2022 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE
MUNICH, GERMANY
DECEMBER 6 - 7, 2022

Types of Robustness Test According to DO-254 Guideline for Avionic Systems

Gözde Asena KILINÇ, Design Verification Engineer, ASELSAN A.Ş., Ankara, TURKEY
(*gakilinc@aselsan.com.tr*)
Yavuz AKSU, Design Verification Engineer, ASELSAN A.Ş., Ankara, TURKEY
(*yaksu@aselsan.com.tr*)
Fatih BAYSAL, Design Verification Engineer, ASELSAN A.Ş., Ankara, TURKEY
(*fbaysal@aselsan.com.tr*)

***Abstract*—RTCA DO-254 is a safety-critical guideline for aircraft electronic hardware, which consists of five Design Assurance Levels (DAL) to make flights as safe as possible and to prevent time and financial losses. Safety criticality of Design Assurance Levels decrease from DAL A to DAL E. As an integral part of DO-254 guideline, requirement-based verification is used to analyze behavior of the design under normal circumstances. However, DAL A or DAL B systems' failure could cause hazardous, irreversible results so that those systems require additional tests rather than only requirement-based verification, which are called robustness tests. Robustness tests provide coverage for undesired conditions and edge cases. This paper examines different types of robustness tests such as invalid access error tests, clock robustness tests, reset robustness tests, glitch filter tests, invalid state transition tests and explains their implementation and expected outcomes of these tests in PLD verification processes.**

Keywords—PLD, DO-254, DAL, requirement-based verification, robustness, UVM, SystemVerilog, interface

I. INTRODUCTION

There are lots of safety-critical systems in modern aviation, they should be able to operate under all conditions including uncertain environments. Requirements-based tests are necessary to observe, whether the hardware operates its functionalities as intended or not. Robustness test cases characterize behavior of the design at the boundaries and beyond the boundaries of the specified operating limits. Robustness tests should be done for safety-critical systems to know how neatly hardware would react to situations not mentioned in the design requirements and also, unexpected cases that allowed by requirements. The design is regarded as robust, if the test passes for the tested conditions.

This paper examines different types of robustness test methods such as clock frequency and duty cycle variance, invalid access, unexpected reset, glitch generation, and invalid state transition based on simulation in programmable logic devices (PLD) verification process.

First of all, during invalid access error tests, the aim is to create error conditions and expected to see error occurrence on the system while the system continue as intended. At second, clock robustness tests verify whether data transfer is disturbed or not when system clock is changed Additionally, the system is checked by changing the duty cycle within/at the boundaries. Thirdly, in reset robustness tests, it is expected to observe system restart, after an unexpected reset occurrence, while the system working under normal condition. Fourthly, glitch filtering is the process of removing unwanted pulses from a digital input signal that is usually high or low. In glitch filter tests, signal changes are controlled to distinguish whether the data is corrupted by glitches, or the filter protected the meaningful data. Finally, in invalid state transition tests, the state transitions of a finite state machine (FSM) is checked to find out if the design could recover from a jump to an unexpected state.

The robustness tests which are mentioned above are performed actively in PLDs of DAL A and DAL B systems of related projects. Throughout these tests, systems' input variables are pushed to their minimum or maximum values to explore edges in the test space. In addition, robustness tests are used in different types of interfaces such as I2C, I2S, SPI, UART, SMI, ARINC429, ARINC708, MIL-STD-1553 to find out how robust these interfaces are. Generally, these tests use SystemVerilog assertions (SVAs) and UVM (Universal Verification Methodology) subscribers as checking mechanisms. If the system works as expected (without any error) between and exceeding

the tolerances, it means the assertion/test is passed. Consequently, operating range and/or problems in the designer's requirements are detected to guarantee the functionality of avionics in all legal conditions and illegal conditions.

II. ROBUSTNESS TEST

RTCA DO-254 is a safety-critical guideline for airborne electronic hardware, which consists of five Design Assurance Levels (DAL) to make flights as safe as possible and to prevent time inefficiencies as well as financial loss. The different DAL levels describe importancy of components for flight safety.

