Global Supply Chain Security for Microelectronics

Secure Design Session Report Out – October 28, 2022

26 – 28 October 2022 workshop

ANSI

Secure Design Session

FACILITATOR

Daniel Radack
Institute for Defense Analyses (IDA)

Supported by the following organizations:

Aerospace Engineering Solutions International	Northrop Grumman
Air Force Research Lab	NSWC Crane
Amazon	OSD(R&E), Critical Technologies, Microelectronics
Boeing	Pathfinder
DMEA	Rockwell Automation
Eaton Corp	SAE International
Georgia Tech Research Institute	Sandia National Laboratories
IDA	Synopsys
Intel Corporation	The MITRE Corp.
MITRE	The Open Group
NASA Electronics Parts & Packaging (NEPP) Program	UL Solutions
National Institute of Standards and Technology (NIST)	University of Connecticut

Q4a Key Takeaways:

What candidate considerations were discussed?

Proposed Candidate Considerations

- Bill of Materials
- Known Vulnerabilities
- Verification & Validation
- On-Die Security Features
- Data Requirements

Secure Design Definition Modification

- Managing risk “from integrated circuit design through final device functional test.”
- Architecture design, manufacturing and development until handing off device for the system

Revised Candidate Considerations

- Bill of Materials
- ~~Known Vulnerabilities~~ -> Continuous Threat Modeling
- Design Best Practices
  - Product development plan
  - Security development plan
  - Verification & Validation
  - On-Die Security Features
  - Data Requirements
- Traceability & Chain of Custody (Provenance)
  - Change Management
- Incident Response

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Bill of Materials

Criteria:

LoA: A	- Level of fidelity of ME BOM informs confidence and assurance level. - Transparency provided to Acquirer.
LoA: B	- Level of fidelity of ME BOM informs confidence and assurance level. - Developer maintains ME BOM that includes all elements integrated into design of integrated circuit and package.
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- Bill of Materials may not be the correct term, need to discuss further.

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Continuous Threat Monitoring

Criteria:

LoA: A	TBD
LoA: B	- Developer documents and utilizes a continuous risk modeling and management program for ME security risks.
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- Variability in the assessments exist, lack of standardization and may be company specific
- Continuously, continuously, continuously: Continuous threat modeling is critical.

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Design Best Practices (Overall)

Criteria:

LoA: A	- Vendors must adhere to documented corporate design and security best practices with a 3rd party certification
LoA: B	- Vendors must adhere to documented corporate design and security best practices.
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

§ N/A- assigned by the sub-topics

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Design Best Practices (Verification & Validation)

Criteria:

LoA: A	- Proof of verification, transparency of evidence of verification
LoA: B	- Security requirements are documented as part of product development plan and are verified and validated. - Requirements for security verification and validation should include negative testing (e.g., fuzzing, penetration) - Depending on the criticality of the LoA-B COTS part – self attestation / internal or 3rd party certification.
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- Functional verification by itself is not enough

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Design Best Practices (On-die Security Features)

Criteria:

LoA: A	- There is no overarching standard, more discussion is needed before making recommendations. - Depending on the ME, debug and reboot capability
LoA: B	- There is no overarching standard, more discussion is needed before making recommendations. - Depending on the ME, proof of authenticity, untampered
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- On-die security is an important tool for securing COTS parts and has implication in multiple supply chain practice areas

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Design Best Practices (Data Availability)

Criteria:

LoA: A	
LoA: B	- No specific requirements beyond VnV outputs, BOM, incident response. Build and comply with standards for the other areas and nothing else is needed here. Self attestation to the standards would be sufficient. - We are unable to identify any standalone data for the acquirer, and if/when standards developed in the other areas include performance measures such that other data is not required.
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- Cost implications are a key consideration and may not support business models especially considering the need.

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Design Best Practices (Product Development Plan & Security Development Plan)

Criteria:

LoA: A	- Must have a Product Development Plans and a Security Development Plan, and have a 3rd party assessment
LoA: B	- Must have a Product Development Plans and a Security Development Plan, and conduct a self-assessment
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- There are standards but they tend to be at the system level. We need to determine how ME require any tailoring or if they can be used as is as well as what other standards exist.

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Incident Response

Criteria:

LoA: A	- Must use an active standard or standardized incident response approach and acquirer must receive reporting of incidents. Continuous threat modeling by acquirers, including incident response, is required. - Timeliness of how to carry out the plan should be set, but it no time specified at this time.
LoA: B	- Must use an active standard or standardized incident response approach and acquirer must receive reporting of incidents. Continuous threat modeling by acquirers, including incident response, is required.
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- There are several standards. DoD will need to review these to ensure they can be tailored to DoD for ME COTS products.

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

Candidate Consideration: Traceability & Chain of Custody (Provenance)

Criteria:

LoA: A	- Chain of Custody provisions shall be made for secure design considerations and incidents are reportable. (Distinctions between LoA-A and B still need to be discussed. Reportability is one factor to be considered).
LoA: B	- Chain of Custody provisions shall be made for secure design considerations and incidents are reportable. (Distinctions between LoA-A and B still need to be discussed. Reportability is one factor to be considered).
LoA: C	TBD
LoA: D	TBD

Key Takeaway(s):

- Procurement Management should include sunset provisions in contracts.

Q4c Key Takeaways:

What areas demonstrated the greatest need in terms of relevant regulations, policy, standards, best practices?

Existing Resources

- Accellera IPSA Whitepaper
- CISSP
- IEEE 15288.1-2014
- IEEE 15288.2
- ISO 20243 / O-TTPS
- ISO 27035
- MITRE Common Weakness Enumeration (CWE)
- RTCA DO-254
- SAE ARP4754
- SAE JA7496
- SAE AS7120

Gaps / Needs

- Bill of Materials
  - Near-term -> Regulation
  - Long-term -> Standard
- Standard on quantitative risk modeling
- Design / security standards which support certification programs *(e.g., DALs component & systems)*
- IC Design Best Practices

Q4d Key Takeaways:

What recommendations does the group have for DoD on next steps?

- Industry and government need to continue discussions to accelerate solutions and recommendations.
- Need to secure broader engagement of various sectors and stakeholder types (industry sectors/government).
  - Consider different mechanisms for obtaining broader ME COTS industry feedback.
  - Need more insight about what industry is currently doing – what standards they are using, what terminology they are using – so we do not reinvent the wheel.
  - Mapping of relevant standards and gaps would be beneficial
- Discuss topics with cross-pollination of experts across the supply chain practice areas – the overlap in the venn-diagrams
  - Identify the common threads and set those topics needing discussions across the supply chain areas

Questions / Discussion?