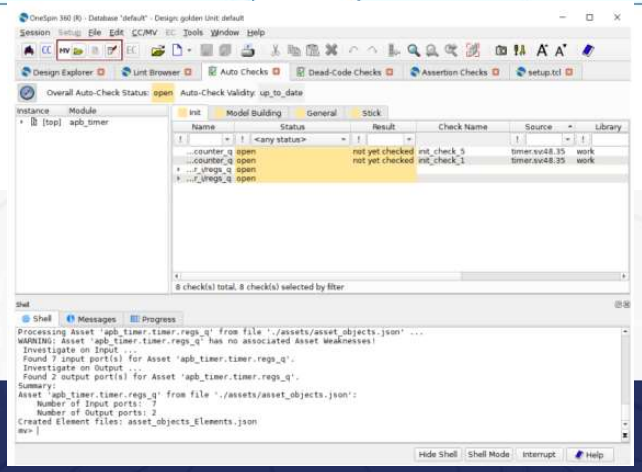
1. Decides which APSO objects are in scope
2. Finds additional APSO objects if needed

```
{
    "Name" : "SO_5",
    "Asset Name" : "wd_top.count_block.wd_control.wd_assert_timeout",
    "Security Objective" : "Availability",
    "Description" : "The timeout assertion should never be gated",
    "Attack Points" : ["wd_top.o_wd_reset"]
}
```

3. Creates integration verification tests for the security objectives

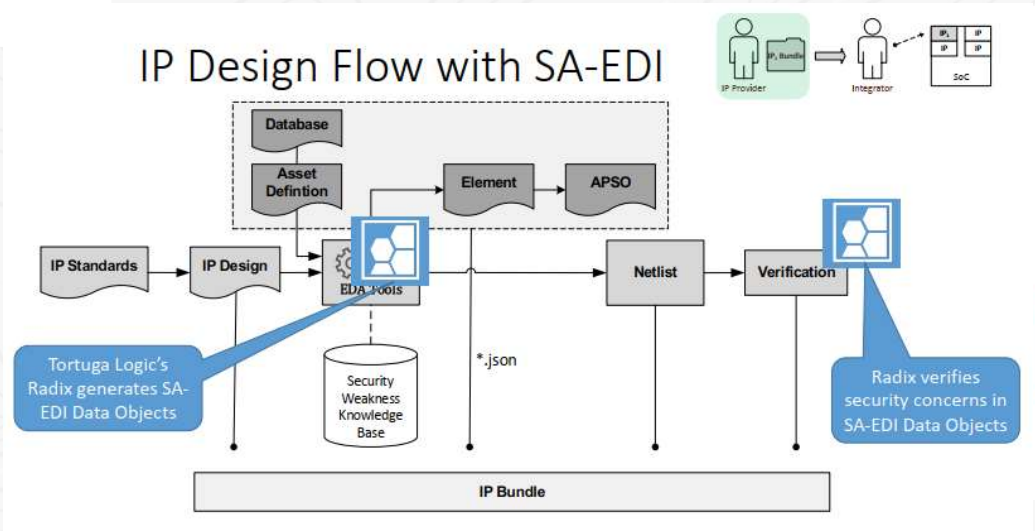
SA-EDI Demo 1 (Methodics™)