In DAL A avionic systems, failure of the hardware would prevent the aircraft to continue flying safely which would cause a catastrophic result including aircraft crash and many deaths aboard the aircraft. DAL B describes avionic systems that in the event of a failure, a hazardous result, which may include heavy injuries or possible deaths, could occur. DAL C describes hardware whose failure would result in unfavorable flight conditions that could cause injuries. Meanwhile, the failure of a DAL D avionic systems could cause some inconvenience and minor failure conditions. Lastly, DAL E defines electronic hardware, that would have no effect on flight safety under malfunction.

Since, failure of DAL A avionic systems, such as flight control computer, could cause hazardous, irreversible results. Therefore, those systems require robustness tests to be able to examine error conditions and to analyze important edge cases. [1]

Robustness testing has two main goals. One of them is to guarantee that the product functions properly in normal conditions. [2] This includes voltage, clock frequency and data alterations, and so on. The second goal is called negative compliance verification. This verification tests and identifies the hardware design limitations that are outside of the requirements to ensure how the system reacts to abnormal conditions. [2] Expectation in this verification is the system to operate the functions it already has, after any error or unwanted condition occurrence rather than being stuck in an undesired state.

III. ROBUSTNESS TEST TYPES

A. Invalid Access Error Tests

Think of a system receiving incorrect combinations of inputs, toggling inputs that are not listed in the associated requirement or unexpected combinations of inputs, how should the system react? Since there are no requirements to cover this type of situations, it is not known how the system would behave. Hence, even if the system works correctly according to the requirements, for safety critical systems it is necessary to find out if the system continues to work as intended or not while invalid access error takes place.

Invalid access error occurs when trying to write any read only register, read any write only register, reach undefined register address areas etc. via bus such as PCIe. For instance, any read only register is chosen from design's memory map randomly and write data is sent to that register by bus to create invalid access error in verification process, result of that error occurrence is waited. If invalid access error does not occur, the design reliability fails.

B. Clock Robustness Tests

In clock robustness tests, upper and lower tolerances of system clock is controlled with increasing and/or decreasing the system clock frequency. For each clock frequency, the system functionality such as FPGA configuration, data transfers via related interfaces are checked. This process is applied for each interface and system separately until reaching the clock frequency which cause to error occurrence. Additionally, similar method can be used by changing the system clock duty cycle within/at the boundaries and with that, system clock duty cycle tolerances can be found. Hence, the system capability against system clock changes can be observed.

Since the synchronous systems are dependent on clock, it is crucial to know how robust they are to clock changes. So, said systems should be tested to know whether the system works properly while variation of the system clock duty cycle and/or frequency between given tolerances and beyond the tolerances, invalid input timing (e.g., setup and hold violations), and lastly asserting and de-asserting input signals between clock edges given to systems.

C. *Reset Robustness Tests*

In reset robustness test, reset input is applied to the FPGA while the system is working under normal conditions, and all ports and registers are expected to return their default values within certain time, without any error. In addition, it is expected that the system is re-configurated and restarted. If any of the ports or registers are not equal to their reset values or do not carry out in expected time, it means the system is not robust for this condition.

D. *Glitch Filter Tests (Data Disruption Tests)*

Glitches are undesired disruptions, high/low pulses, which usually occur on lines carrying signals. Glitch filters are important to eliminate unwanted glitch pulses on digital input lines. [3] In glitch filters tests, while data transfers are continuing for different interfaces such as I2C, SPI, ARINC429, data ports are driven to disrupt the data transfer temporarily and as a result of that data transfers should maintain correctly. To verify correction of data transfers, subscribers and scoreboards are used.

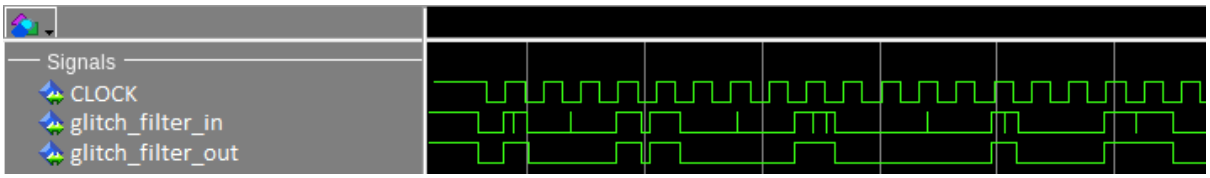

Figure I. Glitch filter operating as expected

In the Figure I. Glitch filter operating as expectedFigure I, it is shown that, the input signal of the glitch filter driven to high and low to corrupt the data, for small amounts of time which glitch filter can catch and eliminate, and observed that the design would filter if such a disruption occurs and outcome of the glitch filter would be as desired.

