Application of DO-254 Level A (Appendix B)

Design Assurance Objectives of

Elemental Analysis

To

Mixed Signal (Analog/Digital)

Discrete Circuitry

By

Dave Duncan
Purple Seal Inc.
Executive Summary

When distilled down DO-254 (Design Assurance) has three primary objectives:

a) Control of the “Configuration” (Requirements, Documentation, Physical Hardware, Validation, etc)

b) Requirements Based Design (Design Traceability)

c) Requirements Based Verification (Verification Traceability)

When these three objectives are applied with a level of independence the reduction in or elimination of common mode errors is the result.

As part of DO-254’s guidance, Level A & B programs are to implement Advanced Verification according to Appendix B. Of the suggested methodologies Elemental Analysis is most often implemented by conducting a coverage analysis of a PLD/FPGA/ASIC design at the VHDL (design coding language) level of abstraction. What this is really accomplishing is an evaluation the “quality” of the implementation of the primary objectives as stated above: i.e. Does independent requirements based verification actually cover requirements based design? For PLD/FPGA/ASIC this analysis is semi automated by built-in tool suites that are used during verification by simulation. These tools track test vectors (from test cases) through the logic as the simulation is being run. The controls and outputs of typical tools allow a coverage analysis with example granularity showing:

a) Line coverage - Coverage of each logical statement in the VHDL design during the tests

b) Toggle coverage - Coverage of all variables (circuit nodes) toggling both high and low during the tests

c) Combinational logic coverage - The logic has been covered by the tests, generally a reduced map of coverage not a $2^n$ coverage

d) Assertion (functional) coverage - Generally the fact that each variable or node that can cause a transition in a state machine or output node, has shown that ability to do so in isolation of the other variables or nodes

There is even a qualification exemption for integrated coverage tools, which are “used to satisfy the completeness of verification.” But there are no tools, which closely mimic those coverage tools for, the discrete hardware designer.

The challenge is to apply this concept (Code Coverage) to mixed signal discrete circuits, where there are no tools to automate the process, and the verification is performed on the physical circuits, not on an abstraction. This paper presents an approach that mimics the action of the "Coverage" tools in a VHDL design. This mimic is limited to specific nodes and criteria appropriate for the mixed signal (analog and digital) nature of this design.

---

1 DO-254 Section 11.4.1 Item 4.
## Release & Revision

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft</td>
<td>Initial draft for limited review</td>
<td>5/31/08</td>
</tr>
<tr>
<td>1.0²</td>
<td>Release for inclusion in data package for: 2008 National Software and Airborne Electronic Hardware Standardization Conference</td>
<td>7/10/08</td>
</tr>
</tbody>
</table>

---

## Contact Information

Dave Duncan  
Purple Seal Inc.  
2121 County Road 143  
Clearwater, MN 55320  
dduncan@purple-seal.com  
320-761-3949  

² Purple Seal hereby grants full use of this paper to attendees of the 2008 National Software and Airborne Electronic Hardware Standardization Conference.
1 Introduction
1.1 Scope
This document presents an approach to applying DO-254 Level A to a mixed signal LRM. The primary content of this paper is a narrative describing the key activities which implement elemental analysis. As a part of that narrative the key points in the main processes that elemental analysis depends upon are highlighted.

1.2 Acknowledgements
The examples used in this paper were derived from work that was performed to demonstrate this compliance by Purple Seal Inc. & Crane Aerospace and Electronics, ELDEC Applied Power Products Division. These descriptions are complete to the point of documenting the approach used without describing the details of process implementation, which are proprietary to Crane Aerospace. Additionally requirements, diagrams and other examples are representative only and are not intended complete enough to implement a design, or represent an actual design, and are included here only for illustrative purposes.

1.3 Prerequisites
1.3.1 Design Elements
In order to effectively analyze the verification coverage, the design should be parsed into manageable sub circuits. The exact level is somewhat arbitrary but consideration should be given so that the scope of the test cases’ coverage can be analyzed with relative ease. The rule of thumb used is to parse sub circuits down until all anomalous behavior within the sub circuit is seen at the outputs as an out of failure of verification. This is the level where the design is traced to the requirements: i.e. Design Element to the Requirements and the Components BOM to the Design Element. The design should be complete in coverage (all requirements covered) and under configuration control.

