CAD for Hardware Security Automation is Key to Adoption of Solutions

Sohrab Aftabjahani
Sr. Staff Security Researcher, Product Security Expert,
Data Center ad Artificial Intelligence Product Group, Intel Corporation

CAD for Security Workshop (collocated with DAC 2022)

July 10, 2022

Why do we need CAD for Hardware Security?

Transitioning from Manual to (Semi/Fully) Automated

- Companies have been actively working on building their hardware security teams to incorporate security into their Product Development Lifecycle (PLC), i.e. Security Development Lifecycle (SDL)
  - SDL ypically includes planning, design, development, validation, manufacturing, testing, and support steps.
- To minimize residual security risks before product shipment, they use
  - Systematic approaches by security architects, product security experts (blue teams) to defend and
  - Ad-hoc approaches by security researchers (red teams) to attack their own products.
- A new generation of security-aware EDA tools incorporating novel scalable approaches and methods are necessary to provide
  - the level of security needed to be built into products
  - the required level of security assurance.

Special Session: CAD for Hardware Security - Automation is Key to Adoption of Solutions

Sohrab Aftabjahani
Dataplatform Engineering and Architecture
Intel Corporation
Hillsboro, USA
sohrab.aftabjahani@intel.com

Ryan Kastner
Department of Computer Science and Engineering
UC San Diego
San Diego, USA
kastner@ucsd.edu

Mark Tehranipoor
Department of Electrical and Computer Engineering
University of Florida
Gainesville USA
tehranipoor@ece.ufl.edu

Farimah Farahmandi
Department of Electrical and Computer Engineering
University of Florida
Gainesville USA
farimah@ece.ufl.edu

Jason Oberg
Totuga Logic
San Jose, USA
jason@tortugalogic.com

Anders Nordstrom
Tortuga Logic
San Jose, USA
andersn@tortugalogic.com

Nicole Fern
Tortuga Logic
San Jose, USA
nicole@tortugalogic.com

Alric Althoff
Tortuga Logic
San Jose, USA
alric@tortugalogic.com

***Abstract*— Although hardware security has received significant attention in the past decade or so, security design and validation engineers and researchers in industry, academia, and government have not still been equipped with a mature security-aware toolset to analyze designs for various types of security vulnerabilities at different levels of abstractions to detect and fix the security issues or build security in designs efficiently and easily. Despite such a demand, currently, there is not an ecosystem of security-aware Electronic Design Automation (EDA) or Computer-Aided Design (CAD) tools whereas the commercial design for security and validation tools are still in their infancy. However, there exist many research works that try to come up with security analysis engines and provide solutions to address different classes of security issues such as data leakage, access control violation, side-channel leakage, hardware Trojans and malicious changes, and vulnerabilities to physical attacks, fault-injection attacks, reverse engineering attacks, and chip counterfeiting or overproduction attacks. This paper presents the foundation established by several academic and industry researchers who have been supporting the realization of an ecosystem of security-aware CAD tools with their focus on hardware security coverage and fault-injection assessment for SoC designs, and security assurance standardization for electronic design integration.**

Keywords—CAD for Security, Hardware Security Coverage, Fault-Injection Attacks, Security Assurance, Electronic Design Integration.

I. INTRODUCTION

incorporate security into their Product Development Lifecycle (PLC) [3], i.e. Security Development Lifecycle (SDL) [3], which typically includes planning, design, development, validation, manufacturing, testing, and support steps. To minimize residual security risks before product shipment, this is an attempt to address their product security requirements using (a) systematic approaches by security architects, product security experts (blue teams) to defend and (b) ad-hoc approaches by security researchers (red teams) to attack their own products.

While the above trend is promising for the stronger hardware security posture of products around us in the market, SDL processes still lack the ideally required scalable, systematic, comprehensive security analysis engines as well as security modeling standards for creating and managing portable security-related design collaterals. Such collaterals generally include security claims of designs, security integration guidelines, and ideally threat models (security objectives, adversary profiles, assets and their security requirements for mitigating possible vulnerabilities, etc.). A new generation of security-aware EDA tools incorporating novel scalable approaches and methods are necessary to provide the level of security needed to be built into products as well as the required level of security assurance. The tools should take advantage of the speed and accuracy possible by automation and modern computation power while having the minimum impact on time-to-market, cost, and efficiency of products.

S. Aftabjahani *et al.*, "Special Session: CAD for Hardware Security - Automation is Key to Adoption of Solutions," *2021 IEEE 39th VLSI Test Symposium (VTS)*, 2021, pp. 1-10, doi: 10.1109/VTS50974.2021.9441032.