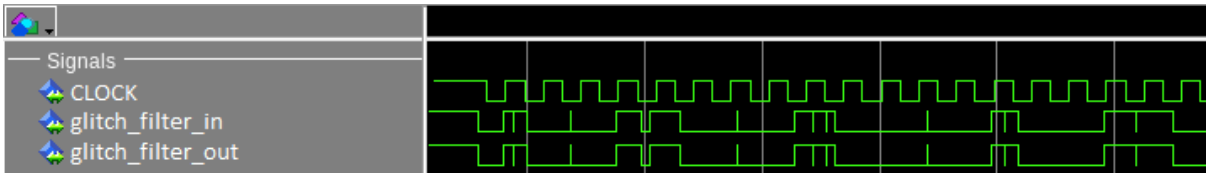

Figure II. Glitch filter not working as intended

On the other hand, Figure II shows that glitch filter would not be able to filter glitches from the data and the output would be as the same as the corrupted input signal, when undesired corruptions occur in the given data.

E. *Invalid State Transition Robustness Tests*

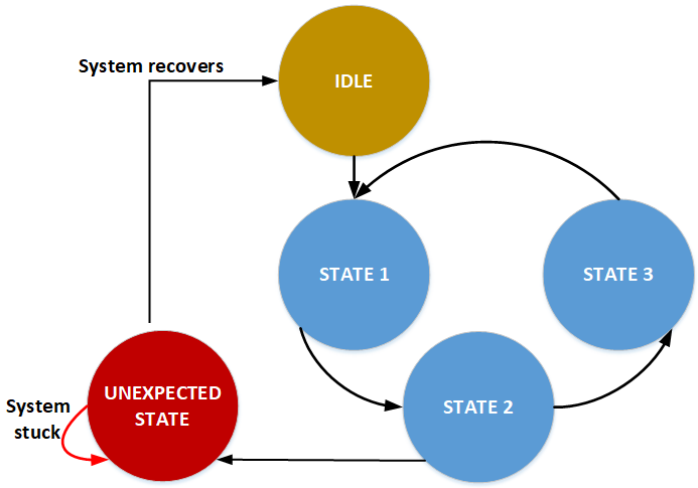

Figure III. Invalid state transition robustness tests block diagram

In invalid state transition robustness tests, finite state machines of the design are checked whether working as expected or not even in the cases that the design is unable to determine the correct way to handle this case. For instance, while testing the finite state machines, as can be seen in the Figure III, the system would be forced to enter an unwanted state rather than the states mentioned in design blocks, and observed to see how the design will handle the case. If the design recovers the unwanted situation gracefully and turns into appropriate state, it means the design is robust enough to handle such a case. If the design stuck forever in the state which is driven by the test but not stated in the design, then it means the system would fail and not operate the cases as intended. On the other hand, finite state machines are not only checked with driving the cases with unexpected states but also, checked whether the state transitions work properly and respectively under normal conditions.

IV. Summary / Conclusion and Feature Work

In conclusion, there are lots of avionic systems in aeronautics which their functionalities are critical for flight safety. These systems should be tested to know how the hardware will take an action under different circumstances which can be stated in requirements or not mentioned by requirements. Robustness tests are the key in both civil aviation and military aviation to prevent catastrophic effects of any crucial avionic systems failure. Hence, several types of robustness methods are performed in simulation to create fault injections by driving the hardware with the conditions at and beyond the given limits by requirements and help designer to make more stable and reliable design after detailed analysis to decide whether the results are reasonable or have potential failure.

References

[1] Brian Butka, Qualification of Tools for Airborne Electronic Hardware, 2013.

[2] Louie de Luna, Robustness Testing for DO-254 Designs, ALDEC The Design Verification Academy.

[3] Cypress Semiconductor Corporation, “PSoC Creator Component Datasheet”, 001-82876 Rev. *A, Revised November 19, 2012.