The example shown in Figure 1 shows a basic functional power supply. There are four primary or Functional Elements parsing these further takes us to the Design Element level seen in Figure 2.

![Figure 1 Example LRM Functional Elements](image-url)
1.3.2 Verification

There are no special considerations that need to be applied to verification. To effectively perform coverage analysis the “test cases” (physical test, simulation, analysis, etc.) should be complete in coverage (all requirements covered) and under configuration control.
2 Elemental Analysis

“Elemental analysis provides confidence and evidence that design errors are precluded by separating a complex implementation of the FFP into elements at the level that the designer generated it. This analysis method provides a measurement of the verification process to support the determination of verification coverage and completeness, and is most suited where the detailed design is visible and under configuration control.”

2.1 Identification of Nodes

The first step in the analysis is identifying the various nodes within each design element. The data from this step will be identified and documented. An example of this documentation can be found in Appendix B (Data Examples)

Table 1 Example Node Data Sheet.

The guidance for determining what nodes to include is as follows:

a) Design Element Inputs
b) Design Element Outputs
c) Critical Internal Nodes
   a. Transition between circuit types (analog to digital, logic families, across isolation barriers)
   b. Transition between circuits that have significant drive or current characteristics
   c. Transition between one sub-function and another

To continue the examples from Section 1.3.1, the Power Stage of the Aux Supply Design Element might be implemented as shown in Figure 3.

Figure 3 Example Power Stage Implementation

Using the above guidelines the nodes identified would be as shown in Figure 4.

---

3 DO-254 Appendix B
2.2 Identification of Corner Cases

Establishing the criteria, or Corner Cases, for the coverage analysis involves a qualitative assessment of the circuit function and the environmental or input parameters for which the performance should be verified. Typical corner variables would be:

a) Temperature (High, Low, Step Changes)

b) Input Power (High, Low, Step Changes, Transients)

c) Output Load (High, Low, Step Changes, Transients)

The idea is not to identify all the corner cases for a particular node, as this would be impractical bordering on impossible for an analog circuit, but to establish those corners of operation that push or stress the circuit or components. The above example would yield 75+ corners of operation that would need to be covered. Sound engineering judgment would parse down this list: For example, High Temperature, Low Input Voltage and High Output Load would maximize the current through the circuits and IR voltage impact on operation.

Each corner case needs to identify a measurable quantity: Voltage, Current, Frequency, Duty Cycle, etc., and the quantifiable conditions under which those measurements should be valid (Temperature, Air Flow, Load Conditions, etc.).

These corner cases must be documented in a manner that their traceability to a circuit node and eventually the case verifying that corner can be established. An example of this documentation can be found in Appendix B (Data Examples).

2.2.1 FFP Cross Referencing

During the node determination a cross reference of Design Elements and Nodes should be developed. This is used to associate circuit nodes and their possible contributions to aircraft hazards. It may also be used to limit the scope of elemental analysis to only those FFP that could contribute to a Level A or B hazard. An example of this documentation can be found in Appendix B (Data Examples).
2.3 Analysis of Case Coverage

This implementation of Elemental “Coverage” Analysis takes advantage of the verification traceability requirements under DO-254. Each “test case” (physical test, simulation, analysis, etc.) will have an ID associated with it: these will be used either manually or with a tool to manage the traceability between verification and the requirements. These same IDs will also be used to document the coverage of the nodes achieved by each case.

The coverage analysis takes the collated Design Element coverage reports and tabulates (within the design element worksheet) which corners of operation were covered.