History of CAD for Hardware Security

- 2015: Few like-minded security experts from industry and academia decided to plan how to close this gap by
  - creating a movement to realize an ecosystem of security-aware CAD tools for Design for Security & Security Validation/Assurance.
  - trying to bring CAD for Security to the prioritized set of national and commercial research investments.
- 2015-2022: Brought Security and CAD for Security to the attention of the HW security community and EDA community from academia, industry, and government by
  - creating panels and tutorial sessions in DAC, IVSW, MTV, HOST, VTS and GLSVLSI.
- 2017: Utilized Trust-Hub, sponsored by NSF, as the venue to bring CAD for Security solutions,
  - First built around Taxonomy of Physical Attacks to create plugins capable of vulnerability analysis for each type of attack.
  - The solutions (from academia and industry) intended to promote collaboration and information sharing among researchers and attract government and industry (especially semiconductor and EDA companies) to invest in them.
  - It had a catalog of more than 100 solutions to various aspects of design for security and security verification from our many partners from academia and industry to realize building blocks of our planned “General Security Design, Analysis, and Validation Framework”.

History of CAD for Hardware Security

- 2019: Noticed wide-spread acceptance of our vision by Semiconductor Industry, EDA Industry, and Accademia
  - Several major and small EDA companies have been getting involved in creating an ecosystem of security-aware tools,
  - Numerous academic security researchers (UoF, UCSD, UT-Austin, UT-Dallas, GaTech, …) have been joining us or have started parallel efforts like CAD for Assurance.
  - Semiconductor industry (Intel, AMD, IBM, TI, NXP, Analog Devices, …), EDA industry (Synopsys, Siemens EDA Business, Cadence, ANSYS, Tortuga Logic, …) and government (DARPA, AFRL, Navy, NSF, …) are willing to support us in this mission by funding research and development projects directly or indirectly (e.g. Semiconductor Research Corporation) to create more specialized security analysis engines and/or to commercialize some of the solutions.
- 2022: Created Security Annotation for Electronic Design Integration Standard (SA-EDI)
  - to improve trustworthiness of IPs and IP providers,
  - to assist IP integrators in understanding and reducing security risk, and
  - to accelerate tool development to enable scalable security assurance.

  Several EDA companies have already supported it in their design security and validation tools
- 2023-2025: Observing maturity and wide-spread availability and usage of CAD Security tools
  - Be eyewitness of maturity of General Security Design, Analysis, and Validation Framework.
  - Mature SA-EDI to become an IEEE standard (PAR P3164).
  - Observe widespread usage of Semiconductor companies and design houses use EDA tools supporting SA-EDI.

SECURITY-AWARE TOOL SETS

- Design for Security (DFS)+Vulnerability Analysis for Integrity and Confidentiality
- Security-Aware Design, Analysis, and Validation Tools for Behavioral, Architectural, Register Transfer, Gate, Transistor Level Modeling; Behavioral and Physical Synthesis; Layout (Placement, Routing, Clock Tree Synthesis, etc.)
- Security-Aware Design for X (DFX); X={Test, Debug, Validation, Manufacturing)
- Formal Security Validation Engines with improved scalability
- Security Validation Plugins/Extensions for Simulation/Emulation Tools
- Security Properties, Tests and Testbench Generation
- Side Channel Observation/Physical Attack Analysis (e.g. Fault Injection Simulation)
- Hardware Trojan Detection and Prevention

Introducing SA-EDI Standard

IEEE format

- IEEE standard is the end goal

Draft complete (45pp)

