FPGA-Development for safety critical application

Christoph Meyer & Rafael Reimann

Institute of Microelectronics
Intro

• Safety critical devices for avionics
  • Why DO-254?
  • What is DO-254?

• Development Process
  • Requirements Capture
  • Design
  • Verification
  • Validation

• Costs & Benefits
We want safe planes
No dangerous situations
No crashes
How can we be sure a plane is safe?
How can we guarantee a plane is safe?
DO-254
DO-254 applies for development of complex components
DO-254 does not define how to implement
DO-254 defines the development process
DO-254 defines Teams
DO-254 defines Documents
DO-254 defines Reviews
DO-254 defines Interactions with Authorities
DO-254 makes development transparent
DO-254 helps to avoid errors
Nothing can be 100% safe
No device has Zero failure rate
No Development is 100% free of errors
Not all possibilities can be forseen and tested
What failure rate is acceptable?
<table>
<thead>
<tr>
<th>Design Assurance Level (DAL)</th>
<th>Description</th>
<th>Target System Failure Rate</th>
<th>Example System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level A (Catastrophic)</td>
<td>Failure causes crash, deaths</td>
<td>$&lt; 1 \times 10^{-9}$</td>
<td>Flight controls</td>
</tr>
<tr>
<td>Level B (Hazardous)</td>
<td>Failure may cause crash, deaths</td>
<td>$&lt; 1 \times 10^{-7}$</td>
<td>Braking systems</td>
</tr>
<tr>
<td>Level C (Major)</td>
<td>Failure may cause stress, injuries</td>
<td>$&lt; 1 \times 10^{-5}$</td>
<td>Backup systems</td>
</tr>
<tr>
<td>Level D (Minor)</td>
<td>Failure may cause inconvenience</td>
<td>No safety metric</td>
<td>Ground navigation systems</td>
</tr>
<tr>
<td>Level E (No Effect)</td>
<td>No safety effect on passenger/crew</td>
<td>No safety metric</td>
<td>Passenger entertainment</td>
</tr>
</tbody>
</table>
Our Project
System Engineer

Specifies the system

IP

Captures requirements
The Requirement should be uniquely identified
The Requirement should be understandable
The Requirement should be testable
The IP interface shall be easy to address

Wrong messages shall be discarded
After the system reset is applied, the IP shall set the FIFO “X” to empty, if its value is read, then the IP shall return the value 0xFFFFFFFF.
The System shall complete the Ethernet frame by byte padding when the message to send is shorter than 100 bytes.
Design Engineer

Concept for the Design
Main Functions:
- Forward byte stream
- Check frame length
- Extend byte stream if needed
Design Item

DI_012_b:
The block zero_padding is extending the byte stream for frames smaller than 100 bytes by keeping the valid signal high and setting the data signal to zero until the frame reaches 100 bytes.

Covers Req_002_a

Req_002_a:
The System shall complete the Ethernet frame by byte padding when the message to send is shorter than 100 bytes.
Design Items cover Requirements
Design Items are covered in the Code
Coverage 100 %
DI_012_b:
The block zero_padding is extending the byte stream for frames smaller than 100 bytes by keeping the valid signal high and setting the data signal to zero until the frame reaches 100 bytes.

Covers Req_002_a
Verification Engineer

**Verification** ensures that the device performs the intended function as specified by the requirements.
IP Requirements

Functional Testing

Requirements Coverage Analysis

Code Coverage Analysis

Testing Complete

Incomplete Requirements Coverage

Incomplete Code Coverage
For each Requirement there is at least one Test Procedure
TC_133_b:
Sending a message that is shorter than 100 bytes and sending a message that is longer than 100 bytes.

Tests Req_002_a

Req_002_a:
The System shall complete the Ethernet frame by byte padding when the message to send is shorter than 100 bytes.
Sending a message that is shorter than 100 bytes and sending a message that is longer than 100 bytes.

Step 0  Send a message with 45 bytes  Expecting a message with byte padding
Step 1  Send a message with 99 bytes  Expecting a message with byte padding
Step 2  Send a message with 100 bytes  Expecting a message without byte padding
Step 3  Send a message with 125 bytes  Expecting a message without byte padding
Validation ensures that the requirements are correct
Validation ensures that the requirements are complete
Validation ensures that the requirements are verifiable.
<table>
<thead>
<tr>
<th>Requirements</th>
<th>Design Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req_001_a</td>
<td>DI_012_b</td>
</tr>
<tr>
<td></td>
<td>DI_001_c</td>
</tr>
<tr>
<td>Req_002_a</td>
<td>DI_022_a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Test Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req_001_a</td>
<td>TC_003_b</td>
</tr>
<tr>
<td></td>
<td>TC_017_a</td>
</tr>
<tr>
<td>Req_002_a</td>
<td>TC_133_c</td>
</tr>
<tr>
<td>Req_003_a</td>
<td>TC_133_c</td>
</tr>
<tr>
<td></td>
<td>TC_051_a</td>
</tr>
<tr>
<td></td>
<td>TC_52_b</td>
</tr>
</tbody>
</table>
Tools

Verification Report

Quality Center

TC_003_b

Req_001_a

Traceability Matrix

Req_001_a

Reqtify

DI_012_b

VHDL
How did we reach a failure rate of $10^{-9}$
Less than 1 failure in $10^9$ hours
Less than 1 failure in $10^5$ years
Single Event Upset due to Neutron Flux
Depends on Location
Depends on Altitude
Depends on Device
Depends on Technology
Depends on Sun Activity
Worst Case for one Flip-Flop: $0.72 \times 10^{-9}$
Error Detection
Error Correction
Industry average: 75...150%
DO-254

- Defines the process
- Requirements
- Transparent
- 100% Coverage
Thank you

Christoph Meyer & Rafael Reimann

Institute of Microelectronics