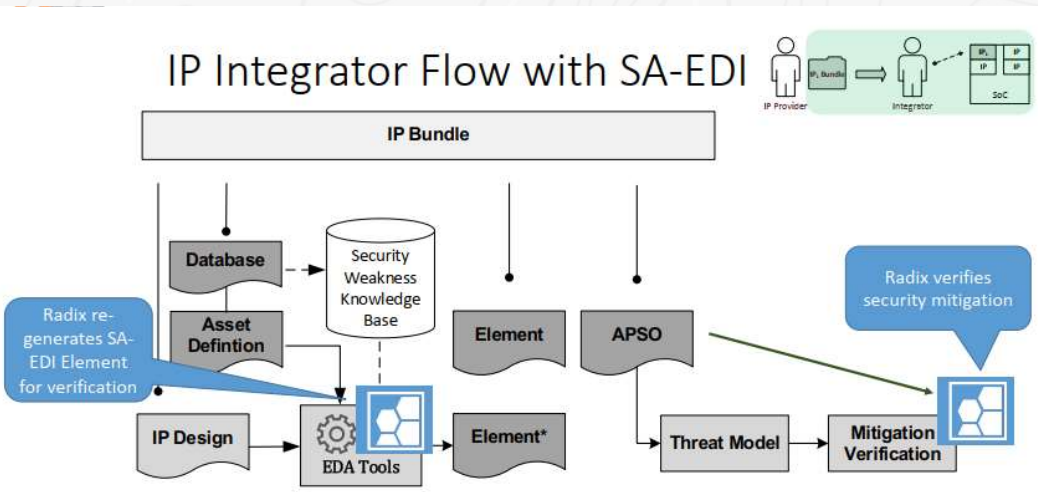


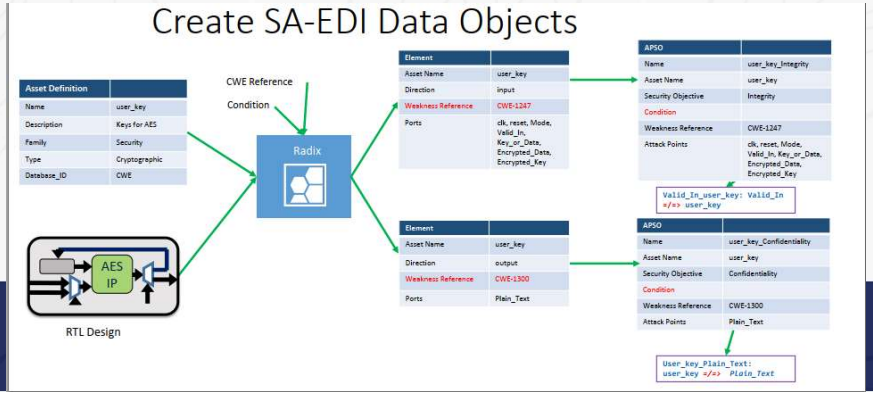


Source: SA-EDI Demonstration with OneSpin, a Siemens Business and Methodics IPLM by Perforce, Design Automation Conference, DAC 2021, John Hallman, Vishal Moondrha, Wayne Kohler

SA-EDI Demo 2 (Tortuga Logic™)

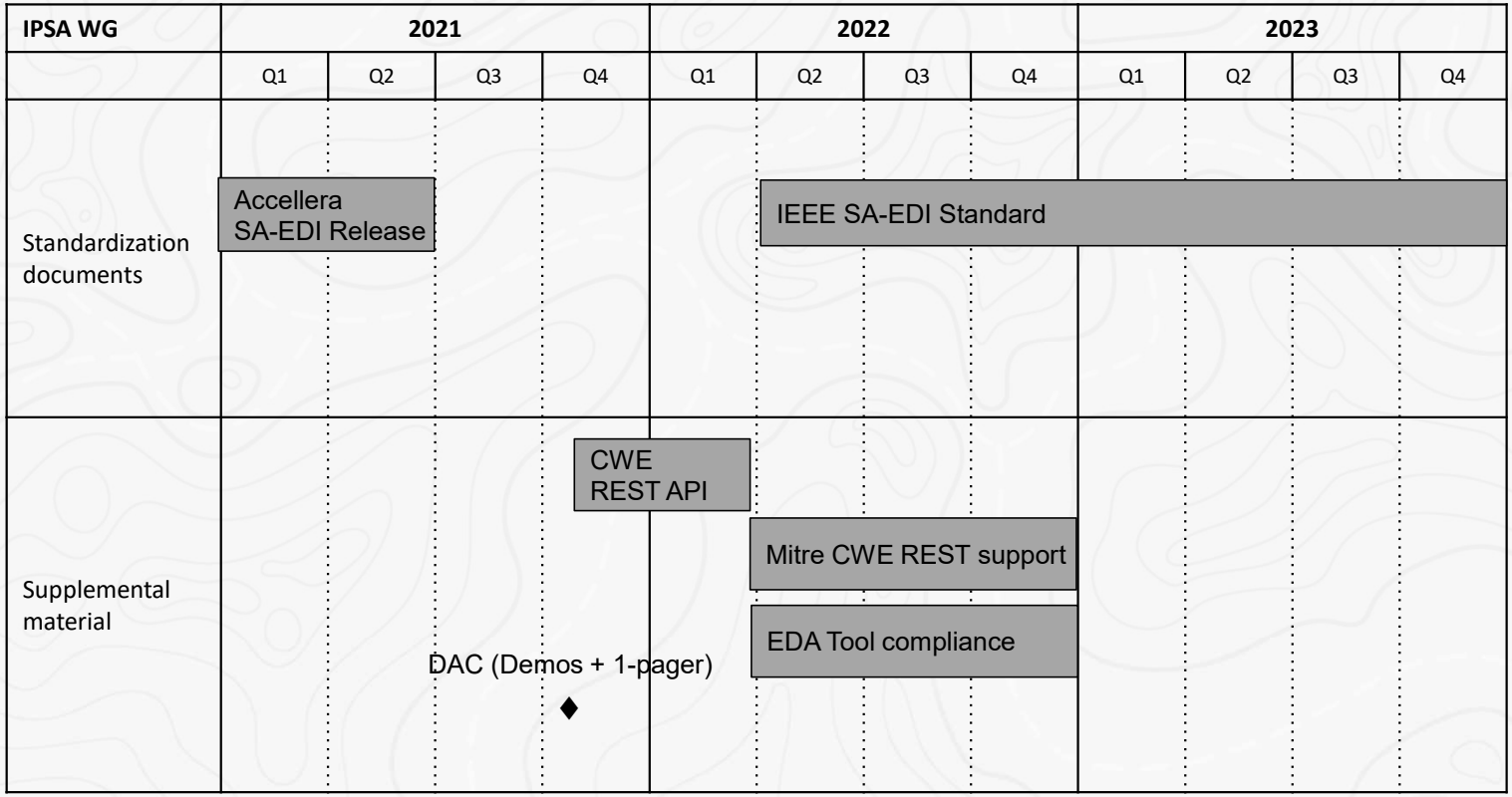






Source: SA-EDI Demonstration (II), IP Creator and Integrator Use Cases, Design Automation Conference 2021, Anders Nordstorm, Tortuga Logic

IPSA Roadmap



IPSA SA-EDI Standard - Summary

#	Requirements	Met?	Details
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

Please consider joining IPSA WG as we work on creating an IEEE standard out of SA-EDI.

Thank You

- 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

Questions

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