

Active System Control



Igor Schagaev • Brian Robinson Kirk

Active System Control

Design of System Resilience

 Springer

Igor Schagaev
Director
IT-ACS Ltd
Stevenage SG1 1RR
Hertfordshire, UK

Brian Robinson Kirk
Research Director
Robinson Systems Engineering Ltd
Painswick GL6 6QJ
Gloucestershire, UK

ISBN 978-3-319-46812-9 ISBN 978-3-319-46813-6 (eBook)
DOI 10.1007/978-3-319-46813-6

Library of Congress Control Number: 2017945950

© Springer International Publishing AG 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

We used the word *active* in the title of our book, *Active System Control*, because we are actively trying to predict the future behaviour of the system, and react accordingly in order to manage the safety and continue the operation of the system being controlled.

We used the word *system* because we create a model of a system, based on an aggregate of models of its elements. It is used to try to predict the parameters of the system's behaviour.

We use the word *control* because we continually monitor the current situation and adapt the control of the system to make the best of the circumstances.

Therefore, *Active System Control* is the right title, and the abbreviation ASC will be used in the text.

In this book we briefly analyse what is required from on-board devices in order to support active system control, that is, what must be done to sustain everyday safe operation and summarise the requirements for this class of devices.

We also introduce the new concept of a safety device—the “active black box”—which might be used for aviation, transport, and nuclear and chemical plants. In the coming age of “driverless” transport, it is particularly relevant to the automotive sector to monitor the behaviour of semi-autonomous and fully autonomous vehicles carrying passengers.

Separately, and briefly, we describe the regulations in transport segments relevant to the application of existing and proposed devices. We start with an analysis of air transport because this is a well-established and reasonably well-understood domain with a relatively mature safety culture.

Stevenage, UK
Painswick, UK

Igor Schagaev
Brian Robinson Kirk

Acknowledgements

This book includes efforts from quite a number of people. Dr. Felix Friedrich, ETH (Zurich), Dr. Florian Negele and Dr. Thomas Kaegi were involved in the development of flight mode algorithms, as well as the system architecture and design required to implement the concept of active system control in the general aviation aircraft application domain.

Engineer Alex Schagaev (IT-ACS LTD) developed and tested various flight scenarios to detect conditions of flight mode changes, and verified flight mode changes using two flight simulators—X-plane and Microsoft—in preparation for field trials using general aviation aircraft. This enabled us to improve our understanding of the conditions for flight mode changes, which were not known before, and to refine the flight mode model.

Several consultants from the areas of aircraft design, testing and simulations were invited and contributed in various chapters: Dr. S. Plyaskota was fully involved in the development of the classification of aviation and analysis of the market domains. His efforts are highly regarded and appreciated. Dr. V Bukov consulted in the “algebraic” description of our graph logic model (GLM) representation. Along with his colleagues, he was involved in modelling and simulating the trial aircraft air pressure system.

Dr. Kai Goebel (NASA) made contributions to the prognostic aspects of our approach and the role of active system control in the whole book, especially in Chap. 10.

We sincerely appreciate help of our colleagues and friends and offer our heartfelt thanks.

Contents

1	Aviation: Landscape, Classification, Risk Data	1
	Introduction	1
	Survey of the Aviation Application Domain	4
	Terminology	4
	Classification of Aviation	5
	The Aircraft Market	13
	Safety and Risk of Flight	24
	Aviation Safety in Commercial Aviation	24
	Main Risk Agents and Their Contribution	26
	Risk Factors and Flight Phases	27
	Risk and Safety in General Aviation	30
	Accident Statistics	30
	Flight Risk Analysis	34
	First Occurrences and Sequence of Events	35
	Causes and Factors of Accidents	36
	Conclusion	37
	Safety Management Scheme	38
	Insurance, Regulation and Aviation Safety	39
	Flight Safety and Safety Control Cycles in Aviation	40
	Constraints and Failures of Safety Management	41
	Conclusions	42
	References	44
2	Active System Control and Safety Approach, and Regulation in Other Application Domains	45
	Approach to Safety in Critical Systems	45
	Safety Approach in Industrial Systems and Machinery	46
	Approach to Safety in Process Plants	46
	Approach to Safety in Small Industrial Systems	47

