Title: Getting to Know Accellera's Emerging Hardware Security Standard: Security Annotation for Electronic Design Integration (SA-EDI)

Authors:
Jean-Philippe Martin, Intel
Brent Sherman, Intel
John Hallman, OneSpin

Systems on chip may integrate hundreds of components referred to as Intellectual Property (IP) blocks or just IPs. IPs originate from various sources such as internal development teams, off-the-shelf third-party IP suppliers, tool-generated IPs, etc. Typically, the product owner integrates multiple IPs from multiple sources, which raises concerns about security risk. How much risk is the product owner inheriting? What potential security concerns exist that an integrator must address to ensure the security objectives of the product are upheld?

This session will introduce an emerging new standard called Security Annotation for Electronic Design Integration (SA-EDI) to address security concerns in a manner that is low-overhead, non-disruptive, and scalable across IP families. The standard specifies an approach to provide information about the IP security relevant to the integrator and recommended mitigations to implement and risk to address.

Topics covered will be:

- **Methodology –** details the overall concept and workflow, along with the individual components, new security data objects, dependencies, and assumptions that all contribute to reducing security risks in IP
- **Security Weakness Knowledge Base –** lists potential IP security concerns; leverages Common Weakness Enumeration (CWE) and/or other security weakness knowledge bases
- **Example –** demonstrates an example Watchdog IP core through the methodology
- **Future Efforts –** captures the next steps required for public release of the standard

At the conclusion of this session, attendees will better understand risks associated with IP and become familiar with the SA-EDI standard, including how it can be applied and when it will be available for reference.