DO-254 Overview, Pros, Cons, and Discussion

(aka, The Joys and Sorrows of DO-254 Compliance)

Michelle Lange
DO-254 Program Mgr

August 09

Mentor Graphics®

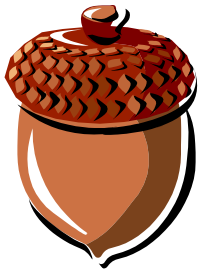
*** Note all references to and quotes from RTCA/DO-254 are used with express permission from the RTCA. Order the complete DO-254 document at www.rtca.org**

Agenda

- History and Current State of DO-254
- DO-254 Compliance Overview
- The Joys and Sorrows of DO-254 Compliance
- Preparing for a Successful DO-254 Program
- Conclusion

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

DO-254 in a Nutshell



- "Design Assurance for Airborne Electronic HW"
- Written to apply to all levels of hardware design
- Invoked as law by the FAA* in 2005
  - Scoped to apply to PLD/FPGA/ASIC design
- Now a worldwide standard
- Spreading into/influencing other adjacent fields
  - Military, medical, transportation, etc around the world
- Causing companies to re-evaluate their design flows
- Can be very costly
  - 400% cost increase is not an uncommon complaint

* Federal Aviation Administration, a US government agency that oversees civilian aviation

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Policy, Documents and Certification

- **Industry organization (90's)**

RTCA / DO-254

- **Product (a standard) developed by the RTCA committee, available via www.rtca.org (2000)**

AC20-152

- **FAA advisory that scopes and puts DO-254 into effect (2005)**

Order 8110.105

- **FAA order that clarifies some DO-254 ambiguities from CAST papers 27-30 (2008)**

AEH Job Aid

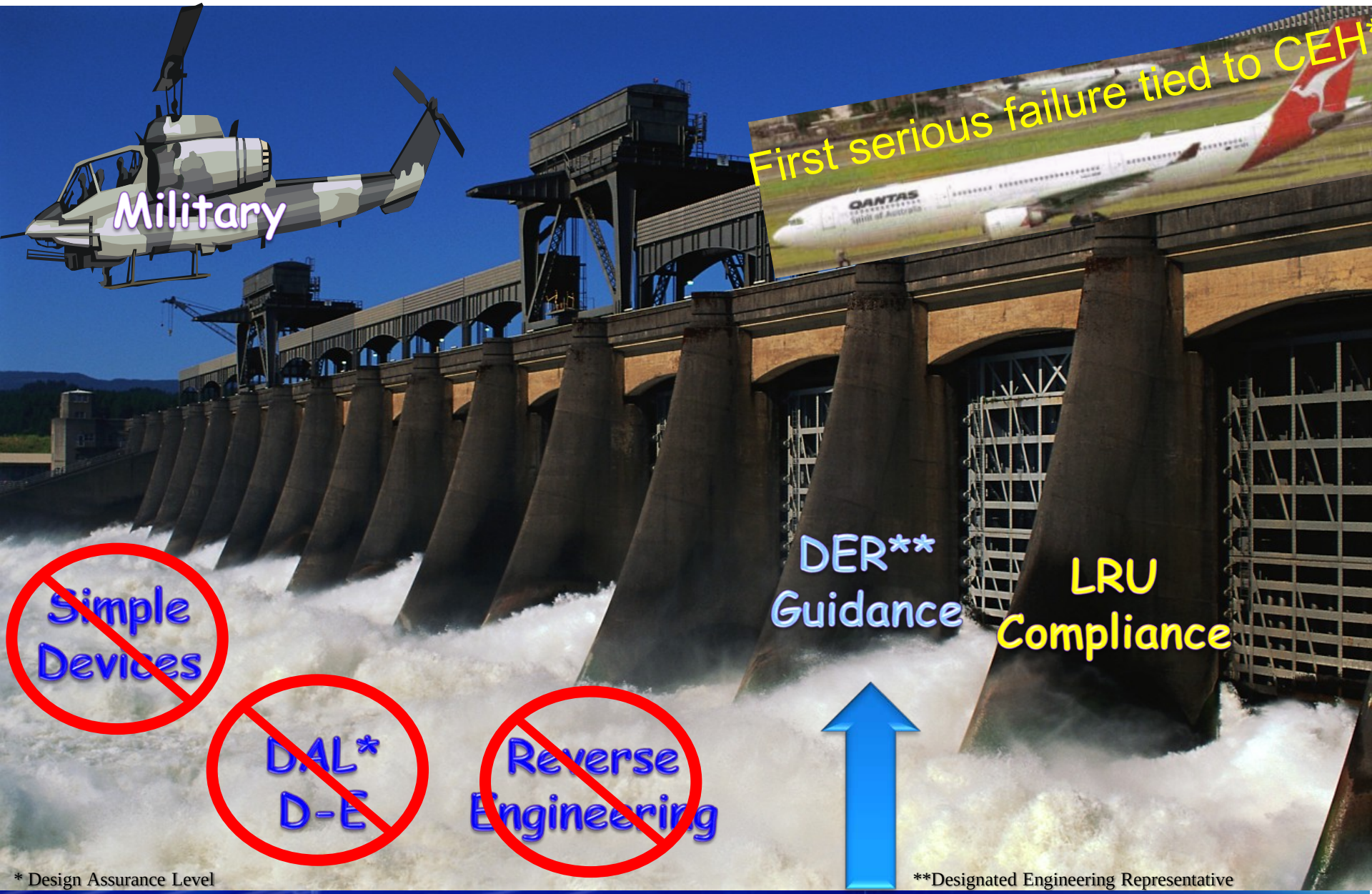
- **FAA guide for cert authorities "Conducting Airborne Electronic Hardware Reviews" (2008)**

CFR Title 14 23, 25, 27, 29

- **Federal rules guiding aviation and space programs that require a device to "perform its intended function"**

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

So What's Changed in the Last Year?



