A Design Process and Certification Strategy for Autonomous Vehicles

by

Michael Sebastian Schmid

B. Eng., Augsburg University of Applied Sciences (2016)

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

Master of Science in Aeronautics and Astronautics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2020

Author .....
Department of Aeronautics and Astronautics
October 13, 2019

Certified by .....
Nancy G. Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by .....
Sertac Karaman
Chairman of the Graduate Program

A Design Process and Certification Strategy for Autonomous Vehicles

by

Michael Sebastian Schmid

Submitted to the Department of Aeronautics and Astronautics
on October 13, 2019, in partial fulfillment of the
requirements for the degree of
Master of Science in Aeronautics and Astronautics

Abstract

Autonomous vehicles have long been predicted to disrupt the transportation industry in the near future. Although numerous companies have shared that optimism and supported development it now seems that the challenges of building autonomous vehicles are becoming apparent and are pushing the vision far into the future. Autonomous vehicles, like most of today's systems, are characterized by the central role of software and their high complexity. As a result, the nature of accidents has changed and many accidents today are related to interactions between system components (hardware, software, and humans) rather than component failures. However, state of the art engineering processes do not provide enough support to design autonomous vehicles effectively. The currently used V-model, for example, requires designers to jump from requirements generation to a fairly detailed system architecture and hence, compromises system design. In order to deal with complexity more effectively architecture selection must be tied more closely to requirement generation and emergent properties such as safety, security, maintainability, etc. need to be designed into the system from the beginning. In the scope of this thesis a new approach to the engineering of autonomous vehicles (including design and certification) is suggested. First, gaps in the standard practices for the design and certification of autonomous vehicles are identified and a set of requirements for the engineering of autonomous vehicles is derived. Second, the standard practices are extended to a design and certification process that covers the new set of requirements. Finally, the process will be demonstrated by using it to create a conceptual architecture for autonomous vehicles.

Thesis Supervisor: Nancy G. Leveson
Title: Professor of Aeronautics and Astronautics

Acknowledgments

- Nancy Leveson:
- John Thomas:
- Lawrence Wong and Dylan Muramoto:
- Diogo Castilho:
- Beata Shuster:
- Bettina Deponte
- Martina, Verena, Gerhard Schmid
- Sandra Pjanic:
- Martin Otcinscki:
- Celina Boesl:
- Gertrud and Siegfried Schmid:
- Laura Roesch:
- Evelyn Taylor-McGregor
- Ingrid Mosquera
- many other significant family members and friends:

Contents

List of Figures

List of Tables

Nomenclature

Acronyms

ATA	Air Traffic Association
AV	Autonomous Vehicle

Number Sets

$\mathbb{C}$	Complex Numbers
$\mathbb{R}$	Real Numbers

Other Symbols

ρ	Friction Index
V	Constant Volume

Physics Constants

c	Speed of light in a vacuum inertial system
g	Gravitational Constant
h	Plank Constant

Chapter 1

Introduction

[Optimists see various benefits in AVs, most importantly higher safety]

[However, doubt about whether AVs will actually bring all those benefits. Scepticism points to whether AVs will actually be safer than human drivers or at least sufficiently safe?]

[It is unclear how we can design AVs effectively so that our society can benefit from them]

- different approach to safety
- new design process

This chapter outlines the gaps in the state-of-the-art processes for the design and certification of autonomous vehicles and argues for a new approach that ties safety, design, and certification together much more closely. First, the motivation for a safety-driven design process is given in section 1.1. Then, in section 1.2, the research objectives of this thesis are outlined.

1.1 Motivation for a Safety-Driven Design Process

[Today's systems and AVs show increased complexity and present new challenges]

- trend to more features and functionality

- trend to more complexity (lines of code, e.g. AV vs. fighter jet)
- complexity poses additional challenges

[Traditional tools insufficient to address the challenges of today's systems challenges]
- safety: focus of current methods on reliability rather than safety
- design approaches: safety considered too late in the design process and therefore limited impact
- ultimately: certification leaves gap of requirement correctness and completeness

[new approach to the design and certification of AVs is needed]

1.2 Research Objectives

[Insufficient design and certification call for a new approach]
- how should our design process be shaped to effectively design AVs?
- how can we AVs be certified?

1.3 Overview of Chapters

[Outline the chapters]

Chapter 2

Literature Review: Standard Engineering Practices and Gaps

This chapter provides a literature review based on which a set of requirements for the design of autonomous vehicles is generated. First, section 2.1 provides an overview on general principles for the design of highly complex systems. Second, section 2.2.2 reviews accidents involving autonomous vehicles for common factors. Then, in section 2.3 the principles and identified common factors are used to generate a set of design process requirements for autonomous vehicles.

2.1 Design and Certification in Automotive: Processes and Standards

[A framework of standards exists within which each covers a different aspect in the Engineering Process]

2.1.1 ISO 26262: Road vehicles – Functional safety

[Description of the standard]

2.1.2 SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

[Description of the standard]

2.1.3 ISO 21448: Safety of the Intended Functionality

[Description of the standard]

2.2 Limitations of the Currently Used Processes, Standards, and Methods

[The state of the art in the engineering of highly-complex systems such as autonomous vehicles insufficiently integrates safety into the design, covers safety only partially, and ultimately provides insufficient guidance during the development process]

2.2.1 Gaps to Principles for the Engineering of Complex Systems

[Methods inadequate: More software and complexity require a non-failure based approach to safety]

[Safety is addressed most effectively when designed into the system early in the design process]

[Standards provide insufficient coverage of the safety problem]
- show coverage graphics
- safety is an emergent systems property rather than a reliability problem

[Popularity of the problem has led to many suggestions, a majority of them based off old techniques]

[A new approach beyond suggestions based off old methods is needed (reference to alternative methods)]

2.2.2 Flaws revealed by Accidents involving Autonomous Vehicles

[Accidents have operators be legally liable but point to gaps in design and therefore can be learned from]

[Each of the following subsections first gives a brief description of the accident and concludes with a set of identified causal factors]

2016-01-20 (China)

Accident Description

[...]

