2024 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE
MUNICH, GERMANY
OCTOBER 15-16, 2024

Functional Safety of a Design Engineer

Darko M. Tomušilović, Vermilion Consulting, Serbia (tomusilovicd@hotmail.com)

***Abstract*—In this extended abstract, I will present challenges that can disturb the functional safety of a design engineer. Furthermore, I will substantiate the claims with a few real-life examples. Finally, I will propose several tips and tricks that can help alleviate the mentioned challenges.**

***Keywords*—design; engineer; test**

I. Extended abstract

The Design Engineer Under Test (DEUT) described in this paper will be its very author. I will provide several fully random stress scenarios that affected me in the past few years, significantly reducing the coverage of previous DVCon events. Despite being highly proficient in Universal Verification Methodology and Portable Stimulus Standard, these examples, accompanied with tips on coping with the scenarios, will contribute much more to the reader than any other materials I could share with them. So, after presenting a Pleiad of DVCon papers discussing subjects like design patterns and register modeling, I am looking forward to this one more than ever due to the circumstances leading to it.

The motivation for writing this paper is the latest in the series of these scenarios, in which, despite spending endless hours developing full-blown ISO26262 compliant verification testbenches, then spending even more endless hours developing an easily traceable safety-driven infrastructure and finally delving into various comprehensive tape-out checklists, I forgot to apply even the most basic sanity checklist on myself. Even though, from the functional standpoint, I know in depth the specifications and potential challenges of a wide range of automotive devices, it turned out that the most safety-critical device in the car was myself, falling asleep while driving and causing a disastrous accident that luckily left only my car with severe consequences.

It cannot be written enough about all the metrics, tools, and Gitlab/Jenkins/Jira/Confluence-based continuous integration flows I encountered during the past several years. Nevertheless, they all primarily address easy things – predictable and boring lines of Verilog / SystemVerilog code. On the other hand, we engineers do not deal with human factors very well. Occasionally, I would get a plain message on my screen telling me to have a break and drink a coffee. However, it feels that much more effort is invested into writing endless guidelines, manuals and booklets explaining how to get the most out of my infotainment system or what to do in a misfortunate case that mud hinders the operation of my rear parking sensors.

In this paper, which by all means will be a technical one, I plan to look at things from a different perspective. I will put into focus other aspects of functional safety, which are being severely neglected when doing our engineering work – aspects like human psychology, our feeling of superiority and invincibility, sense of competition, and sense of machismo, all of which are overly exaggerated when sitting at the car's steering wheel. All these senses are increased even further when an engineer is driving; we are considered intelligent, yet usually stubborn, and trusting all the safety equipment even more than we should.

To summarize, I cannot explain how thankful I am to all the safety engineers who worked on developing my ex-car. My airbags did open, the side windows did close, and my front seat belts did tighten at the moment of the crash. However, on the other hand, there is much improvement to be done in terms of prevention – my car certainly could have done better in detecting that I am tired and encouraging me to rest. I am certainly confident that all the safety equipment would not even be given a chance to prove itself in such a case.