* Design Assurance Level

**Designated Engineering Representative

Agenda

- History and Current State of DO-254
- DO-254 Compliance Overview
- The Joys and Sorrows of DO-254 Compliance
- Preparing for a Successful DO-254 Program
- Conclusion

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

DO-254 and Design Assurance

- ***Assurance* means *certainty***
- **Design assurance means certainty that a design operates as it should**
- **DO-254 forces you to design quality in (proactive) rather just testing errors out (reactive)**
- **DO-254 requires a two-fold approach to achieve design assurance**
  - **A structured and audited design process with thorough planning, reviews, and double-checking of each step within the flow**
  - **Thorough verification at all junctures of the process to catch errors in the design**

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

DO-254 & Design Assurance Levels (DALs)

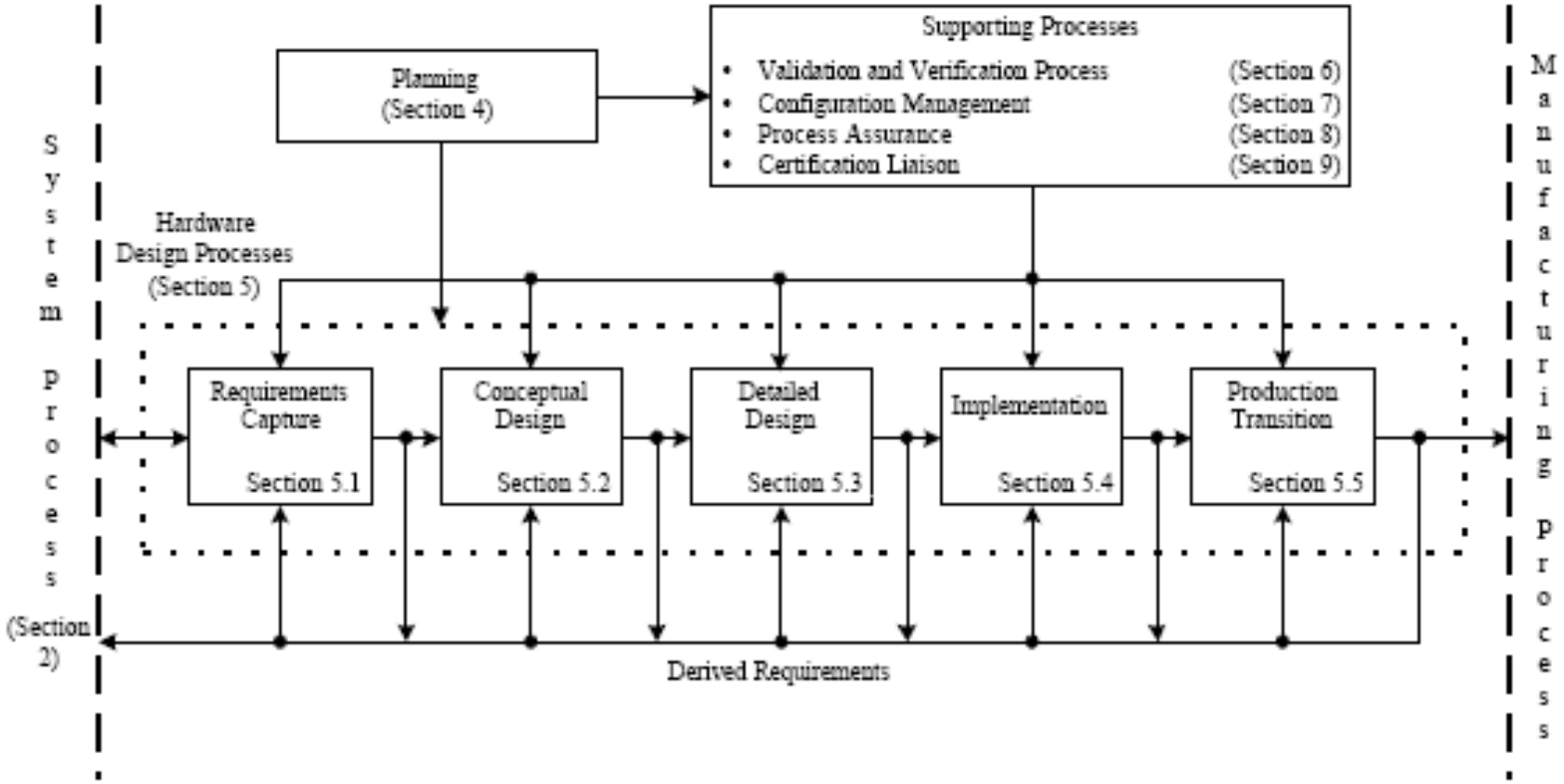
Design Assurance Level (DAL)	Description	Target System Failure Rate	Example System
Level A (Catastrophic)	Failure causes crash, deaths	<1 x 10-9 chance of failure/flight-hr	Flight controls
Level B (Hazardous)	Failure may cause crash, deaths	<1 x 10-7 chance of failure/flight-hr	Braking systems
Level C (Major)	Failure may cause stress, injuries	<1 x 10-5 chance of failure/flight-hr	Backup systems
Level D (Minor)	Failure may cause inconvenience	No safety metric	Ground navigation systems
Level E (No effect)	No safety effect on passengers/crew	No safety metric	Passenger entertainment