Accellera Public Release

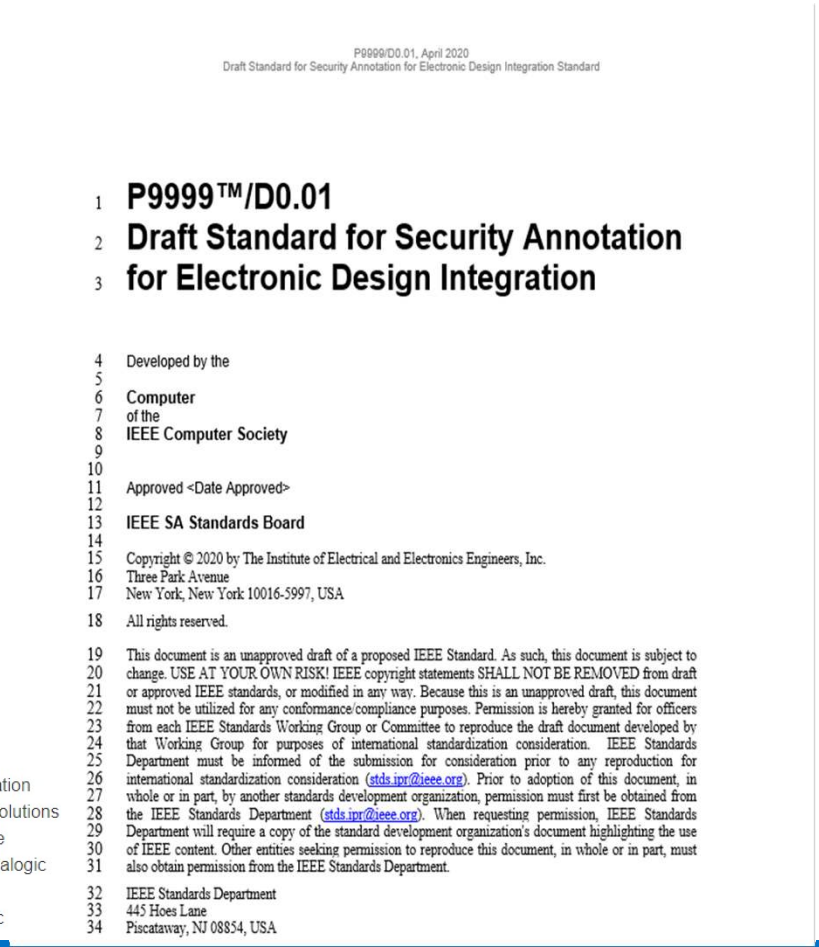
- July 2021, 21 authors, 11 companies
- Available online through Accellera:

  Security Annotation for Electronic Design Integration Standard

EDA's Companies' PoC/Demo @ DAC'21

- Tortuga Logic ™
- Methodics ™

In-Person Presenters:
Mike Borza - Synopsys
Jason Fung - Intel Corporation
John Hallman - Onespin Solutions
Vishal Moondhra - perforce
Anders Nordstrom - Tortugalogic
Jeremy Bellay - Battelle
Jason Oberg - Tortugalogic


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:

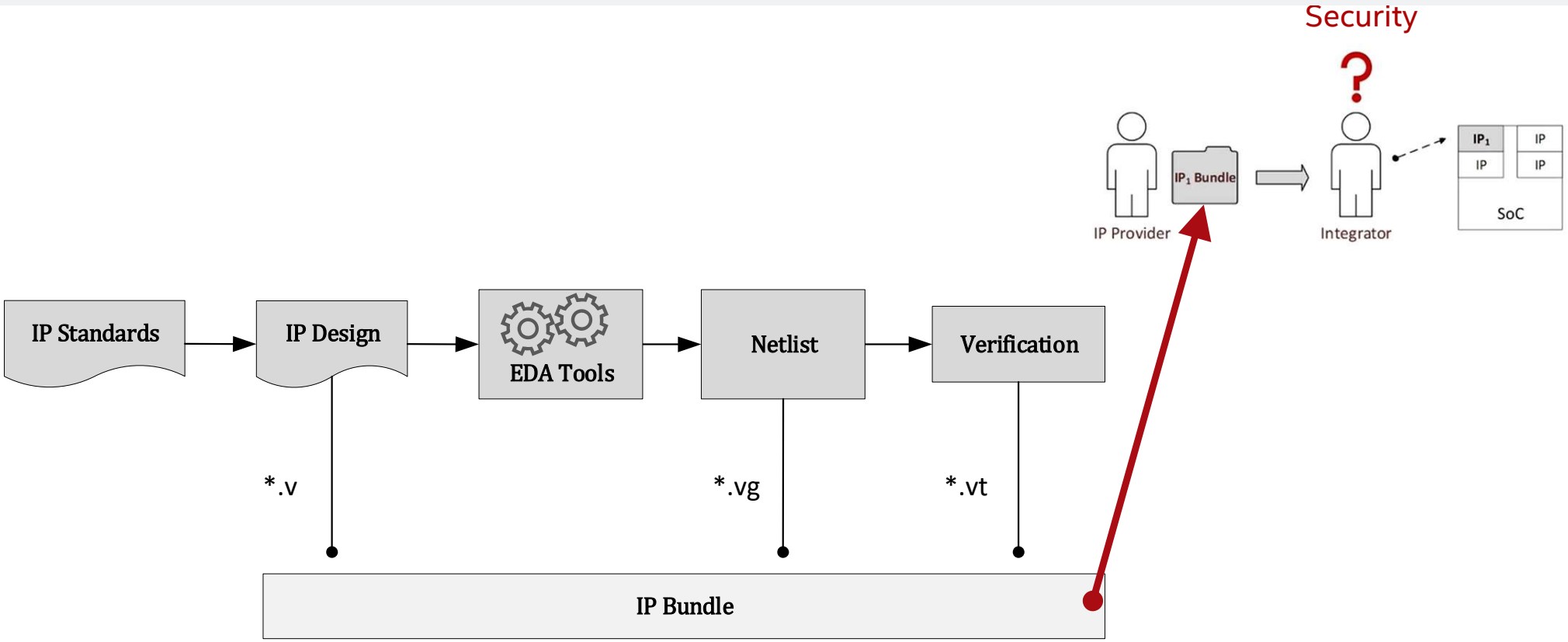
- Improve trustworthiness of IPs and IP providers
- Assist IP integrators in understanding and reducing security risk
- Accelerate tool development to enable scalable security assurance

