SECURE DESIGN

MODERATOR: DAN RADACK

SECURE DESIGN

- Design practices to improve assurance (e.g., verification and validation), manage risk when the part is outside vendor or user control, and address supply chain volatility (e.g., open architecture or modularity). May overlap with other supply chain practice areas.

Breakout Staff

- Facilitator: Daniel Radack, PhD, Assistant Director, Information Technology and Systems Division, Institute for Defense Analyses (IDA)
- Scribe: Christine Bernat, Associate Director, Standards Facilitation, ANSI
- Remote Participant Interface: Rachel Hawthorne, Sr. Manager, ISO Outreach and Enhanced Services

OVERVIEW

Overview

- FY20 NDAA Section 224 requires that “other matters germane to supply chain and operational security” be considered in the evaluation of suppliers for DoD microelectronics.
- DoD Microelectronics Assurance Framework identifies four categories of microelectronics:
  - Custom Integrated Circuits (CICs)
  - Field Programmable Gate Arrays (FPGAs)
  - Commercial (includes COTS) <- **subject of this workshop**
  - PCB (handled by the PCB Executive Agent)

Candidate Risks

- If procured devices include vulnerabilities (intentional or unintentional), then system performance or integrity may be adversely impacted .
  - See: Hardware Assurance Definition (from workshop objectives)

CANDIDATE CONSIDERATIONS

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

BILL OF MATERIALS
CANDIDATE CONSIDERATION

Consideration

- Device security risk cannot be evaluated without understanding what is in the design, device
- What should be included in a device/IP BOM? 3PIP? Legacy design? Verification elements? What about custom designed – blocks, glue logic, etc.? Manufacturing information? Materials selection?
- What information can be shared with acquirers to inform their assessment of risk?
- Is there a way to standardize this information? (requirements language, standard, etc.)

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

KNOWN VULNERABILITIES
CANDIDATE CONSIDERATION

Consideration

- ***DoD:*** assessment of vulnerabilities must be conducted on an ongoing basis.
  - What information is required to support this by the acquirer?
- What baseline requirement helps provide confidence?
- What is the expectation for 3PIP?
- What considerations are needed for tools (e.g., EDA tools)?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

VERIFICATION & VALIDATION
CANDIDATE CONSIDERATION

Consideration

- How can an acquirer gain confidence that a device does what it is supposed to – and nothing else?
  - Security, functional requirements
  - Quantity, quality of verification
  - Assumptions made by developer (e.g., quality of 3PIP, legacy, etc.)
- What type of safety standards could be leveraged to improve confidence? (e.g., automotive, medical, aviation)

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

ON-DIE SECURITY FEATURES
CANDIDATE CONSIDERATION

Consideration

- Recommendations for minimal requirements?
- Overlap to Supply Chain Traceability – physical / digital thread?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

DATA REQUIREMENTS IN SUPPORT OF SECURE DESIGN
CANDIDATE CONSIDERATION

Consideration

- What data is required?
- Is the data available?
  - Data exists and can be delivered
  - Data does not exist but can be generated
  - Data cannot be made available
- When is the data available?
- Can the data delivery be standardized?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

SECURE DESIGN
CANDIDATE CRITERIA

Leverage existing value judgements when practicable (don't reinvent the wheel)

LoA: A	
LoA: B	• BOM: • Known Vulnerabilities: • Verification & Validation: • On-die Security Features: • Data Availability:
LoA: C	
LoA: D	

REGULATION, POLICY, OTHER
REFERENCES

Regulation

- DFARS 52.246-11

Policy

-

Other

-

STANDARDS & BEST PRACTICES
REFERENCES

- ISO 9001:2015: Quality management systems — Requirements (not microelectronics specific)