FH | JOANNEUM
Luftfahrt / Aviation

Bachelor's Thesis

Safety as Service

Service oriented Architectures for safety-critical Systems

Submitted by:	Stefan Lengauer
Registration number:	1210587029
Academic Assessor:	FH-Prog.Dipl.Ing.Dr. Holger Flühr
Date of Submission:	xx August 2015

Declaration of Academic Honesty

I hereby affirm in lieu of an oath that the present bachelor's thesis entitled

"Safety as Service - Service oriented Architectures for safety-critical Systems"

has been written by myself without the use of any other resources than those indicated, quoted and referenced.

Graz, xx August 2015

Stefan LENGAUER,

Preface

This thesis was written as result of the internship at VIRTUAL VEHICLE at Inffeldgasse, Graz from April to July 2015, which was conducted as part of the Degree Programme in Aviation at FH Joanneum in Graz, Austria.

The VIRTUAL VEHICLE research center is an international company, specialized in automotive and rails industry. In total, it has over 200 employees, which are splitted up in four main research areas. For the time of my employment, I worked as part of the Electrics/Electronics (E/E) & Software Area, ... more specificly .. functional safety.

During my employment is was part of the EMC2 project, a European project, ... my part soa

This thesis consists mainly of two documents, which were produced during my internship. The first one is a glossary, which aims at defining certain terms and unifying the opinions from different research areas. The second document, was an extensive investigation on how the service oriented architecture paradigm can be applied in a safety-critical embedded system. In detail, with a vehicle as the system.

Although the employment was oriented towards the automotive industry, the functional safety and fault tolerance concepts, reappear in a very similar way in other engineering disciplines, like aviation. Furthermore, the service oriented approach, which is considered in terms of automotive, will most likely become also an important issue for aviation in near future.

Furthermore, the location of the company at Inffeldgasse was another big advantage, for it allowed the conduction of various courses at the Technical University of Graz, alongside the employment.

At this point I want to thank my supervisor from FH JOANNEUM, FH-Prof. Dipl.Ing. Dr. Holger Flühr, as well as my supervisor provided by the company, Dipl.Ing. Helmut Martin. ...

and also Dipl.Ing.Dr. Andrea Leitner and Mr. Mario Driussi, which helped develop the ideas and concepts featured in this thesis during numerous meetings and discussions.

Contents

Abstract

One of the major issues in the automotive industry is the constant growing complexity of E/E (Electrics/Electronics) systems and the thereof resulting fault propagation due to the strong interconnection of the systems. The area of *functional safety* is concerned with the prevention of non tolerable risks in event of error. This is conducted by identifying possible hazards, estimating the potential risks and developing necessary countermeasures, based on these investigations. The requirement therefore is an accurate and thorough comprehension of the observed E/E system.

The service oriented architecture is a design paradigm, which features the concept of software reuse by implementing functionalities as technology independent and loosely coupled services. Although the design paradigm is already standard for Web applications, it has not yet been applied in safety-critical embedded systems.

Thus, this Bachelor's thesis investigates the applicability of service oriented architectures for such systems, with a focus on *functional safety* and *fault tolerance* context.

The first part of the thesis is mainly a glossy, which defines certain terms, which are critical for the subsequent presented concepts. On this basis it is defined what *safety as a service* can mean in general, and how the actual implementation in a given safety-critical system may look like, in order to meant with the requirements specified in the ISO 26262 standard. This is the safety standard for safety-critical E/E systems in vehicles with a maximum gross weight of 3500 kg.

Kurzfassung

List of Figures

List of Tables

List of Abbreviations

Chapter 1

Introduction

Due to the very different comprehension of certain terms by different people from different fields of research The first part of my work during the internship was the creation of a glossary describing certain given terms ... in order to unify the understanding of these terms and create a basis for discussions ans researches.

- The glossary was later taken as standard for this tasks ... - and deals with the terms: *service*, *system*, *system of systems*, *architecture*, *service-oriented architecture*, *configuration*, *static reconfiguration*, *dynamic reconfiguration*, *inter-core communication*, *intra-core communication* and *binding*. The most important parts of this glossary will be covered within this chapter. - furthermore a database with the used literature was created in order to provide the necessary references for the glossary and provide a ... where to find further information for the employees.

- disambiguity safety and security - what is safety and fault tolerance

1.1 Related instances

1.1.1 ISO 262662 international standard

1.1.2 MISRA

1.1.3 AUTOSAR

1.2 service

1.3 System

1.4 Component

1.5 Service

1.6 Architecture

1.7 Service oriented Architecture

1.7.1 Definition

1.7.2 Historic Development

1.7.3 Structure of SoA

1.7.4 Service Composition

1.8 Communication in SoA

1.9 Dependability

1.9.1 Reliability

1.9.2 Availability

1.10 Functional Safety

1.10.1 Safety related terminology

Chapter 2

Methods

2.1 SoA in Embedded Systems (Embedded SoA)

2.1.1 Correlation of design philosophies

2.1.2 Difference between Web SoA and Embedded SoA

2.1.3 εSoA

2.1.4 SoA in automotive

Location of the service repository service contract

2.2 Safety services

2.2.1 Fault detection service

2.2.2 Error detection service

2.2.3 Memory Protection Service

2.3 Use Case: Error Detection Service

2.3.1 Service Investigation/Planning

2.3.2 Service inventory analysis

2.3.3 Service oriented analysis

2.3.4 Service oriented design

Chapter 3

Results

Chapter 4

Discussion

Chapter 5

Conclusion

- still a long time until real application + many advantages of the soa paradigm - vermarkung von soa schwierig -¿ was ist der vorteil von auto mit soa + wsl unvermeidbar für selbstfahrende fahrzeuge und etc. - das problem ist safety critical ...