- **Higher DALs require more stringent DO-254 process**

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

The Essence of DO-254

A Requirements-Based Design Flow with Strict Process Assurance

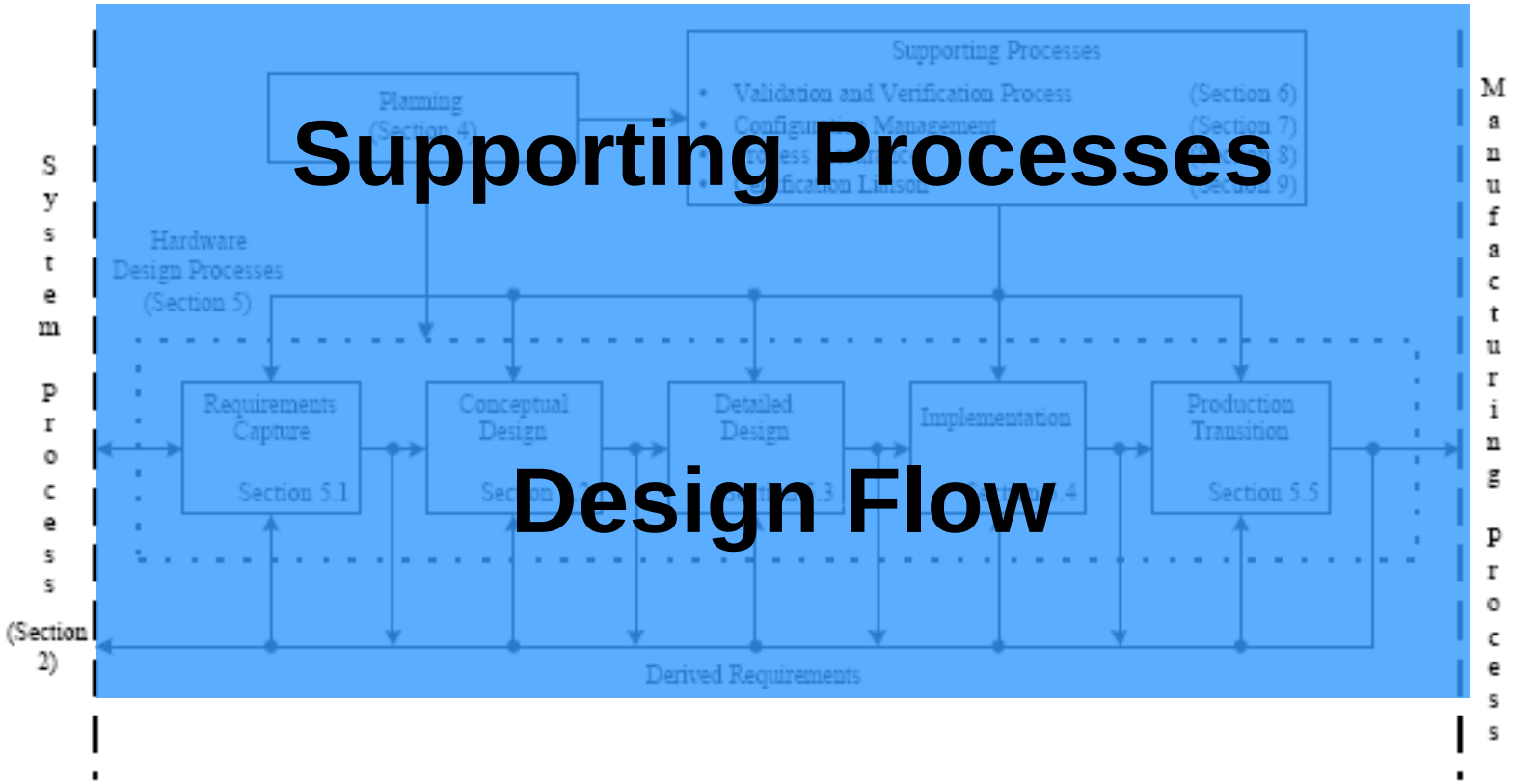


DO-254 Process as you'd see it shown in the DO-254 Document

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

The Essence of DO-254

A Requirements-Based Design Flow with Strict Process Assurance



Supporting Processes

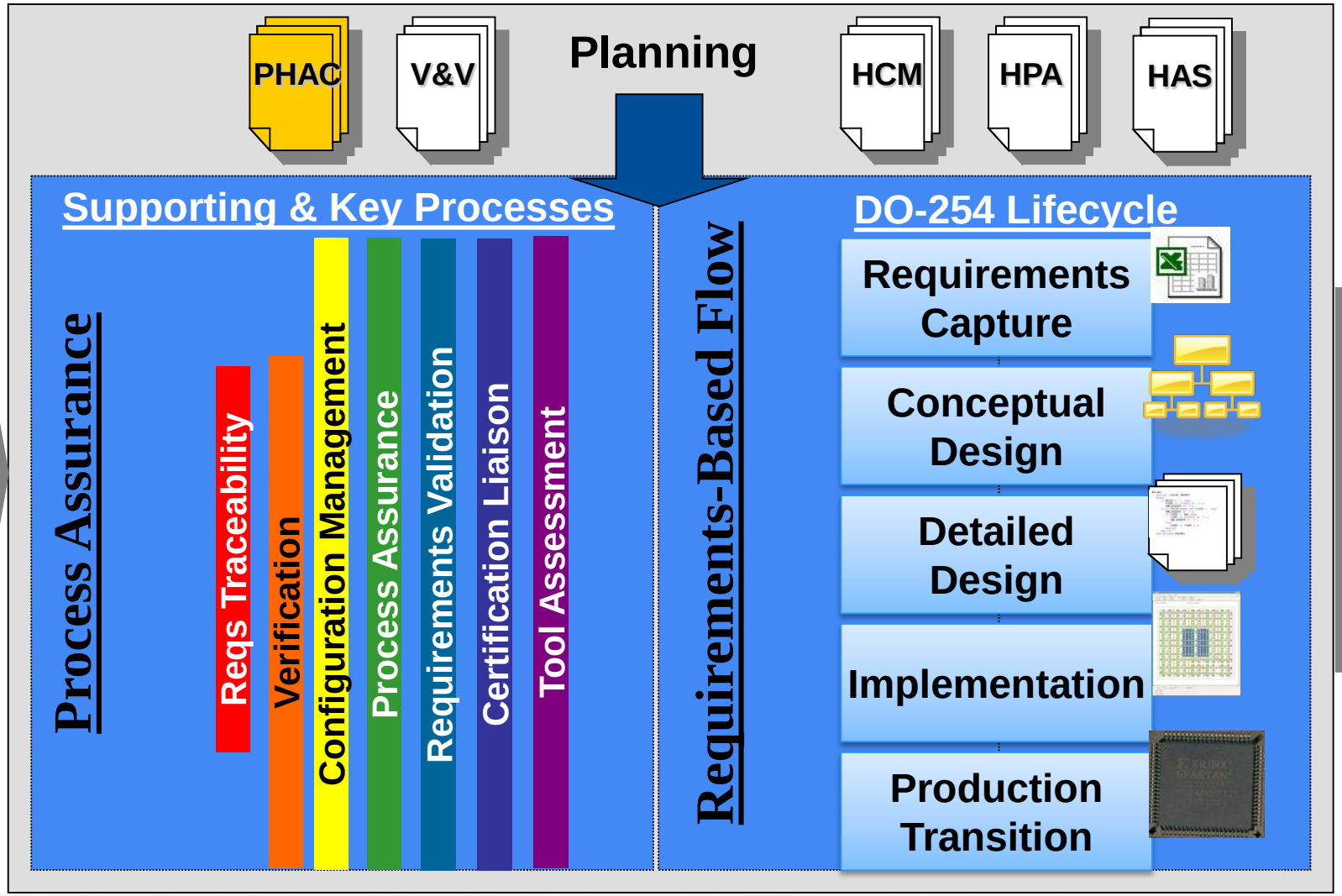
Design Flow

DO-254 Process as you'd see it shown in the DO-254 Document

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

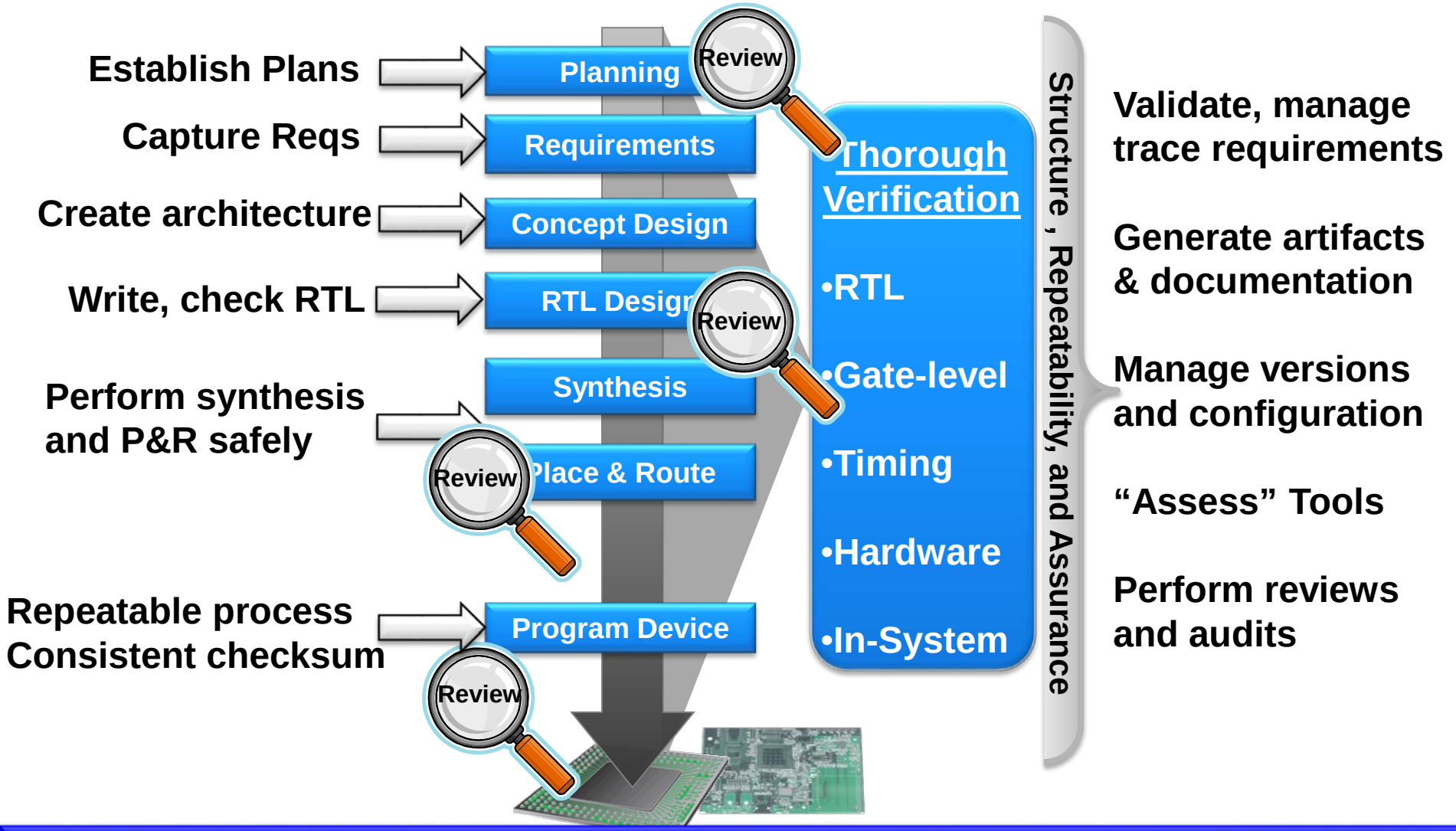
What is DO-254?

A Requirements-Based Design Flow with Strict Process Assurance



May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

A DO-254 Compliant FPGA Flow



DO-254 = A thoroughly planned, highly structured, repeatable, requirements-based flow, which delivers a design that "performs its intended function."

Planning (4.0)

- Many DO-254 cost overruns can be avoided by proper planning
- Investing in training, consulting, and research should be part of the planning phase
- The PHAC* is the master planning document covering all aspects of a DO-254 project