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

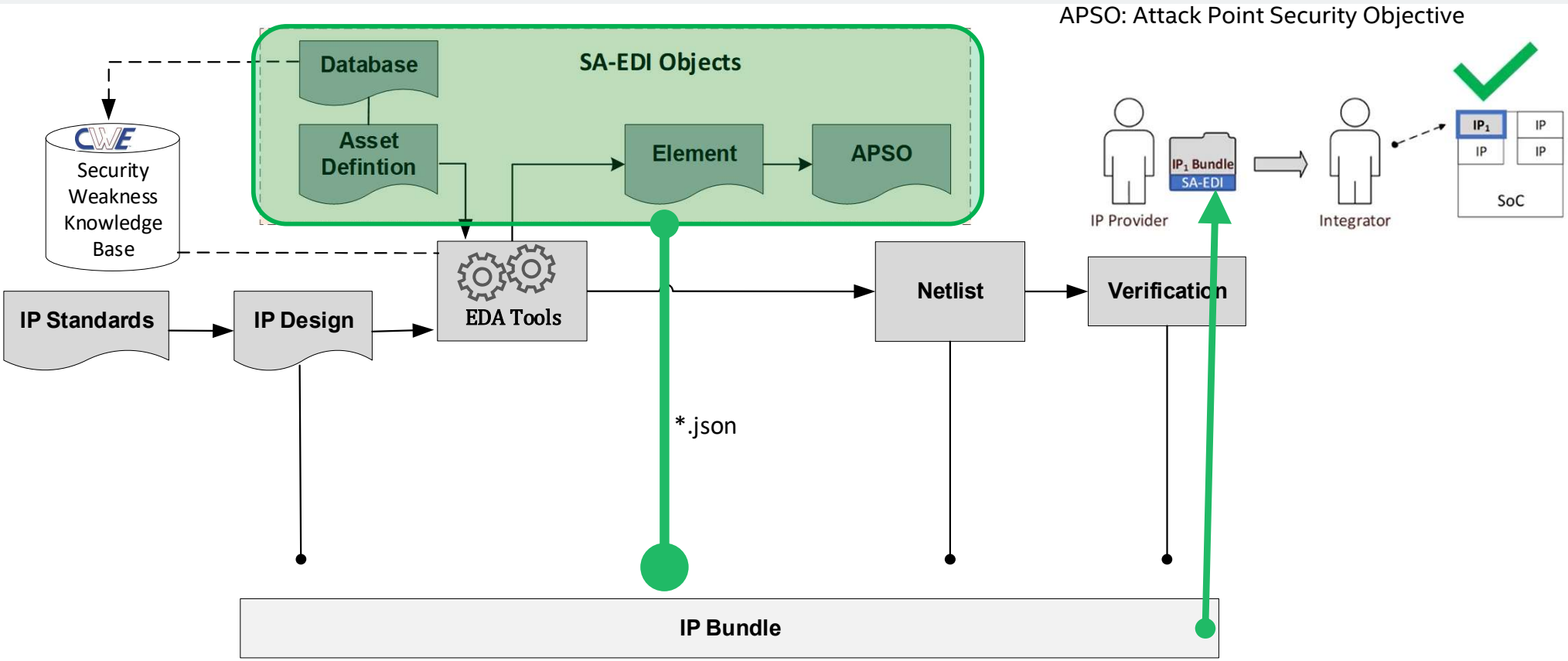
Today's IP Design Flow

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

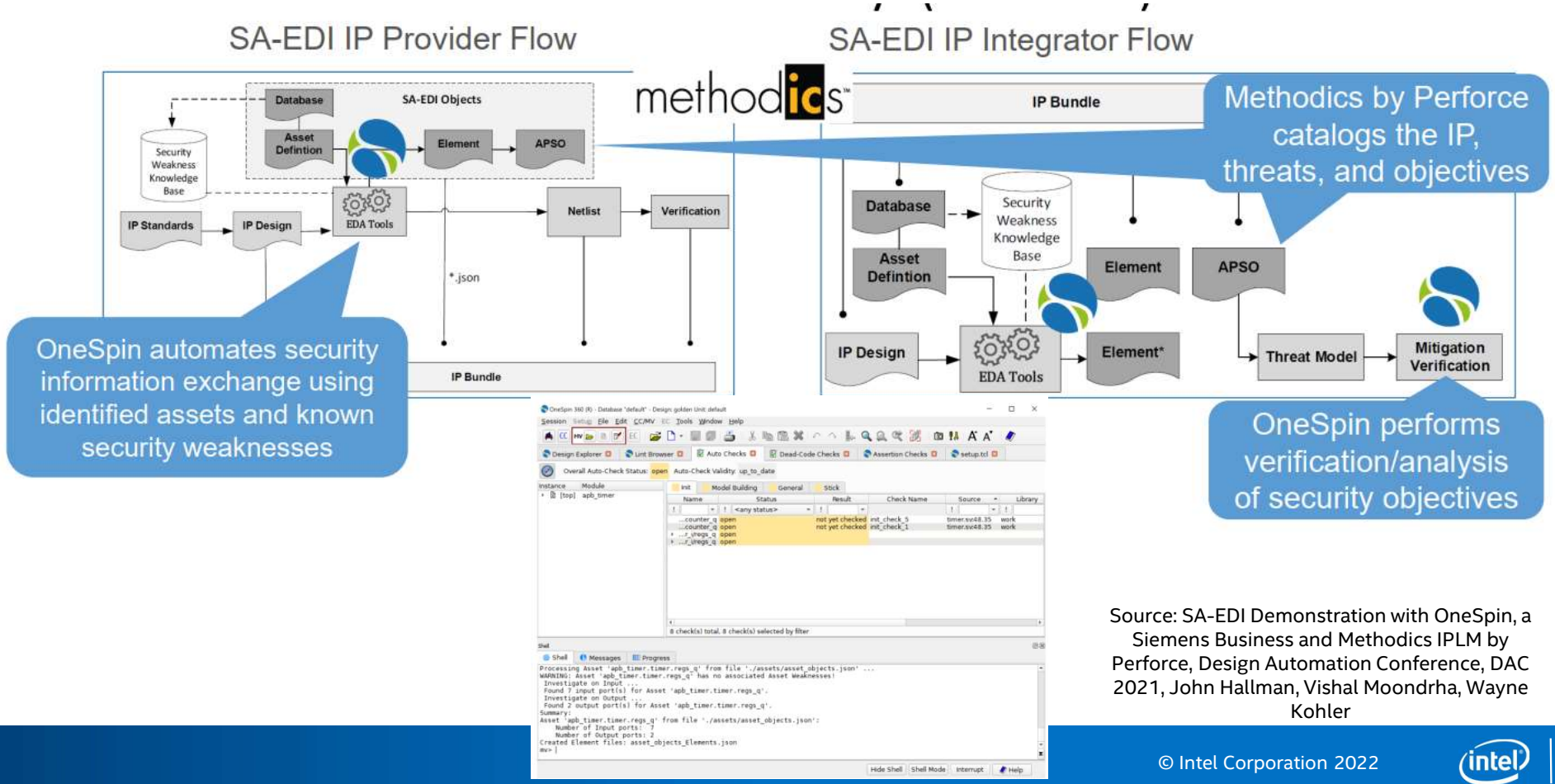


