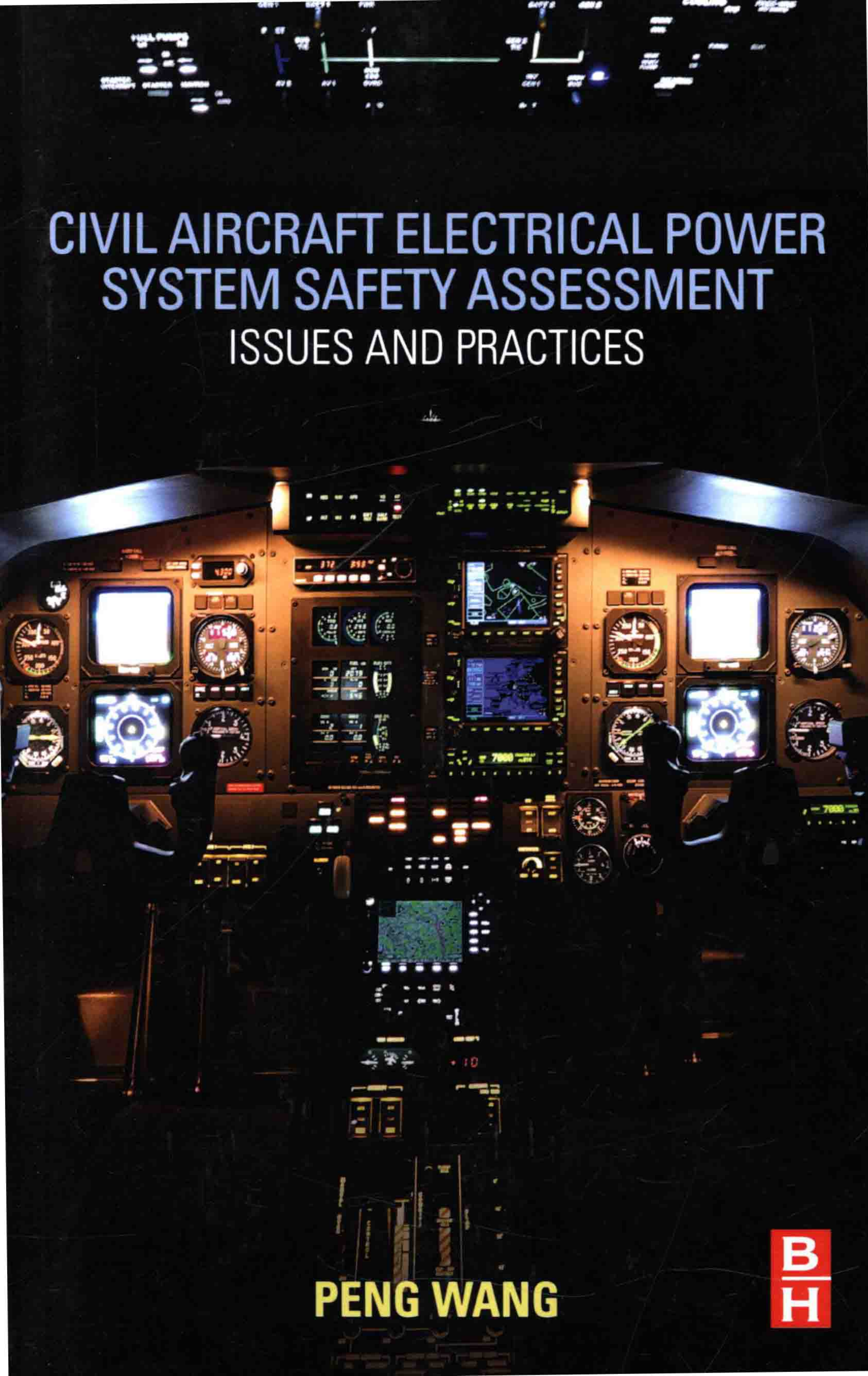

CIVIL AIRCRAFT ELECTRICAL POWER SYSTEM SAFETY ASSESSMENT

ISSUES AND PRACTICES

PENG WANG

CIVIL AIRCRAFT ELECTRICAL POWER SYSTEM SAFETY ASSESSMENT
ISSUES AND PRACTICES

PENG WANG

Civil Aircraft Airworthiness Technology and Management Research Center of CAAC,
Civil Aviation University of China

Civil Aircraft Electrical Power System Safety Assessment: Issues and Practices provides guidelines and methods for conducting a safety assessment process on civil airborne systems and equipment. Featuring a case study on the continuous safety assessment process of the civil airborne electrical power system, this book addresses problems, issues, and troubleshooting techniques such as single event effects, the failure effects of electrical wiring interconnection system (EWIS), formal theories, and safety analysis methods in civil aircrafts.