The tradeoffs of early vs. later Elemental Analysis are that the early analysis will allow feedback of deficiencies with minimal schedule impact, but the analysis is qualitative in nature. Later application is quantitative in nature, but is likely to have significant schedule impact. A reasonable compromise is to start the analysis as the verification procedures (cases) are going into the final review and approval stages: this will naturally extend the analysis into dry runs, if not actual for-credit runs, of the verification.
2.4 Analysis of Coverage

The analysis of the coverage can be done either manually or semi-automated with scripting tools to sort and compare the data. Depending on the tasks automated these tools should also fall under the qualification exemption of the code coverage tools\(^4\) referenced in the Executive Summary.

2.4.1 Nodal Coverage

Nodal coverage is simply a Yes/No analysis of the data sheets for coverage of every identified corner case for every identified node. This level of analysis should identify hardware that is not covered by verification. If this occurs, it is indicative of an incomplete verification case development, or perhaps an ambiguous or incomplete requirement and should trigger further investigation.

2.4.2 Design Element Coverage

Design element coverage has prerequisites of:

a) 100% Design traceability to requirements
b) 100% Verification traceability to requirements
c) 100% Nodal coverage

This coverage analysis reconciles the traceability using the following logic;

a) A given design element traces to a sub-set of requirements, therefore the verification cases traceable to the same sub-set of requirements should provide full coverage of the design element. The test of this is that all of the case IDs documented in the node data sheets for a given design element do in fact also show up in the case IDs traceable to that design element’s requirement sub-set.

a. For the case ID’s from above that were not documented in the nodal data sheets above, do they cover the design element, but perhaps cover a corner that was not identified as critical? If it is found that a case does not target the design element it is indicative of an incorrect verification trace, or perhaps an ambiguous or incomplete requirement and should trigger further investigation.

2.5 Analysis Team

The purpose of elemental analysis is to evaluate the completeness of the requirements based verification activities against the targeted hardware. A level of independence should be maintained to continue the reduction in common mode errors. (Independence between coverage analysis and the verification cases being analyzed for coverage.)

2.6 Problems and Deficiencies

The mechanism for feeding back problems or deficiencies is the same as what is used for the project as a whole; however, those PRs triggered by elemental analysis should be tracked so that regression elemental analysis can be accomplished with relative ease. The number of PRs also may serve as a metric as to the effectiveness of the initial requirements based design and verification.

\(^4\) DO-254 Section 11.4.1 Item 4.
2.7 Developing Process

Appendix C (Compliance Checklist) may be used along with this paper as an aid in developing processes or work instructions that will comply with the objectives in DO-254 Appendix B for Level A or B hardware designs.
3 Appendix A (References)

3.1 Documents

DO-254 Design Assurance Guidance for Airborne Electronic Hardware

3.2 Acronyms and Abbreviations

ASIC Application Specific Integrated Circuit
BOM Bill Of Material
COTS PWM Commercial Off the Shelf Pulse Width Modulator
FET Field Effect Transistor
FFP Functional Failure Path
FPGA Field Programmable Gate Array
ID (ID’s) Identification
IR Current * Resistance = Power (Ohms Law)
LRM Line Replaceable Module
PLD Programmable Logic Device
PR (PRs) Problem Report
VHDL Very High Level Descriptive Language

3.3 Terminology

Code Coverage A measure used to evaluate the completeness of software testing
Corner Case Conditions where multiple environmental or operational parameters are simultaneously at their extremes
Design Element The lowest level of the design’s architecture where requirements are captured.
Functional Element High level functional block or circuit
Node A specific interconnection point within a discrete circuit
Qualitative Data that can not be traced to a physical or traceable measurement, the data is somewhat subjective
Quantitative Data that is traceable to a physical or traceable measurement
Traceability An identifiable association between pieces of data
### 4 Appendix B (Data Examples)

#### Table 1 Example Node Data Sheet

<table>
<thead>
<tr>
<th>Circuit Node</th>
<th>Voltage (H/L)</th>
<th>Current (H/L)</th>
<th>Freq. (H/L)</th>
<th>H Temp</th>
<th>L Temp</th>
<th>H Load</th>
<th>L Load</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Input</td>
<td>13V</td>
<td>11V</td>
<td>90ma</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13V</td>
<td>11V</td>
<td>90ma</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13V</td>
<td>11V</td>
<td>90ma</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13V</td>
<td>11V</td>
<td>90ma</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

