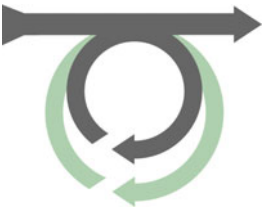
Active System Control



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

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 — Igor Schagaev
Painswick, UK — 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 fight 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.

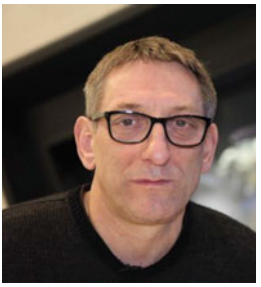
Several consultants from the areas of aircraft design, testing and simulations were invited and contributed in various chapters: Dr. S. Plyaskota was fully involved in the development of the classification of aviation and analysis of the market domains. His efforts are highly regarded and appreciated. 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

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.