Future's IP Flow w/ SA-EDI Data Objects

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

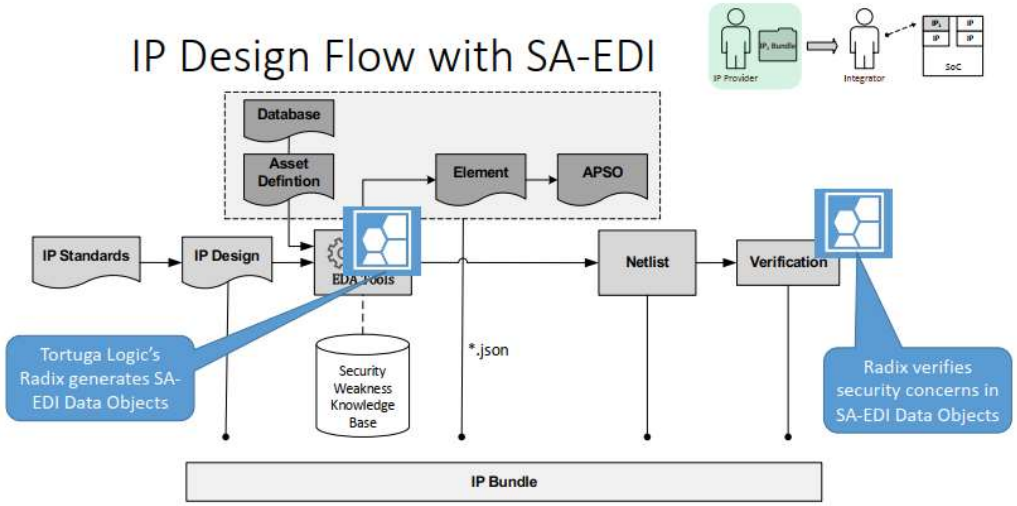


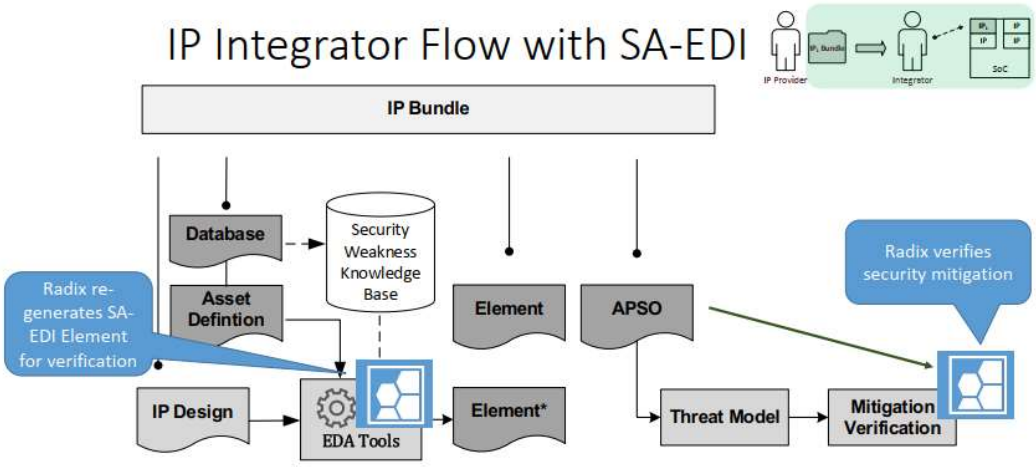
SA-EDI Demo 1 (Methodics™)

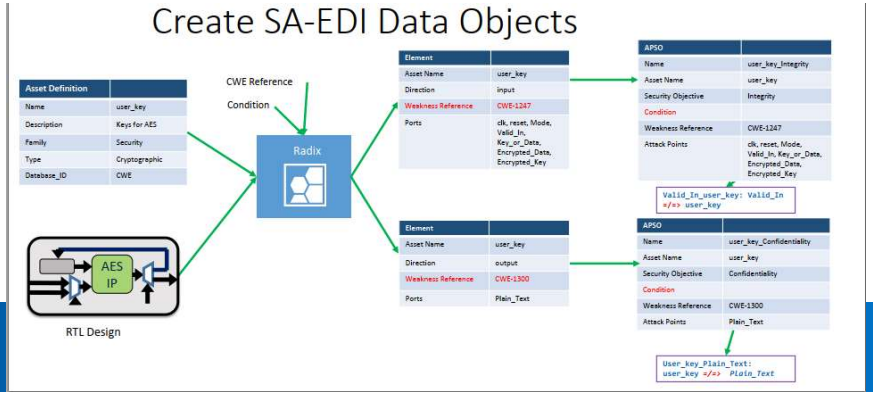


Source: SA-EDI Demonstration with OneSpin, a Siemens Business and Methodics IPLM by Perforce, Design Automation Conference, DAC 2021, John Hallman, Vishal Moondrha, Wayne Kohler

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