Dependability Analysis of Two Candidate Architectures for a Brake-By-Wire System

Laboratory report in
EDA122 Fault-Tolerant Computer Systems

Dan Larsson
Jonas Hemlin
Group Lab Class Thursday 17-21 C

Chalmers University of Technology
Gothenburg, Sweden 2012
Version no.: 0.0

October 27, 2014

Contents

1 Introduction **3**

2 Overview of the Candidate Architecture **4**
2.1 Centralized Architecture 4
2.2 Distributed Architecture 4
2.3 Modes of Operation 4
2.3.1 Full Functionality 4
2.3.2 Degraded Functionality 4
2.4 Assumptions and modeling parameters 4

3 Description of Models **6**
3.1 Wheel Unit Model 6
3.2 Wheel Unit Subsystem Model 6
3.3 Central Unit (CU) 7
3.3.1 Distributed Duplex Architecture 7
3.3.2 Centralized Triplex Architecture 8
3.4 System Model 9
3.4.1 Centralized Architecture 9
3.4.2 Distributed Architecture 9

4 Results **10**

5 Discussion **11**

6 Conclusions **12**

References **13**

1 Introduction

/This section shall introduce the reader to the subject addressed by the report. It should include i) a brief explanation of how a brake-by-wire system works and its main advantages and drawbacks compared to existing brake systems, and ii) a description of the purpose of the report, i.e., a formulation of the problem to which the report provides an answer. The last paragraph should consist of a roadmap of the report./

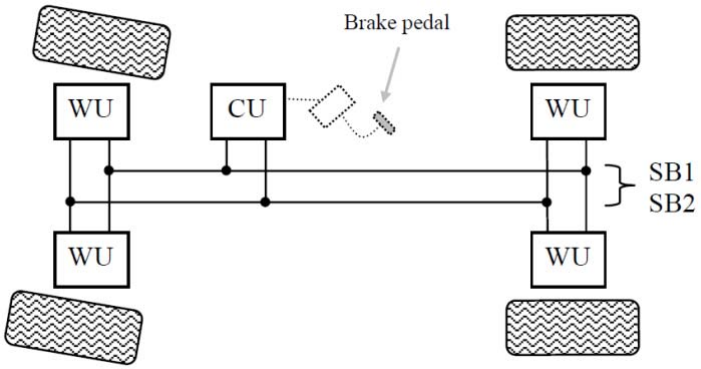

Figure 1: Brake-by-wire system

2 Overview of the Candidate Architecture

This section shall describe the centralized and distributed architectures, and the two modes of operation (full functionality and degraded functionality). It should also describe the modelling assumptions, including the model parameters.

2.1 Centralized Architecture

/text/

2.2 Distributed Architecture

Cite the reference list shall be formatted as the reference list in this document. For an example of how to write references, see Kopetz and Bauer [1]. (This paper is part of the course literature and is published by the Institute of Electrical and Electronics Engineers, Inc, known as IEEE, and therefore follows the IEEE format for scientific journal papers. Other publishers use slightly different formats.)[1]

2.3 Modes of Operation

In this section you describe the two modes of operation of the system; full functionality and degraded functionality.

2.3.1 Full Functionality

/text/

2.3.2 Degraded Functionality

/text/

2.4 Assumptions and modeling parameters

/text/

Subsystem	Part	Failure rate	Coverage
System bus	Serial bus	FailureRate	1
Wheel unit	Computer module	FailureRate	1
Wheel unit	Sensor	FailureRate	1
Wheel unit	Actuator	FailureRate	1
Central unit	Computer module	FailureRate	0.99

Table 1: Failure rates and coverage factors for the distributed architecture

Subsystem	Part	Failure rate	Coverage
System bus	Serial bus	FailureRate	1
Wheel unit	Computer module	FailureRate	1
Wheel unit	Sensor	FailureRate	1
Wheel unit	Actuator	FailureRate	1
Central unit	Computer module	FailureRate	First CM failure:1 Second CM failure: 0.99

Table 2: Failure rates and coverage factors for the Centralized Architecture

3 Description of Models

This section shall describe your models for the different subsystems for the two architectures and the two levels of functionality. Figures should be explained in the text.

