POLYTECHNIC UNIVERSITY OF CATALONIA

MASTER THESIS

SafeDM a light-lockstep approach

Author:
Francisco BAS JALÓN

Supervisor:
Dr. James SMITH

A thesis submitted in fulfillment of the requirements
for the degree of Master's degree in Electronic Engineering

in the

Research Group Name
Department or School Name

May 25, 2022

Declaration of Authorship

I, Francisco BAS JALÓN, declare that this thesis titled, "SafeDM a light-lockstep approach" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

"Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism."

Dave Barry

Polytechnic University of Catalonia

Abstract

Faculty Name
Department or School Name

Master's degree in Electronic Engineering

SafeDM a light-lockstep approach

by Francisco BAS JALÓN

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

Contents

List of Figures

List of Tables

List of Abbreviations

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

Physical Constants

Speed of Light $c_0 = 2.997\,924\,58 \times 10^8\,\mathrm{m\,s^{-1}}$ (exact)

List of Symbols

a	distance	m
P	power	W ($\mathrm{J\,s^{-1}}$)
ω	angular frequency	rad

For/Dedicated to/To my…

Chapter 1

Introduction

1.1 Motivation

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.2 Contribution

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.3 Structure of the Thesis

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

Chapter 2

Background

2.1 Faults, Failures and Errors

During this thesis, the common terminology in fault-tolerant systems add reference is employed:

Faults, failures and errors are abstract concepts that can be applied to different systems. Since the scope of this work is computing systems, we will restrict the provided examples to this kind of systems.

Any electronic system delivers a service that the user of that system perceives. This service comprises all the external states of the system. A service failure or system failure occurs when the delivered service (i.e. one or more external states) deviates from the correct service state. The correct service is defined by the functional specification of the system. A failure in safety-critical systems can endanger lives or produce high economic losses. Thus, the main goal of safety-critical systems is to minimize the probability of a system failure.

The deviation between the correct internal or external state and the real state is called an error. The cause of an error is called a fault. Thus, a fault is a defect within the system. A fault first causes an error in one of the components that form the system, altering the system's internal state. If this error propagates to the system's output altering the external state and the service provided, we will say that the error led the system to a failure. However, not all faults produce errors and not all the errors reach the external estate of the system producing a failure.

For instance, consider a two-inputs AND gate inside a system. If one gate input is '1' and the other is '0', the expected output will also be '0'. In this scenario, a fault that flips the input driving the '0' input to a '1' will produce an error because the output of the gate will be '1' instead of '0'. However, if a fault flips the other input from '1' to '0', the output will still be '0', the expected value.

Following the same logic, an AND gate, whose inputs are driven from two registers, one of them with an incorrect value (error), could correct the error preventing it from spreading to other registers and reaching the output of the system.

Faults can be classified into two main categories: Systematic faults that are related in a deterministic way to a certain cause and are avoidable by construction i.e. taking into account possible faults during the first step of the design or investing enough resources into verification and validation processes (examples....). Random faults that occur unpredictably following a probabilistic distribution and are unavoidable. This work focuses on addressing a method for handling Common Cause Faults (CCF) a especial type of random faults that will be explained later.

2.2 Safety Related Systems

2.3 Fault detection

2.4 Redundancy and Sphere of Replication

2.5 Diversity

2.6 Lockstep execution

2.6.1 Hardware Lockstep Execution

2.6.2 Software Lockstep Execution

2.7 Other Fault detection Approaches

Chapter 3

SafeDE

3.1 SafeDE Motivation

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

3.2 Architecture

3.3 Features and limitations analysis

3.4 N-modular redundancy

3.5 SafeDE Implementantion and Integration

3.5.1 De-RISC Platform

3.5.2 SELENE Platform

3.5.3 Hardware Integration

3.5.4 Configuration and Operation

3.5.5 Software Integration

Sed ullamcorper quam eu nisl interdum at interdum enim egestas. Aliquam placerat justo sed lectus lobortis ut porta nisl porttitor. Vestibulum mi dolor, lacinia molestie gravida at, tempus vitae ligula. Donec eget quam sapien, in viverra eros. Donec pellentesque justo a massa fringilla non vestibulum metus vestibulum. Vestibulum in orci quis felis tempor lacinia. Vivamus ornare ultrices facilisis. Ut hendrerit volutpat vulputate. Morbi condimentum venenatis augue, id porta ipsum vulputate in. Curabitur luctus tempus justo. Vestibulum risus lectus, adipiscing nec condimentum quis, condimentum nec nisl. Aliquam dictum sagittis velit sed iaculis. Morbi tristique augue sit amet nulla pulvinar id facilisis ligula mollis. Nam elit libero, tincidunt ut aliquam at, molestie in quam. Aenean rhoncus vehicula hendrerit.

3.6 SafeDE Evaluation

3.6.1 Functional Validation

3.6.2 Fault Injection

3.6.3 Time Overhead

3.6.4 Hardware Costs

Morbi rutrum odio eget arcu adipiscing sodales. Aenean et purus a est pulvinar pellentesque. Cras in elit neque, quis varius elit. Phasellus fringilla, nibh eu tempus venenatis, dolor elit posuere quam, quis adipiscing urna leo nec orci. Sed nec nulla auctor odio aliquet consequat. Ut nec nulla in ante ullamcorper aliquam at sed dolor. Phasellus fermentum magna in augue gravida cursus. Cras sed pretium lorem. Pellentesque eget ornare odio. Proin accumsan, massa viverra cursus pharetra, ipsum nisi lobortis velit, a malesuada dolor lorem eu neque.

3.7 Conclusions

Chapter 4

Conclusions and Future Work

Appendix A

Published Work

Write your Appendix content here.