Security Annotation for Electronic Design Integration

Info Sheet

SA-EDI Standard 1.0

Developed by the IP Security Assurance (IPSA) Working Group

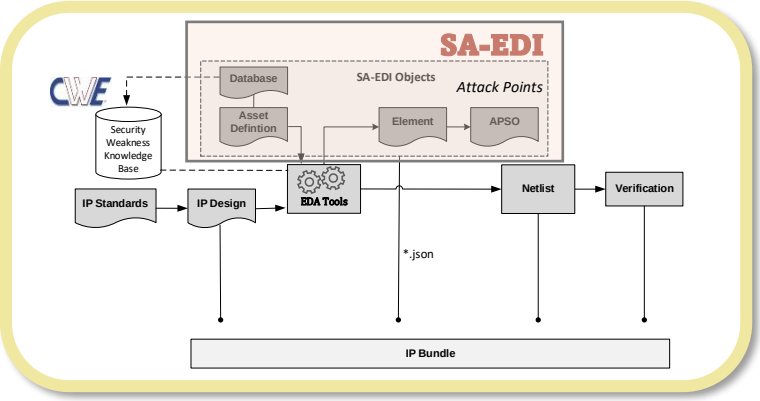
accellera SYSTEMS INITIATIVE™

Identify Security Concerns in IP with SA-EDI

The SA-EDI standard provides a consistent way to manage and verify security assurance for IP integration. This supports a much-awaited security assurance pass into the chip design workflow, helping to identify any potential security concerns or weaknesses associated with hardware IP throughout the whole design.

Security Assurance for Chip Design

SA-EDI is a lightweight standard that is designed to integrate security assurance checks directly into existing workflows for easy and straightforward adoption.



The methodology starts with a database of known security weaknesses, including ***MITRE's Common Weakness Enumeration (CWE)*** for hardware. By interfacing with industry databases, users can utilize a rich repository of known weakness, mitigations and prevention efforts while also having the capability to add their own custom entries.

Security Standard CWE Database IP Security Assurance

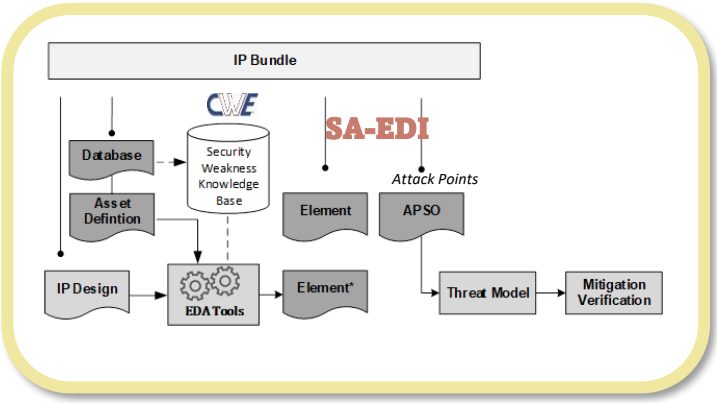
> "There has been tremendous interest from the stakeholders in the development of a standard to address security concerns for hardware IP."
>
> Lu Dai
> Chair of Accellera

- Standard is supported by IP developers, IC integrators and EDA vendors
- Designed to easily insert into current EDA flows and allow for custom extensions, SA-EDI makes adoption easy, straightforward and automated
- SA-EDI's goals are to not only identify security concerns when integrating an IP into an electronic design, but also identify known security weaknesses based on the properties of the IP
- Offers a major advantage by providing the ability to prioritize and/or sort based on security objectives, weaknesses, etc. to meet design goals
- Includes ability to verify matching SA-EDI objects with RTL, providing a level of confidence that the IP supplier delivered an acceptable bundle
- SA-EDI simplifies the scenario by making the security assurance collateral, methods and outcomes standard across the industry and manageable using JSON data modeling

Developing IC Threat Models

The methodology continues as the IP assets and weakness knowledge base are identified and captured in Asset Definition and Database data objects, respectively. These objects will be used by **EDA tools** to create Element objects which identify which ports and security weaknesses are associated with an asset.

The Element objects are then used to create the Attack Points Security Objective (APSO) objects which are inputs for creating the IC threat models. The **Threat Model** contains the security objective, attack points, and a condition which may violate the security objective.



SA-EDI Integrator

See you at DAC 2021!

Watch a demo and learn more about SA-EDI from the IPSA Working Group and EDA vendors

58 DESIGN AUTOMATION CONFERENCE

FROM CHIPS TO SYSTEMS — LEARN TODAY, CREATE TOMORROW

December 5-9 | San Francisco

The SA-EDI Standard

The SA-EDI standard provides a consistent way to manage and verify security assurance for IP integration. By focusing on the ability to automate the data mining, such as sorting on security objectives or common threats, less time will be spent consuming security assurance while maintaining all the advantages of threat modeling.

Please contact the **IPSA Working Group** or your **EDA tool vendors** for the latest information on the SA-EDI standard and associated tools.

Chip Level Security Assurance

Security assurance is required when designing a chip, but this can only be achieved when **ALL** of the components within the design have a similar security assurance.

Designs are complex, some containing 10s or 100s of IPs, many coming from third parties. An automated **industry standard** is required to standardize the methodology and outcomes.

EDA Tools are looking to use SA-EDI to organize the data by assets, security objectives, security weakness references, attack points and/or violating conditions. These outputs can then be documented in the chip's formal requirements, architect specifications, test plans, build assertions and more to create a **full chip solution for security assurance**.

References

1. Security Annotation for Electronic Design Integration (SA-EDI) 1.0, 2021-07-13, *www.accellera.org/downloads/standards/ip-security-assurance*
2. Common Weakness Enumeration, *cwe.mitre.org/*
3. IPSA Working Group www.accellera.org/activities/working-groups/ip-security-assurance