  - With focus on "how" to meet DO-254 objectives
  - PHAC is the agreement between applicant and certification authority on the method for compliance
  - Deviations need to be discussed and reviewed, documented in HW accomplishment summary (HAS)
- A SOI-1 audit to review the PHAC typically occurs at the end of the planning phase

* Plan for Hardware Aspects of Certification

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Requirements (10.3.1)

- Requirements management is a key DO-254 theme
- DO-254 flows mandate that requirements be
  - Captured – stored for retrieval (5.1)
  - Validated – reviewed against numerous criteria (6.3.3.1)
  - Managed – a process to manage changes
  - Traced – links to design/verification activities (10.4.1)
- Requirements are validated and fed back to the appropriate processes at every design stage
- Requirements may be derived
  - Derived from a design decision, possibly no parent requirement
- Requirements tracing problems are one of the most common “findings” in SOI audits

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Conceptual Design (5.2)

- **High-level design concept that may be assessed to determine the potential for the resulting design implementation to meet the requirements**
- **Concepts are usually informally verified (providing information for design decisions)**
- **Conceptual design description includes**
  - **Key characteristics & parameters**
  - **Product architecture – major components, interfaces**
  - **Safety-related aspects and constraints**
- **Conceptual design description should**
  - **Walk reader through the design (similar to datasheet)**
  - **Include a visual explanation (e.g. block diagram)**

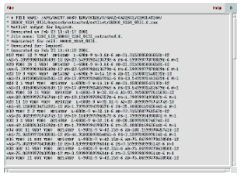
May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Detailed Design– RTL (5.3)

- RTL design is part of the DO-254 lifecycle phase "Detailed Design"
- Requirements ⇔ RTL
  - RTL is written from and must trace to requirements
- RTL coding standards should be documented and verified (reviews and/or checked with tool) (10.2.2)
- RTL code must be reviewed
  - Internally, design process gates (e.g., PDR, CDR)
  - Externally, typically in SOI-2 audit
  - Reused RTL source code is no exception
- Artifacts from design must be produced and put under configuration management

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Detailed Design (Synthesis, P&R)