Key Features

- Introduces how to conduct assignment of development assurance levels for the electrical power system
- Includes safety assessments of aging platforms and their respective EWIS
- Features material on failure mechanisms for wiring systems and discussion of failure modes and effects analysis sustainment

About the Author

Peng Wang is a deputy director of the Civil Aircraft Airworthiness Certification Technology and Management Research Center of CAAC, and an associate professor of civil aviation at the Civil Aviation University of China. He holds his Masters' degree in safety management (ENSICA, France). He has 12 years of experience in system safety analysis, airborne electronic hardware engineering research and certification, and he has involved and participated in many Chinese-type certification and abroad-type validation projects. He has also led several aviation safety projects funded by CAAC and MIT (Ministry of Industry and Information Technology of China).

ISBN 978-0-08-100721-1

9 780081 007211

ELSEVIER

Butterworth-Heinemann
An imprint of Elsevier
elsevier.com/books-and-journals

CIVIL AIRCRAFT ELECTRICAL POWER SYSTEM SAFETY ASSESSMENT

WANG

BH

CIVIL AIRCRAFT ELECTRICAL POWER SYSTEM SAFETY ASSESSMENT

Issues and Practices

PENG WANG
Civil Aviation University of China, Tianjin, China

ELSEVIER

Butterworth-Heinemann
An imprint of Elsevier

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-08-100721-1

For Information on all Butterworth-Heinemann publications
visit our website at https://www.elsevier.com/books-and-journals

Publisher: Matthew Deans
Acquisition Editor: Carrie Bolger
Editorial Project Manager: Carrie Bolger
Production Project Manager: Anusha Sambamoorthy
Cover Designer: Matthew Limbert

Typeset by MPS Limited, Chennai, India

CIVIL AIRCRAFT ELECTRICAL POWER SYSTEM SAFETY ASSESSMENT

ABOUT THE AUTHOR

Peng Wang is Deputy Director of the Civil Aircraft Airworthiness Certification Technology and Management Research Center (CAAC) and Associate Professor of Civil Aviation at the University of China. He holds a master's degree in safety management from ENSICA, France.

He has 12 years of experience in system safety analysis, airborne electronic hardware engineering research and certification, and he has involved and participated in many Chinese-type certification and abroad-type validation projects. He has also led several aviation safety-related research projects funded by CAAC and MIT (Ministry of Industry and Information Technology of China).

FOREWORD

Since the Wright brothers took the aircraft "Flyer 1" into flight for the first time in 1903, the global aviation industry has enjoyed its development for more than 100 years. While safety acts as the lifeline of the civil aviation industry and premise of civil aircraft products to be put on the market, the safety assessment is a "measuring scale" for the safety of civil aircraft products. With respect to new technologies of aviation products, the safety assessment methods have a direct impact on the civil aircraft safety and innovation.

Over the past 30 years, China's civil aircraft manufacturing industry has made considerable development and progress with the emergence of a number of new civil aircraft types such as Y-12, MA60, ARJ21, MA700, Dragon 600, and C919, keeping up with the international trend of civil aircraft industry. Chinese aeronautical industries have also accumulated certain experience during a large amount of type developments and made explorations and innovations in solving the problems related to safety assessment methods of new technologies for some aviation products based on the national conditions.

Civil aircraft airworthiness certification technology and management research center of Civil Aviation Administration of China has been committed to the research and practice of civil aircraft safety assessment. In this book, through the safety assessment of the electrical power system of a certain type of transport category aircraft, the author, in the combination with civil aircraft safety standards and practical industrial experience, demonstrates the process and methods of the safety assessment to indicate the understanding and promotion to the development of international safety standards by the aviation industry of China. In addition, it discusses how to address the issues (e.g., single-event effects) and methods (e.g., the formal methods) in current safety process.

This book provides help and reference for engineers, students, and newcomers who are engaged in airborne system safety assessment.

Bai Jie

Vice President of Civil Aviation University of China, Tianjin, P.R. China

PREFACE

This book supplements the content of the advisory material to the regulation as well as the main supporting industry standards, and tries to discuss how to efficiently organize and manage safety activities. This book emphasizes on practices and guidelines by demonstrating the contiguous safety assessment process of civil airborne electrical power system. In addition, it discusses how to address the issues (e.g., single-event effects) and methods (e.g., the formal methods) in current safety assessment process.

Chapter 1, Airworthiness Regulations and Safety Requirements, and Chapter 2, Safety Management, summarize airworthiness regulations and safety requirements and also the management of safety activities.

The main safety assessment process and safety analysis methods, such as AFHA, SFHA, PSSA, CCA, FMEA, and SSA, are discussed in Chapter 3, Aircraft Functional Hazard Assessment, Chapter 4, System Functional Hazard Assessment, Chapter 5, Preliminary System Safety Assessment, Chapter 6, Common Cause Analysis, Chapter 7, Failure Modes and Effects Analysis, and Chapter 8, System Safety Assessment. From Chapter 4, System Functional Hazard Assessment, Chapter 5, Preliminary System Safety Assessment, Chapter 6, Common Cause Analysis, Chapter 7, Failure Modes and Effects Analysis with Summary, and Chapter 8, System Safety Assessment, each chapter first summarizes inputs, detailed process, and outputs of safety assessment process and safety analysis methods, and then a case study of civil airborne electrical power system is performed. The case study, which provides the continuity through Chapter 4, System Functional Hazard Assessment, Chapter 5, Preliminary System Safety Assessment, Chapter 6, Common Cause Analysis, Chapter 7, Failure Modes and Effects Analysis with Summary, and Chapter 8, System Safety Assessment, can show the reader how to bring the whole safety assessment activities together in a logical and efficient manner.

