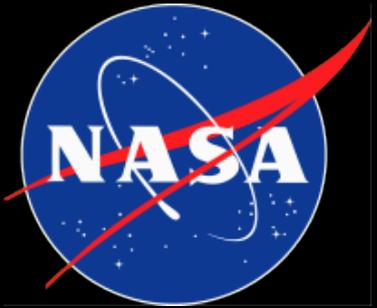


ASIC/FPGA Trust Assessment Framework



Melanie Berg

AS&D in support of NASA/GSFC Melanie.D.Berg@NASA.gov



Acronyms

- Application specific integrated circuit (ASIC)
- Defense Microelectronics Activity (DMEA)
- Electronic Design Automation (EDA)
- Framework for Assessing Security and Trust in MicroElectronics (FASTIME)
- Field programmable gate array (FPGA)
- Information Technology (IT)
- NASA Electronic Parts and Packaging (NEPP)
- Physical unclonable function (PUF)
- Verification and Validation (V&V)



Synopsis of Framework

ASIC: Application specific integrated circuit

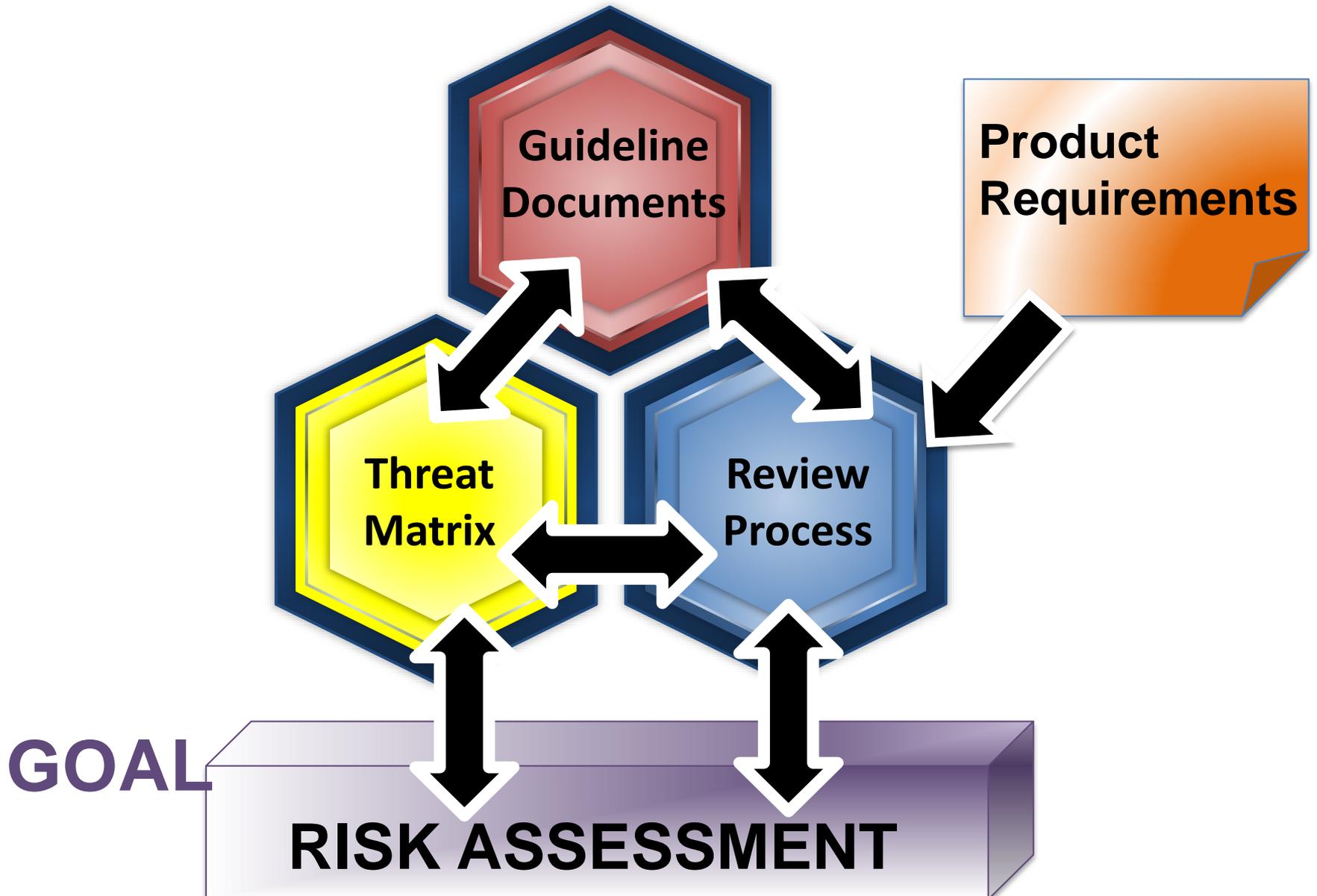
FPGA: Field programmable gate array

- **NASA Electronic Parts and Packaging (NEPP) is developing a systematic framework for practicing security and trust in ASIC and FPGA applications.**
- **Goal: User is provided guidance in mitigation best practices; correspondingly, missions are expected to follow guidelines to the best of their abilities; and a risk assessment is performed on the implementation.**

