UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

MASTER THESIS num. 1981

Software and Hardware Architecture for Redundant Embedded Systems

Dino Šarić

Zagreb, August 2020.

Umjesto ove stranice umetnite izvornik Vašeg rada.
Kako biste uklonili ovu stranicu, obrišite naredbu `\izvornik`*.*

Thanks to my parents for supporting me financially and giving me an opportunity of studying away from home. Thanks to my aunt Dijana and my friends for supporting me emotionally. Thanks to all the helpful current and former students from the college forums. Finnally, thanks to the Youtubers that made understanding the college curriculum much easier.

Contents

List of Figures

Introduction

In a world with increasing number of electronic systems in hazardous environment, the correct operation of active systems is ever more important for ensuring less catastrophes. In year 2000, Air France Concorde flight crashed soon after its take-of killing 113 people, in 2005 Texas City refinery exploded killing 15 people and injuring 180. Similar disasters were the motivation for the creation of functinal safety principles.

Figure 1: Texas refinery disaster

Figure 2: Air France Concorde disaster

Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.[1] In other words, the goal of functional safety is ensuring even when the system fails its response is predictable and safe. Today, the concept of functional safety is part of everyday life and applies to every industry one can think of. For example, functional safety ensures that airbags in a car instantly deploy during impact to protect the passengers. Another good example is an automated flight control system in the airplanes. Autopilot controls pitch and roll of the aircraft changing the heading and altitude, all of which is developed with respect to functional safety parameters, activating alarms and other measures when they are breached.[1]

Motivation of this paper is exploring how are principles of functional safety applied to the engineering projects. Investigate how and why redundancy is implemented in hardware and software. As a part of that, redundant microcontrollers are explored and compared to non-redundant counterparts. Additionally, functional safety additions to FreeRTOS operating system are implemented. Modifications add task replication and a option to measure execution time of tasks. Finally, secure bootloader is added, bootloader has a command shell interface and has option of updating the current application.

The thesis is organized in the following way. Chapter 1 gives brief introduction of functional safety process. Moreover, chapter gives a overview of how is hardware of embedded systems designed to support redundancy. **TODO** what is done to software. Chapter 2 investigates ARM Cortex R microcontroller inner workings and what do they add over Cortex M. Chapter 3 gives overview of added safety functions to the FreeRTOS kernel and gives a brief overview of FreeRTOS's inner workings. Chapter 4 explains how the developed secure bootloader functions and its features.

1. Functional safety in embedded systems

Opis functional safety-a, definicija, proces... **TODO**

HW **TODO**

SW **TODO**

2. Cortex R additions over cortex M

TODO uniti koje imaju pojedine cortex r implementacije **TODO** Sto cortex M ima

3. FreeRTOS functional safety additions

TODO Motivacija, zasto 1oo2D i 2oo3D. **TODO** Opis FreeRTOS-a. **TODO** Motivacija za timed tasks, periodicki taskovi Jeleknovic. **TODO** Opis FreeRTOS-a.

4. Secure bootloader

TODO Koristeni coding standard. **TODO** Kako izgleda flow bootloadera **TODO** Opis vektora u cortex M-u **TODO** Koja stanja ima **TODO** Kako se updatea aplikacija **TODO** Koje funkcije ima **TODO** Persistent memory

5. Conclusion

Zakljucak rada.

Bibliography

[1] Briefing paper: Functional safety essential to overall safety. URL `https://basecamp.iec.ch/download/functional-safety-essential-to-overall-safety/`.

Software and Hardware Architecture for Redundant Embedded Systems

Abstract

Abstract.

Keywords: Keywords.

Programska i sklopovska arhitektura redundantnih ugradbenih računalnih sustava

Sažetak

Sažetak.

Ključne riječi: Ključne riječi, odvojene zarezima.