Safety Approach in the Automotive Industry	49
Current On-Board Safety Systems	49
Physical Safety Systems	49
Route Safety Systems	49
Driving Safety Systems	50
Driver Safety Assurance	50
Safety Improvement	50
Operational Safety Cycle	51
Future Safety Systems in the Automotive Industry	53
Safety Approach in the Rail Industry	54
Current On-Board Safety Systems	54
Physical Safety Systems	55
Route Safety Systems	55
Driving Safety Systems	56
Driver Safety Assurance	56
Safety Improvement	57
Operational Safety Cycle	57
Future Safety Systems in the Rail Domain	59
Safety Approach in the Space Domain	60
Existing Standardisation	62
Standards in the Industrial Domain	62
Safety Definitions of IEC 61508	62
Functional Safety Analysis	63
Standards in the Rail Domain	64
The Safety Case	64
Development Life-Cycle for Safety-Related Systems	65
Safety Integrity Levels (SILs)	65
Standards in the Space Domain	66
Conclusions	68
Functional Safety Standards Based Upon IEC 61508	69
References	70
3 Aircraft Flight Reliability and the Safety Landscape	
of Aircraft Use	73
Introduction	73
An Operational Reliability Model for Aircraft	74
Reliability Model of a Flight	75
Operational Reliability Model: Equations	76
Measures of System Reliability	78
The Safety Maintenance Landscape	80
Developments in Modern Aviation and Safety	80
Developments in Risk	82
Chain Mode Flights	83
Latency of Fault and Safety Monitoring	84

The Safety Maintenance Landscape: Commercial Aviation	86
On-Ground Management of Safety	87
Timing for Safety Management between Flights	89
Social, Political and Commercial Aspects of Aviation Safety	90
Flight Safety Versus Risk and Statistics:	
Flight Data Paradox	92
Risk and Statistics	94
External and Internal Aspects of Aircraft Safety	94
Conclusion	96
References	97
4 Active Safety Relative to Existing Devices	99
Active System Control and System Safety Versus Aircraft Management	99
Safety Tools and Supportive Devices	101
Safety Devices: Brief History and Evolution	101
Existing Flight Data Recording Devices	105
Military Flight Data Recording Devices and Testing Recorders	106
Requirements for New Flight Data Recording and Processing System	109
Flight Data Processing System Post-flight Analysis	110
Constraints	112
The Nature of Devices for Future Aircraft	114
Conclusion	117
References	118
5 Principle of Active System Control (Theory)	121
Introduction	121
The Goals, Role and Structure of the Chapter	121
Active System Control Overview	123
Defining and Implementing the PASC	126
Structure of Research of Active System Control	128
Principle of Active System Control	129
Factors to Take into Account Making Active System Control Work	129
Definition of the PASC	131
PASC and Elements of Redundancy Theory	134
The PASC Algorithm in More Detail	137
PASC: Dependability and Fault Tolerance	139

Improving the Control and Safety of a System	140
A Generalised Information Model for Active System Control	143
On Coverage	146
Conclusion	147
References	148
6 Principle of Active System Control:	
Aspects of Implementation	149
Introduction	149
Implementation of PASC in-the-Medium	149
The PASC for General Aviation:	
The Cycle of Operational Management	150
Process-Oriented Informational Model	152
Conclusion	184
References	188
7 Active System Control: And Its Impact on Mission Reliability	189
Reasoning	189
Preventive and Conditional Maintenance Versus	
Active System Control: A Semantic Difference	191
Reliability Gains: Conditional Maintenance Versus Active System	
Control	193
Preventive Maintenance with Implementation	
of Active System Control	197
The Real-Time Reliability Corridor:	
Introduction and Definitions	200
Conditional Maintenance Versus Active System Control	205
Summary and Conclusions	206
References	207
8 Flight Mode Concept and Realisation	209
Introduction	209
Goals and Objectives of the Chapter	210
The Objectives of Implementation	212
The Flight Mode Model	213
Flight Mode Definitions	213
The Flight Mode Detection Algorithms	217
Visualisation of Flight Mode	220
Presentation of Advice to the Flight Crew	220
Information Processing of Flight Data Including	
Flight Mode	221
Flight Mode Detector	223
Real-Time Diagnosis and Prognosis	223
Determination of Response	223
Configurability of the System	224