Framework for Assessing Security and Trust In MicroElectronics (FASTIME)

The methodology incorporates work/research performed by a variety of groups: NASA, The Aerospace Corporation, RAMBUS, Global Foundries, Mentor Graphics, Synopsys, Xilinx, Graf Research, Sandia National Laboratories, and Microsemi.

FASTIME





FASTIME Strengths

- Two perspectives are used: **V&V: Verification and Validation**
 - Guidelines and requirements are provided to the target team and are used as references for the review process (what should be done).
 - Actual implementation is reviewed.
- Framework takes into account:
 - Observed gaps.
 - Potential gaps (unobtainable information, lack in V&V coverage, not vetted personnel).
 - Multiple layers of mitigation (co-dependencies).
 - Potential for adversary's learning process as it pertains to the actual implementation of mitigation.
 - Full ecosystem (personnel, IT, tools, design process, data handling, etc,...)
- Risk analysis is robust:
 - Includes V&V coverage but does not end there... coverage is not the only element that defines risk.
 - Risk metrics are more than colors or simple strength descriptions.
 - Risk metrics are based on time-to-infiltration and weighted outcome.
 - Risk items can be red-lined for immediate attention.
- Eventual integration with model based system engineering tools.

Vulnerabilities are determined by coverage of guidance, requirements, and implementation discrepancies.

FASTIME: Review Process

V&V: Verification and Validation
EDA: Electronic design automation



Does not restrict EDA tools.
However assesses coverage.

- **Creates visibility and traceability for each step of the design process and potential contribution to threat.**
- **Requires an external assessment team.**
- **For the manufacturer's design process evaluation, it is unlikely that the trust and security assessment team will have access to all files to perform V&V.**
- **Hence, detailed checks of the manufacturer's V&V coverage and mitigation processes are expected to be performed by the assessment team.**
- **Employs established "checklist" approach.**
- **Enables risk analysis because of detailed information gathering.**

FASTIME Review Process: Use of An Assurance Checklist



- Derived from NASA design review checklist and information gathered from partnering organizations.
- Assessments are divided into subcategories with associated risks.
- Links to previously assessed items are included (do not want to spend time on vetted items if its listed risk-level is acceptable).
- New column is added to **link to Guidelines and Requirements**.

Traceability!!!!



1	Information Security(example section)	Comments	Guidelines/Requirements Link	Risk Metric
1.1	Is the design house DMEA Trust certified?	links to DMEA accreditation	TAGn0	
1.2	If the design house is not under DMEA trust, explain IT security	links to IT security documents	TAGn1	
1.3	List personnel that have access to the design database; and extent of their accessibility/visibility (restrictions)	Links to personnel documentation plus highlighted comments	TAGn2	

Example: FPGA Security Features Subsection



PUF: Physical unclonable function

3	FPGA Security Features	Comments	Guidelines/Requirements Link	Risk Metric
3.1	Does FPGA require a Key?	A key is required. Requirement ##.##	Link to Requirements Matrix	
3.2	If a Key is required, what type of Key is being implemented (e.g.: embedded PUF, soft PUF , stored Key, components (memory versus ring oscillator);	links to datasheet: Embedded PUF – ring oscillator.		
3.3	Provide link to Key implementation radiation results (Single event effects, total dose, and prompt dose);	No radiation data is available	RISK! Depending on target environment	
3.4	Assess functional coverage of implementation. Is there potential for lockout due to Key access failure ? Example of failure can be due to radiation effects, adversary learning, or gaps in mitigation.	No tests have been performed to determine lockout threat		
3.5	If no lockout, show proof.			

Road Ahead

EDA: Electronic design automation

- A great deal of work has been completed. However, there is still more to be done.
- Further development is required of guidelines, review checklist, and threat matrix.
 - Will require research into manufacturer design flow.
 - Will require research into fabrication house flows.
- EDA tool evaluation.
- Links into model based system engineering tools.
- Risk metrics.