Identification of Causal Factors

[...]

2018-01-22 (California)

Accident Description

[...]

Identification of Causal Factors

[...]

2018-03-18 (Arizona)

Accident Description

[...]

Identification of Causal Factors

[...]

2018-03-23 (California)

Accident Description

[...]

Identification of Causal Factors

[...]

2018-06 (Newfoundland)

Accident Description

[...]

Identification of Causal Factors

[...]

2019-05-07 (Florida)

Accident Description

[...]

Identification of Causal Factors

[...]

Summary of Common Factors in Accidents Involving Autonomous Vehicles

[...]

2.3 Summary of Design Process Requirements for Autonomous Vehicles

[create set of autonomous vehicle design process requirements]

Chapter 3

Formulation of a Safety-Driven Engineering Process

In this chapter the requirements identified in Chapter 2 are used to formulate a safety-driven design process for autonomous vehicles. First, Section 2.1 presents state-of-the-art processes used in the design and certification of autonomous vehicles. Second, Section 3.1.1 introduces Systems-Theoretic-Process-Analysis (STPA) and outlines the benefits for a more effective design process. Finally, in Section 3.3 the state-of-the-art and STPA are composed into a safety-driven design process that draws on STPA from an early stage.

3.1 Methodological Extension of the Engineering Process

[Methods described in Chapter 2 insufficiently cover safety and leave gaps in engineering process: STPA provides a methodological extension]

3.1.1 Systems Theoretic Process Analysis and Key Benefits

[What is STPA?]

[Advantages and Strengths of STPA]

[Benefits of STPA for highly-complex systems such as automotive]

3.1.2 Improved Safety Coverage by Combination of Techniques

[...]

3.2 Structural Improvement of the Engineering Process

[The Engineering process needs to leverage safety early to drive high-level decisions (e.g. architecture selection) and generate knowledge for the next design steps (i.e. in the form of a set of requirements)]

3.2.1 Integration of Safety into Early Engineering Activities

[...]

3.2.2 Linking Design Iterations by Requirement Generation

[...]

3.3 Synthesis of a Safety-Driven Engineering Process

[Describe the overall process: Unite V-model]

- show process graphic
- elaborate on the steps

[Process extends to certification: Certification against conceptual architecture]

- identify baseline ideas that enforce basic safety constraints (that always apply).
- mention: even certification of online learning approaches may be possible

Chapter 4

Process Validation: Derivation of a Conceptual Architecture

In this chapter the process formulated in Chapter 3 is used to derive a conceptual architecture for autonomous vehicles. In Section 4.1 safety requirements are identified by following the steps from Section 3.3. Then, in Section 4.2 the generated requirements are used to adapt the control structure and derive a conceptual architecture for autonomous vehicles.

4.1 Identification of Safety Requirements

[In this section STPA will be applied to the generic control structure defined in the previous section]

4.1.1 Step 1: Define Purpose of Analysis

[...]

4.1.2 Step 2: Define Control Structure

[core modules of an autonomous vehicle and their relationship (provide a few reference examples)]

[control actions and functionality of the different components > control responsibilities]

[control-theoretic abstraction comprises these relationships and functionalities]

4.1.3 Step 3: Identify UCAs & Requirements

[Exemplarily identify UCAs]

[Exemplarily derive requirements]

4.1.4 Step 4: Identify Scenarios & Requirements

[Exemplarily identify scenarios]

[Exemplarily derive requirements]

4.2 Synthesis of a Conceptual Architecture for Autonomous Vehicles

[Analyze the safety requirements and derive architectural artifacts (let them drive the design, identify measures)]

[Adapt the control structure so that the safety requirements are satisfied (Conceptual Architecture)]

Chapter 5

Summary

This thesis has suggested a new approach to the design and certification of autonomous vehicles. The motivation for a novel approach to the design and certification of autonomous vehicles was demonstrated in Chapter 1. In Chapter 2 the state-of-the-art processes in the design and certification of autonomous vehicles was presented and requirements for a more effective design process were generated. Based on these requirement a safety-driven design process was developed in Chapter 3. The application of this process to the design of autonomous vehicles was demonstrated in Chapter 4.1 and a conceptual architecture was derived. In the following sections first the research contribution of this thesis is summarized in Section 5.1 and then an outlook on future contributions to extend this work is provided in Section 5.2.

5.1 Research Contribution

[Research Question 1 was answered by integrating ISO 26262, ISO 21448, ISO 21434 and STPA into one process]

[Research Question 2 was answered by deriving a conceptual architecture that can be used for certification]

5.2 Future Work

[Include safety not only in the design process but in the overall life cycle]

- Accident analysis based on CAST using the STPA design information would help to further cover unknown unknowns

- Collecting data from vehicle in field and feed into an Active STPA (reference to Diogo)

Appendix A

Figures

Figure A-1: Example picture 1.

Figure A-2: Example picture 2.

Appendix B

Tables

Table B.1: Example table.

This	is
an	example

Bibliography