3.1 Wheel Unit Model

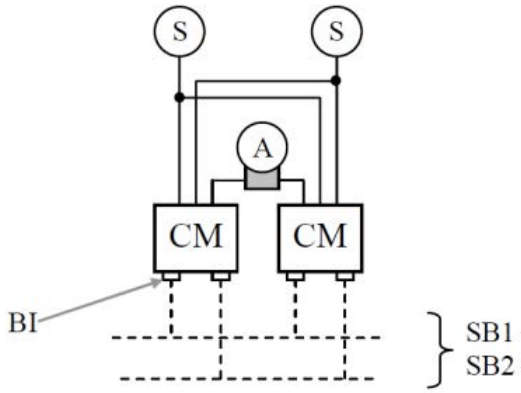

Figure 2: Wheel Unit

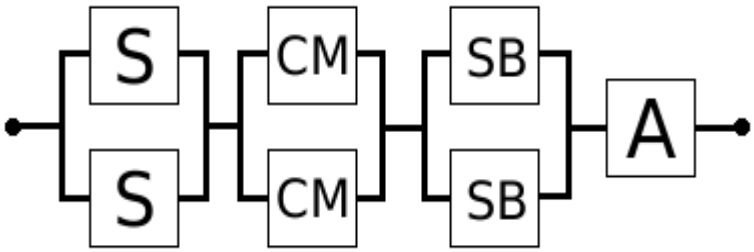

Figure 3: Reliability block diagram of the wheel unit

3.2 Wheel Unit Subsystem Model

/text/

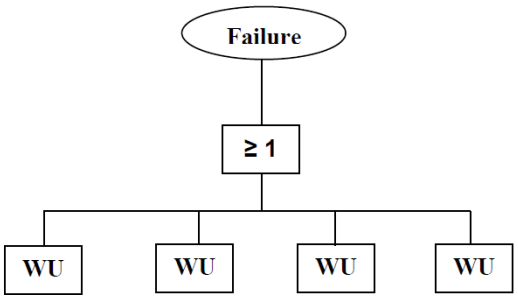

Figure 4: Fault tree for the Wheel Unit Subsystem, full functionality

Figure 5: Fault tree for the Wheel Unit Subsystem, degraded functionality

3.3 Central Unit (CU)

3.3.1 Distributed Duplex Architecture

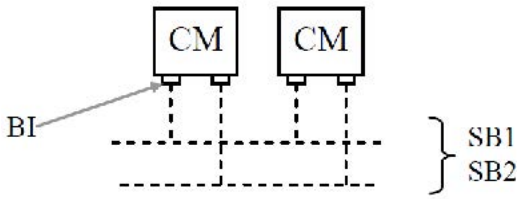

Figure 6: Central Unit, duplex configuration

Figure 7: Reliability block diagram for the Central Unit, duplex configuration

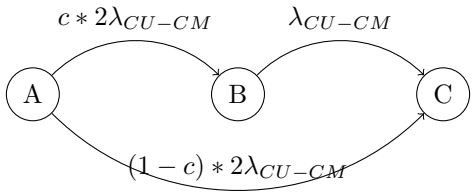

Figure 8: Markov chain model

3.3.2 Centralized Triplex Architecture

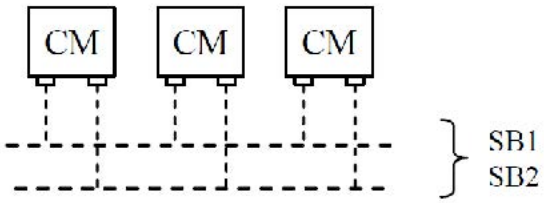

Figure 9: Central Unit, triplex configuration

/Reliability block diagram for , Figure 10. Make sure the caption number is correct./
/Markov model for , Figure 11./

Figure 10: Caption

Figure 11: Caption

3.4 System Model

3.4.1 Centralized Architecture

Figure 12: Fault tree for Full Functionality

Figure 13: Fault tree for Degraded Functionality

3.4.2 Distributed Architecture

Figure 14: Fault tree for Full Functionality

Figure 15: Fault tree for Degraded Functionality

4 Results

/Describe the results. Graphs and tables shall be commented in text. To facilitate the comparison of the results for different design solutions, include several reliability graphs in one diagram./

Units	Distributed	Centralized
Wheel Unit Subsystem Full Functionality	Reliability= MTTF=	Reliability= MTTF=
Wheel Unit Subsystem Degraded Functionality	Reliability= MTTF=	Reliability= MTTF=
Central Unit	Reliability= MTTF=	Reliability= MTTF=
Entire System Full Functionality	Reliability= MTTF=	Reliability= MTTF=
Entire System Degraded Functionality	Reliability= MTTF=	Reliability= MTTF=

Table 3: Reliability and MTTF results

/Insert Reliability Graphs and comment them in the text. Make sure that the caption numbers are correct./

5 Discussion

/Discuss the pros and cons of the different design solutions. /

6 Conclusions

/Present your conclusions and recommendations./

References

[1] Leslie Lamport, *LaTeX: A Document Preparation System*. Addison Wesley, Massachusetts, 2nd Edition, 1994.

Please use Vancouver/IEEE style for your referencing. For more information please check: http://www.lib.unimelb.edu.au/cite/ieee/index.html
The reference list shall be formatted as the reference list in this document. For an example of how to write references, see Kopetz and Bauer [1]. (This paper is part of the course literature and is published by the Institute of Electrical and Electronics Engineers, Inc, known as IEEE, and therefore follows the IEEE format for scientific journal papers. Other publishers use slightly different formats.)