- **DO-254 focus is on design assurance, *not optimization***
  - **Some DERs are very concerned with synthesis**
    - **Document your tool usage and ensure it is examined during design reviews**
  - **Know your tool and its default operation**
  - **Ensure you are using all safety-appropriate settings**
- **Tool output should be repeatable**
- **Tool output must be verified**
- **Pertinent constraints should be linked back to requirements**
- **Mentor has a paper that can help identify design assurance concerns and appropriate synthesis settings**

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Implementation (5.4.1)

- Produce hardware item from the model (i.e., program FPGA from P&R generated bitstream)
- Integrate into the system
- Debug
- Involves requirements-based testing of the HW item
  - Standalone
  - In the target system
- Last step before committing to the production process
- Ensure your design process establishes a consistent and repeatable bitstream
  - You will likely be asked to demonstrate this, checksum will be examined

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

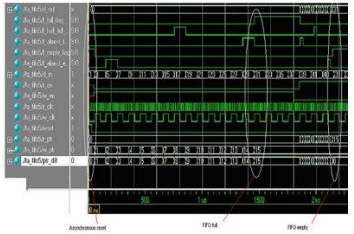
Production Transition (5.5.1)

- Establish a process to consistently replicate the HW item
- Document procedure including all the design and manufacturing data
- Consider safety aspects of manufacturing and manufacturing controls
  - Safety aspects are tested at box level
- You will likely be asked to demonstrate your repeatable manufacturing process

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

DO-254 Supporting Process Info/Tips

RTL Verification (6.2)

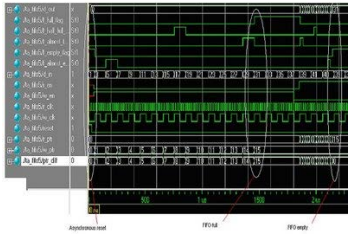


- Requirements ⇔Verification
  - Tests are developed from requirements (not the design)
  - Test plan, testbench, test procedures, test results must trace to requirements
- DAL A/B designs require (Appendix B)
  - Independence
    - Someone other than designer must develop (or at least review) tests
    - Designer can do some informal verification (but generally not for DO-254 credit)
  - Layered methods of assurance
  - Advanced methods
    - Typically done as “elemental analysis” (i.e., requirements-based testing combined with a target of 100% statement and decision coverage)
  - Robustness testing (testing outside normal conditions)
  - CDC analysis does not fit neatly into a specific requirement of DO-254 but should be considered for safety purposes
- Verification must be repeatable and will be audited (usually during SOI-3)

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

DO-254 Supporting Process Info/Tips

Gate-Level Verification



- Requirements-based tests (with timing) should be re-run after synthesis/P&R
- Hot topic is how much gate-level simulation is needed
  - Some say run complete test suite
  - Others understand not possible
  - LEC can possibly augment/reduce amount
    - Some programs starting to use this
    - Cannot eliminate gate-level simulation entirely
    - Must be used with Static Timing Analysis
- Verification must be repeatable, reviewed and will be audited (usually during SOI-3)
- Verification is not done until HW item is tested in target system – another hot topic…

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Configuration Management (7.0)

- Purpose is to control the DO-254 lifecycle and outputs
  - Ensures replication of data, method of identifying and tracking changes
- Requires identifying and documenting items
- Items placed under CM include
  - Documents
  - Design data
  - Hardware
  - Tools
- What needs to be under CM and to what degree depends on the device's DAL

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

DO-254 Supporting Process Info/Tips

Reviews and Audits (8.0, 9.0)

- **Process Assurance**
  - **Must be an independent process**
  - **To assess the process according to plan**
  - **Identify and correct deviations**
  - **Best practice is to hold internal reviews before external audits**
    - **Use "FAA CEH Job Aid" as a preparation tool**
- **Certification Liaison**
  - **Job Aid clarifies level of involvement needed**
  - **Typically four SOI (stage of involvement) audits**
    - **SOI-1 (planning)**
    - **SOI-2 (design)**
    - **SOI-3 (verification)**
    - **SOI-4 (completion)**

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Agenda

- History and Current State of DO-254
- DO-254 Compliance Overview
- The Joys and Sorrows of DO-254 Compliance
- Preparing for a Successful DO-254 Program
- Conclusion