#### Table 2 FFP vs. Design Cross reference

<table>
<thead>
<tr>
<th>FFP (Fault Tree)</th>
<th>Design Element</th>
<th>Circuit Node</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 5 Appendix C (Compliance Checklist)

### Table 3 Compliance Checklist

<table>
<thead>
<tr>
<th>DO-254 Reference</th>
<th>DO-254 Guidance</th>
<th>Coverage Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO-254 Section 3.3.1.1 Analysis Methodology - 1</td>
<td>Identification and a definition of the elements at an appropriate level of the hardware design</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.1 Analysis Methodology - 2</td>
<td>The verification coverage to which each element should be verified</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.1.1 Element Determination</td>
<td>The analysis may show either that all the low-level primitive blocks, such as counters, registers, multiplexers, adders, op amps and filters, have been adequately tested or that all groups of interconnected primitives have been adequately tested and achieve the verification coverage criteria.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.1.2 Performing Elemental Analysis Environment 1</td>
<td>Tests with the circuitry implementing the functional path installed in the target assembly.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.1.2 Performing Elemental Analysis Environment 2</td>
<td>Tests performed on a standalone prototype. Such tests are typical for an ASIC or PLD.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.1.2 Performing Elemental Analysis Environment 3</td>
<td>Manufacturing acceptance tests. Note: Since manufacturing tests often are not based on the requirements, manufacturing acceptance tests may be restricted in their application to elemental analysis.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.1.2 Performing Elemental Analysis Environment 4</td>
<td>A post-layout simulation, typically for an ASIC or PLD, that has been assessed and, if necessary, qualified for use as a verification tool as described in Section 11.4.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.2 Analysis Resolution</td>
<td>Shortcomings may arise if the test cases simply do not test the elements in the hardware item in compliance with the criteria in Appendix B, Section 3.3.1.1.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.2 Analysis Resolution</td>
<td>The requirements should be modified or additional derived requirements identified. Additional verification tests should then be developed for the new or revised requirements, executed and analyzed.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.2 Analysis Resolution</td>
<td>The hardware item may contain functions that are not used in its target circuit application, such as test structures used only for component-level acceptance tests. Such functions should either be shown to be isolated from the other used functions or shown to present no potential anomalous behavior that could have an adverse effect on safety.</td>
<td></td>
</tr>
<tr>
<td>DO-254 Section 3.3.1.3 Life Cycle Data</td>
<td>Identify the FFPs to be addressed by elemental analysis, and propose at what levels in the design hierarchy the elements are defined and how they are to be analyzed for verification adequacy, which are parts of the verification coverage completion criteria.</td>
<td></td>
</tr>
</tbody>
</table>

© Purple Seal Inc 2008
<table>
<thead>
<tr>
<th><strong>DO-254 Reference</strong></th>
<th><strong>DO-254 Guidance</strong></th>
<th><strong>Coverage Reference</strong></th>
</tr>
</thead>
</table>
| **DO-254 Section 3.3.1.3**  
Life Cycle Data  
2. Level of Analysis | Describe the methods and identify the FFPs addressed in the analysis and the levels in the design hierarchy at which the analysis was performed. | |
| **DO-254 Section 3.3.1.3**  
Life Cycle Data  
3. Traceability Data | Ensure that the traceability data, as described in Section 10.4.1 shows the explicit relationship of the verification procedures to the elements in the elemental analysis. | |
| **DO-254 Section 3.3.1.3**  
Life Cycle Data  
4. Additional Verification or Requirements | Identify the verification test cases and requirements added or modified as a result of the elemental analysis. | |
| **DO-254 Section 3.3.1.3**  
Life Cycle Data  
5. Verification Completeness | State the level of the verification completeness achieved for the FFPs addressed by elemental analysis, including identification of the analysis discrepancies not resolved by modification to verification tests or requirements and the rationale for acceptability. | |