DO-254 Compliance
Pitfalls, Challenges, and Solutions

For MAPLD 2008

Michelle Lange
DO-254 Program Mgr

Sept 18, 2008
DO-254 Background

In 2005, the FAA* began enforcing a new standard for HW (PLD/FPGA/ASIC) design.

This standard is known as DO-254, “Design Assurance of Airborne Electronic Hardware.”

DO-254 is based on a similar SW standard (DO-178B).

DO-254 today applies to civil aviation but is spreading to some military projects.

DO-254 is a concern because it adds significant time, risk and cost** to design projects.

* And other worldwide aviation safety agencies

** Compliance can increase project cost by up to 400%! 
What DO-254 Is…and Isn’t

- It’s like a guide that shows you where you need to be
- It **does not** tell you how to get there
  - That is up to you to determine
- It **does not** tell you what you need to watch out for
  - That’s for you to learn
DO-254 in the Aircraft Certification Process

**System Safety Assessment**
- Criticality of systems determined
- Design assurance level (DAL) A-E assigned

**DAL of Component**
- DAL handed down to component
- Determines DO-254 requirements

**FPGA/ASIC**
- Built to DO-254 standards as reviewed by DER

**DO-254 Compliance**
- DER form 8110-3 submitted to FAA recommending approval of the ASIC/FPGA

**Type Certificate (ATC/TC/STC)**
- The FPGA/ASIC is approved only as part of an FAA approved equipment installation
- TC form describes every item on aircraft
- Components now “DO-254 certified”

**Timeline**
~2 years
What is DO-254?
A Requirements-Based Design Flow with Strict Process Assurance

Supporting Processes

Design Flow

DO-254 Process as you’d see it shown in the DO-254 Spec
A Look Inside DO-254

Supporting & Key Processes

Process Assurance
- PHAC
- V&V
- Planning
- TLD
- HAS

DO-254 Lifecycle
- Requirements Capture
- Conceptual Design
- Detailed Design
- Implementation
- Production Transition

Requirements-Based Flow
- Planning
- Conceptual Design
- Detailed Design
- Implementation
- Production Transition
A DO-254 Compliant FPGA Flow

1. Establish Project Plans (PHAC and others)
2. Capture/Validate Requirements
3. Generate architectural artifacts
4. Effectively verify RTL and gate-level design
5. Safely synthesize design, and prepare for P&R
6. Generate review and audit sites
7. Write, generate, reuse, and check RTL code
8. Assess all Tools

- Trace requirements
- Version manage all artifacts and docs
- Verify RTL Design
- Verify Gate-Level Design
- Synthesis
- Place & Route
- Program Device
- Debug Hardware Item
- Debug Hardware
## Common* Issues We are Seeing

<table>
<thead>
<tr>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies are engaging in DO-254 programs without proper preparation</td>
<td>Lots of mis-steps and rework, failed audits, costs increasing 400%</td>
</tr>
<tr>
<td>Companies think they can “get around” DO-254</td>
<td>Parts cannot be used (or reused) for in-flight systems</td>
</tr>
<tr>
<td>Requirements traceability is a reactive process</td>
<td>Failed audits, much rework and increased expense</td>
</tr>
<tr>
<td>Groups within a company don’t talk and share information</td>
<td>Each group re-invents the wheel, wasted resource</td>
</tr>
<tr>
<td>Companies don’t consider reuse or future uses of current design</td>
<td>Comply to lowest level, and then have to re-certify</td>
</tr>
<tr>
<td>Companies are struggling with verification</td>
<td>Losing bids, avoiding projects, producing poor quality products</td>
</tr>
<tr>
<td>Tool qualification is difficult</td>
<td>Much time spent on this task</td>
</tr>
</tbody>
</table>

* This is not an all inclusive list!
<table>
<thead>
<tr>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies are engaging in DO-254 programs without proper preparation</td>
<td>Lots of mis-steps and rework, failed audits, costs increasing 400%</td>
</tr>
<tr>
<td>Companies think they can “get around” DO-254</td>
<td>Parts cannot be used (or reused) for in-flight systems</td>
</tr>
<tr>
<td>Requirements traceability is a reactive process</td>
<td>Failed audits, much rework and increased expense</td>
</tr>
<tr>
<td>Groups within a company don’t talk and share information</td>
<td>Each group re-invents the wheel, wasted resource</td>
</tr>
<tr>
<td>Companies are struggling with verification</td>
<td>Losing bids, avoiding projects, producing poor quality products</td>
</tr>
<tr>
<td>Companies don’t consider reuse or future uses of current design</td>
<td>Comply to lowest level, and then have to re-certify</td>
</tr>
<tr>
<td>Tool qualification is difficult</td>
<td>Much time spent on this task</td>
</tr>
</tbody>
</table>
Before Your First Project…

<table>
<thead>
<tr>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies are engaging in DO-254 programs without proper preparation</td>
<td>Lots of mis-steps and rework, failed audits, costs increasing 400%</td>
</tr>
</tbody>
</table>

Instead

Hot Tip #1
Invest in training (it's worth it!)

Hot Tip #2
Work with your DER *early* in your project

Hot Tip #3
Consider having methodology assessments
  — Both for compliance and for methodology efficiency
### Requirements Tracing...

<table>
<thead>
<tr>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements traceability is a reactive process</td>
<td>Failed audits, much rework and increased expense</td>
</tr>
</tbody>
</table>

**Instead**

- **Hot Tip #1**
  - Take a proactive approach
  - Plan for requirements management and traceability as part of the process

- **Hot Tip #2**
  - Don’t assign this job to the intern
  - Value this effort as a key part of the flow

- **Hot Tip #3**
  - Consider automation
Verification...

**Issue**
- Companies are struggling with verification

**Result**
- Losing bids, avoiding projects, producing poor quality products

**Instead**

**Hot Tip #1**
Get a verification methodology assessment

**Hot Tip #2**
Educate yourself on new methodologies
  - Understand the benefits and skill sets required

**Hot Tip #3**
Consider consulting experts to reduce risk
  - Get your team trained and project underway quickly
### Tool Assessment and Qualification…

<table>
<thead>
<tr>
<th><strong>Issue</strong></th>
<th><strong>Result</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool qualification is difficult</td>
<td>Much time spent on this task</td>
</tr>
</tbody>
</table>

### Instead

- **Hot Tip #1** Understand the meaning and purpose
- **Hot Tip #2** Work with tool vendors who will support you
- **Hot Tip #3** Whenever possible, take the “Independent Output Assessment” approach
For More Information

  - Download publications and information
  - Register for DO-254 training
    - Next training: Seattle, Sept 23-24
- Email [michelle_lange@mentor.com](mailto:michelle_lange@mentor.com)
  - Questions
  - Request product information
  - Arrange a visit or demo
- Any Questions?