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Design Assurance

Premium Price, Competitive Advantage

Flexibility & Freedom

Foundation for Security Assurance

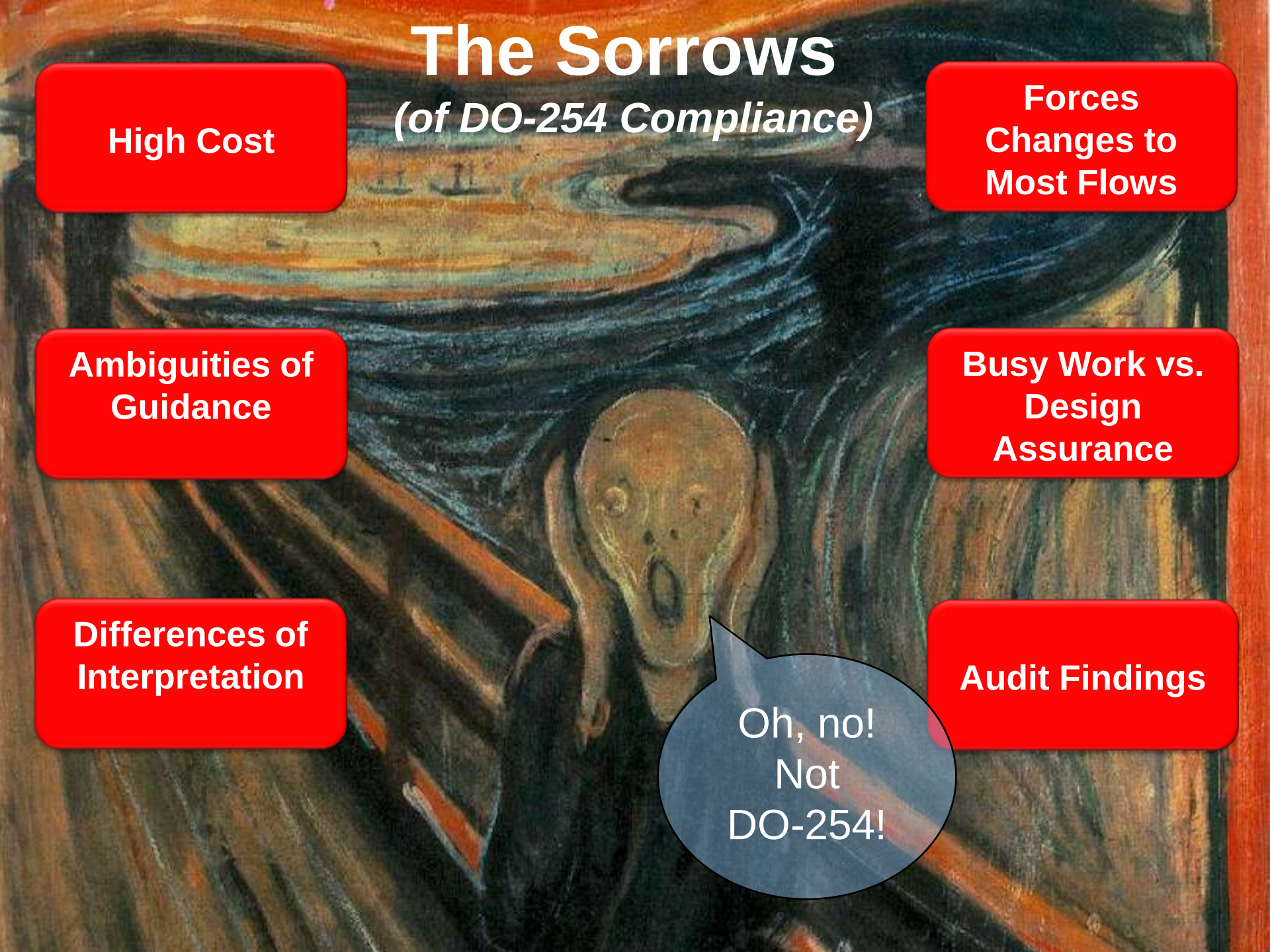
Enforces Examination of Design Flow

Passing the Final Audit!

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

The Sorrows

(of DO-254 Compliance)



Benefits/Challenges of a DO-254 Program

- DO-254 has many aspects that are a double-edged sword
  - With the good, comes the bad
  - With the bad, improvements are being made
- Its almost impossible to separate the issues
- We will talk about the pros/cons of many aspects of DO-254 by issue

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Benefits/Challenges

Design Assurance

1 Goal/Intent of DO-254 is Design Assurance

- + Most aspects of DO-254 support this goal
  - + Examples
    - + Requirements-based design
    - + Thorough, overlapping verification
    - + Reviews/audits
- – Some aspects of DO-254 questionably contribute to design assurance
  - – Examples
    - – Tool assessment or qualification
    - – Varying interpretations of certain objectives

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Ambiguity vs. Flexibility

DO-254 guidance is not meant to be prescriptive

- In theory…
  - This gives applicants much freedom and flexibility to meet objectives
  - Ensures DO-254 does not become outdated as technology advances
- New guidance and training is providing clarification and more consistency
- DO-254 User Groups are tackling ambiguous areas

- Certification authorities have come primarily from the software domain
- Interpretations and opinions as to how to meet DO-254 objectives varies wildly

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Benefits/Challenges

Design Flow Changes

DO-254 compliance will mean design flow changes

- + Many of these changes are long overdue
  - + Design complexity has dramatically increased but development methods (especially verification) have not kept up
- + Changes should result in higher quality designs
- + An improved, consistent, compliant design flow
  - + Reduces compliance cost
  - + Can be competitive advantage
- – Changes requirement additional investment
  - – Training
  - – Additional resource
  - – Audit services, etc
- – Compliance can be very costly
  - – 4X increase is not uncommon
  - – Especially first programs requiring compliance

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Benefits/Challenges

Audits and Findings

Audits are required and findings are common

- Audits are a key element of assurance
- Many findings can be avoided with proper planning
- New AEH "Job Aid"* is a vital tool to help
  - Use it to hold mock audits prior to real ones
- Passing the final audit should be cause for celebration