Chapter 9, Single Event Effects in Avionics, discusses how to address the issues of single-event effects in safety assessment process. The sensitivity assessment method is included, as well as an example of single-event effects, sensitivity assessment of electrical power system.

Chapter 10, Formal Model Based Safety Analysis Methods and the Application, discusses formal methods used in civil airborne system safety assessment, and a case study of the safety assessment for civil airborne electrical power system using the formal methods is given.

ACKNOWLEDGMENTS

I would like to thank all the people who have contributed to this book, and I especially acknowledge the following main contributions of my colleagues:

Xiao Nyue (Chapters 1, 2, and 6)
Yan Fang (Chapter 2)
Ma Zan (Chapters 5 and 8)
Dong Lei (Chapters 3, 4, and 10)
Dang Xiangjun (Chapter 7)
Zhao Changxiao (Chapter 10)
Xue QianNan (Chapter 9)

A special thanks to Cheng Wei, who provided great support and help for this book.

I would like to thank Guo Qiang, Zheng Jian, and all the other people who had contributed to this book.

I am grateful to my wife and my daughters for their years of understanding and support.

I am also grateful to Carrie Bolger, Anusha Sambamoorthy, and all the teams at Elsevier for their professional assistance.

ABBREVIATIONS AND ACRONYMS

AC	Advisory Circular
AC	Alternative Current
ADCU	Automatic Deploy Control Unit
AFHA	Aircraft Functional Hazard Assessment
AFM	Aircraft Flight Manual
AGCU	Auxiliary Generator Control Unit
APU	Auxiliary Power Unit
ARP	Aerospace Recommended Practice (SAE)
ASA	Aircraft Safety Assessment
ATA	Air Transport Association of America
ATC	Air Traffic Control
BIT	Built-In Test
BPCU	Bus Power Control Unit
CAAC	Civil aviation administration of China
CAS	Crew Alerting System
CCA	Common Cause Analysis
CCAR	China Civil Aviation Regulations
CCMR	Candidate Certification Maintenance Requirements
CI	Configuration Index
CMA	Common Mode Analysis
CMCC	Certification Maintenance Coordination Committee
CMR	Certification Maintenance Requirements
CMS	Central Maintenance System
COP	Cockpit Overhead Panel
COTS	Commercial-Off-The-Shelf
CP	Certification Plan
CS	Certification Specification
DAL	Development Assurance Level
DC	Direct Current
DCU	Data Concentrator Unit
DCTR	DC Tie Relay
DD	Dependent Diagram
EASA	European Aviation Safety Agency
EICAS	Engine Indication and Crew Alerting System
EMI	Electromagnetic Interference
EPS	Electrical Power System
ETSO	European Technical Standard Order
ETOPS	Extended Operations
EWIS	Electrical wiring interconnection systems
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FC	Failure Condition
FDAL	Function Development Assurance Level

FFS Functional Failure Set
FH Flight Hour
FHA Functional Hazard Assessment
FMEA Failure Modes and Effects Analysis
FMES Failure Modes and Effects Summary
FTA Fault Tree Analysis
GCU Generator Control Unit
HAS Hardware Accomplishment Summary
HCI Hardware Configuration Index
HIRF High Intensity Radiated Fields
ICAO International Civil Aviation Organization
IDAL Item development assurance level
IDG Integrated Drive Generator
ILS Instrument landing system
IMA Integrated Modular Avionic
INV Inverter
LACTR Left AC Tie Relay
LGCU Left Generator Control Unit
LPDA Left Power Distribution Assembly
LRU Line Replaceable Unit
MA Markov Analysis
MBSA Model Based Safety Analysis
MEL Minimum Equipment List
MFD Multifunction Display
MMEL Master Minimum Equipment List
MOPS Minimum Operational Performance Specifications
MRB Maintenance Review Board
MRBR Maintenance Review Board Report
MSG Maintenance Steering Group
NPRD Nonelectronic parts reliability data
OEM Original Equipment Manufacturers
PASA Preliminary Aircraft Safety Assessment
PDA Power Distribution Assembly
PHAC Plan for Hardware Aspects of Certification
PLD Programmable Logic Devices
PRA Particular Risk Analysis
PSAC Plan for Software Aspects of Certification
PSSA Preliminary System Safety Assessment
PTS Purchaser Technical Specification
RACTR Right AC Tie Relay
RAT Ram Air Turbine
RGCU Right Generator Control Unit
RPDA Right Power Distribution Assembly
RTCA (Previously) Radio Technical Commission for Aeronautics
SAE Society of Automotive Engineers, Inc.
SAS Software Accomplishment Summary
SCI Software Configuration Index