- A Trial Architecture for Flight Mode Detection 224
 - The Avionics System: System Block Diagram 225
 - Flight Data Memory 226
 - Software Architecture and Partitioning 227
- Using Flight Modes to Tune Flight Performance and Safety 229
- Conclusions 231
- Further Steps 231
- Appendix: Flight Mode Model: XML Specification 232
- References 239
- 9 Active System Control: Realisation 241**
 - Introduction: The Safety Aspects of Active System Control 241
 - Objectives of the Chapter 242
 - The Active System Control for Safety: Theoretical Model 242
 - Fault Detection and Handling: Algorithms and Procedures 243
 - The Theory: Based on Applied Graph Logic 244
 - The Algorithms of Fault Localisation 253
 - The Application Example: Air Pressure System 256
 - Summary and Conclusion 265
 - References 266
- 10 Active System Control: Future 269**
 - Igor Schagaev, Brian Robinson Kirk, and Kai Goebel
 - Introduction 269
 - Classification of Aircraft: Reiterated 270
 - What Else Can Active System Control Do? 272
 - Active System Control: Life-Cycle of Design and Manufacturing 273
 - Active System Control: Life-Cycle of Aircraft Application 273
 - Active System Control: Risk Information Paradox: RIP? 276
 - Active System Control in Almost One Page, “During” and “After” 278
 - Active System Control Dependency Matrixes: Who Is Doing What 279
 - The Impact of Prognostics on Active System Control 282
 - Embedding Active System Control into Aircraft 283
 - Software Organisation of Active System Control 284
 - Active System Control Essential Device: Active Black Box 286
 - Summary and Conclusion 287
 - References 288
- Index 291**

Author Biographies



Professor Igor Schagaev is the Director of IT-ACS Ltd. Stevenage, UK. He received his Ph.D. in Computer Science in 1983 from the Russian Academy of Sciences, Institute of Problem of Control; Certificate in Business Organization of International Research Program Management, TACIS (EC) 1996; Certificate in Learning and Teaching in Higher Education, University of North London 2001. He has been Fellow of the Institute of Analysts and Programmers (UK) since 1992 and Fellow of British Computer Society since

2013. Igor has previously worked as an Electromechanical Engineer at the Smolensk aviation factory, USSR; a Senior Programmer and Design Engineer at the Institute of Advanced Computations, Central Statistical Bureau of USSR; and as Head of the Fault-Tolerant System Branch at the Institute of Control Sciences. The latter was combined with work as Senior Design Engineer and System Programmer for Avionics at Sukhoi Design Bureau. Since 1992, Igor has been Director of ATLAB Ltd. Bristol (now converged into IT-ACS Ltd.). Since 1983, Igor has published internationally 70+ papers in journals and conferences, and seven books. Igor has been a keynote speaker at world conferences in the UK, China and the USA, and has provided consultancy for the *Financial Times*, *Sunday Times*, Boston Facultimedia and Swedish government, all on the subject of ICT, avionics and aerospace domains. Igor has been honoured with several industry awards, achievements and grants. He is author of the Springer titles: V Castano and I Schagaev, *Resilient Computer System Design*; and Schagaev I, Kaegi T, *Software Design for Resilient Computer Systems*. Since 2007, together with Dr. Brian Kirk and Alex Schagaev, Igor has held a patent on the Method and Apparatus for Active System Safety, GB 2448351.



Dr. Brian Robinson Kirk is the founder and Director of Robinson Systems Engineering Ltd. in the UK, which has specialised in designing and building safety-related computing and control systems for over 40 years. He received his Ph.D. in Methods of Active System Safety in 2007, formerly attaining an M.Sc. in Industrial Electronics from Imperial College and a B.-Sc. (Hons) in Electronics from Salford University in the 1960s. He worked on early graphics-based CAD and simulators for microchip design with Marconi

Research Labs. In the 1970s, he worked as design manager for microprocessors and memories at General Instrument Corp. There, he worked on custom IC design and early 1-, 4-, 8- and 16-bit processors, including the PIC series, the Sinclair calculators and early TV games (such as Pong). After working for Mergenthaler Linotype on system designs during the phototypesetting revolution, he founded Robinson Systems Engineering Ltd. He has presented many papers linking theory to practical applications at conferences around the world and collaborated with Professors' Wirth and Gutknecht's group at ETH Zurich for over 20 years, co-authoring the Zonnon Language Report. As joint author of the book *Programming Oberon in Windows*, he released Robinson's Oberon compiler for Windows as part of the Programmers Oberon Workbench as freeware, inspired by the usability and ubiquity of Borland Pascal. More recently he has provided technical advice to US legal teams on the causes of sudden unintended acceleration in vehicles that contributed to a billion-dollar settlement in a single case and contributed to Tom Murray's book *Deadly by Design*. As a Chartered Engineer he is currently working with the Institute of Engineering and Technology (UK) and IEEE (USA) on guidance for improving the Electromagnetic Resilience of Systems. He is a member of the British Computer Society, Institute of Directors, and a life member of the ACM (USA) and the International Society of Bassists, being an enthusiastic double-bass player in various jazz bands.