- Audit findings can
  - Disrupt schedule
  - Cause rework
  - Be costly

* Conducting Airborne Electronic Hardware Reviews Job Aid, Feb 2008, available free from www.faa.gov

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Benefits/Challenges

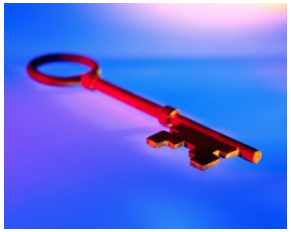
Design->Security Assurance

Security is the next big "Assurance" issue

- **DO-254 and its design assurance principles are pre-requisites for security assurance**
  - **Lays the foundation for additional security assurance**
    - **First, ensure device performs intended function**
    - **Next, ensure no one has tampered with the function**
- **DO-254 is not intended to provide security assurance**
- **DO-254 does not directly address security issues**

* Conducting Airborne Electronic Hardware Reviews Job Aid, Feb 2008, available free from www.faa.gov

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.



Key *Assurance* Principles

Design Assurance

- Ensures a device performs its intended function
- Includes principles of
  - Planning
  - Requirements-driven flow
  - Structure and repeatability
  - Thorough verification
  - Configuration management
  - Reviews and audits
- DO-254 compliance is a means to achieve design assurance

Security Assurance

- Ensures a device/process is not tampered with
- Builds on design assurance
  - Stricter oversight of contractors
  - Tighter security on configuration management
  - Verification to find or prevent malicious intent
- Security requirements must address these issues

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Adding Security-Focused Tasks

With DO-254 You Have…

- Design/verification linked to requirements
- Configuration management to ensure process structure
- Layered verification to verify intended function
  - Code coverage to find unintended code

For Security You Might Add

- Closer inspection of this traceability
- Configuration management to ensure secure access
- Additional verification to search for malicious intent
  - Code coverage to find maliciously added code
  - Model checking to find unintended behaviors
  - Equivalency checking to ensure no changes to netlists

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Agenda

- History and Current State of DO-254
- DO-254 Compliance Overview
- The Joys and Sorrows of DO-254 Compliance
- Preparing for a Successful DO-254 Program
- Conclusion

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Best Practices
Observed from Other Companies

- **Invest in training, consulting, proper preparation**
  - **Upfront investment can save a lot of later anguish**
  - **Work out flow issues/inefficiencies in advance**
  - **Develop thorough and proper plans, and review early with DER**
- **Take QA/compliance process role seriously**
  - **Involvement throughout project**
  - **Driving internal audits prior to SOI reviews**
  - **Use the AEH Job Aid as a guide**
- **Share best practices from one group to another**
- **Work with others in the industry who take DO-254 seriously**

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Best Practices
*Advice from a DER**

Tammy Reeve
Patmos Engineering

- **Get DER involved early and seek agreement**
- **Be proactive about requirements traceability**
- **Identify and deal with COTs up front**
- **Ensure verification is repeatable, traceable, maintainable, and includes board level testing**
- **Don’t make tool assessment harder than it has to be**
- **Ensure device programming/build environment is repeatable**

*This is a small set of items that Tammy has presented at various events. Full presentations are available upon request.

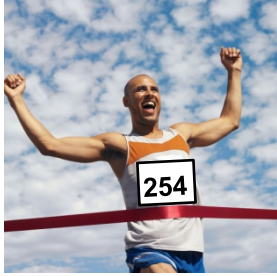
May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Agenda

- History and Current State of DO-254
- DO-254 Compliance Overview
- The Joys and Sorrows of DO-254 Compliance
- Preparing for a Successful DO-254 Program
- Conclusion

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.

Conclusion



- DO-254 provides guidance for *Design Assurance* of airborne electronic hardware
- It is spreading from civil/commercial air to other similar industries including military
- DO-254 is like a double-edged sword
  - It has its pros/cons, its advocates and its critics
- DO-254 is costly but valuable
  - Costs can be reduced with experience and best practice
  - Value can be both immeasurable and extendable

May be published with permission by MAPLD 2009
Copyright ©2000-2008, Mentor Graphics.


Mentor Graphics®
www.mentor.com
www.mentor.com/go/do-254

More Mentor at MAPLD

What	When
Exhibits – Information and demonstrations of Mentor's FPGA design and verification solutions	Tuesday, 2:30-6:00pm
Avoiding Metastability in FPGA Devices (Poster session)	Wednesday, 3:10-6pm
A Requirements-Driven PLD Design Flow (Poster session)	Wednesday, 3:10-6pm
Architectural Analysis for Quantifying Trade-offs to Make the Right Decision for Implementation (Poster session)	
Vendor Independent SEE mitigation solution for FPGAs (Poster session)	Wednesday, 3:10-6pm
Synthesis of fault tolerant circuits for FSMs & RAMs (Poster session)	Wednesday, 3:10-6pm
Formal Verification of Advanced Synthesis Options	Thursday, 9:00-9:20am
RTL and Synthesis Design Approach to Radiation-Hardened and Fail-Safe Targeted Applications	Thursday, 10:20-10:40am

Copyright ©2000-2008, Mentor Graphics.