

Simplicity is Complex

Hermann Kopetz

Simplicity is Complex

Foundations of Cyber-Physical System
Design



Springer

Hermann Kopetz
Vienna University of Technology
Baden-Siegenfeld, Austria

ISBN 978-3-030-20410-5 ISBN 978-3-030-20411-2 (eBook)
<https://doi.org/10.1007/978-3-030-20411-2>

© Springer Nature Switzerland AG 2019

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.

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

Preface

It is the objective of this book to investigate what are the characteristics of *simple* versus *complex* systems and to find out what are the *design principles* that make a *Cyber-Physical System* understandable, simple to use, and easy to maintain. The adherence to these principles in the design of a *Cyber-Physical System* should lead to a significant reduction of the system complexity.

The targeted audiences of this book are engineers, managers, and advanced students who are involved in the design and evolution of Cyber-Physical Systems and are willing to spend some time outside the silo of their daily work in order to widen their background and learn more about the pervasive problems of *system complexity*.

My interest in the topic of complexity started when I was a manager of a process control department industry more than 40 years ago. This topic kept me hostage up to today. Forty years ago, the design of a process control system (today these systems are called *Cyber-Physical Systems*) was more of an art than an engineering endeavor. The software technology at that time was concerned primarily with *functional correctness* and did not pay much attention to the *temporal dimension* of program execution that is as important as functional correctness when a physical process must be controlled.

In the following years in academia, we tried to develop a *real-time system design methodology* where time was considered a first-order citizen. By taking time from the *problem domain* and putting it into the *solution domain*, many problems in the design of Cyber-Physical Systems can be simplified. We developed the *time-triggered protocols* and the *time-triggered architecture* that are now deployed in industry. But with an increase in the functional requirements and system size, the complexity problems appeared again in a different disguise.

A sound analysis of the *complexity problem* requires some insight in cognition, human problem-solving, and parts of philosophy. After becoming an *emeritus*, I had the time to look into these diverse fascinating fields more seriously.

After the introductory chapter, this book is divided into two parts. The first part (Chaps. 2–5) deals with the foundational issues of complexity, i.e., the conceptual, psychological, and philosophical aspects of complexity and the multi-level hierarchy

of models that are required to orient oneself in a complex world. The distinction between *essential data* (e-data) and *context data* (c-data) in Chap. 3 is of particular importance when a responsive real-time communication system must be designed and helped us in the design of the time-triggered protocol (TTP).

A reader who does not want to start with the rather heavy foundational issues of the first part is advised to initially jump over this part and go directly to Chap. 6. The reader may go back to these foundational issues at a later time when some deeper degree of understanding of the complexity problem is desired.

Chapter 6 points out that Cyber-Physical Systems are fundamentally different from conventional data processing systems. Chaps. 7–10 deal with the simplification and the engineering design of understandable Cyber-Physical Systems and present a framework for the development of a safety-critical CPS.

More than 100 small examples are interwoven throughout the text to demonstrate how the abstract ideas are related to concrete situations.

The present book contains the essence of my thinking about complexity accumulated over the past 40 years. In some sense, this book presents the rationale for the design of the time-triggered architecture (TTA). The TTA provides a sound engineering framework and methodology for the development of Cyber-Physical Systems.

The ideas presented in this book have grown over many years: first in the industry and then out of the numerous discussions at the Institute of Computer Engineering at the Vienna University of Technology, at IFIP WG 10.4 meetings, and in a number of exciting European research projects (particularly the AMADEOS projects on *Cyber-Physical Systems of System*, headed by Andrea Bondavalli). At this point, I would like to thank many friends who have contributed valuable comments on the earlier drafts of this book: Bernhard Froemel, Frank Furrer, Laila Gide, Radu Grosu, Brian Randell, Klaus Schmidt, Lui Sha, Rob Siegel, Wilfried Steiner, Neeraj Suri, and Martin Törngren.

Parts of the material have been derived from some of my previous publications and have been revised in order to bring them into a coherent whole.

Baden-Siegenfeld, Austria

H. Kopetz

Contents

1	Introduction	1
1.1	A Look Back in Time.	2
2	Understanding and Complexity	5
2.1	Introduction	5
2.2	Concepts.	5
2.3	Causal Explanation	7
2.4	Teleological Explanation	10
2.5	Complexity.	11
2.5.1	Complexity as a Property —Object Complexity	11
2.5.2	Complexity as a Relation—Cognitive Complexity	12
2.5.3	Complexity of a Model	15
2.6	Points to Remember.	16
3	Information Versus Data	19
3.1	Introduction	19
3.2	Information	20
3.2.1	Properties of an Itom	22
3.2.2	Human Communication.	23
3.3	Data	24
3.3.1	Data for Humans	26
3.3.2	Data in Cyberspace	26
3.3.3	Explanation and Generation of Data	27
3.3.4	Sense Data and Refined Data.	29
3.4	Essential Data (e-data) Versus Context Data (c-data)	31
3.5	Stigmergy.	33
3.6	Points to Remember.	35

4	Modeling	37
4.1	Introduction	37
4.2	Modeling Relation	40
4.2.1	Execution Time of Model Algorithms	42
4.2.2	Model Error	43
4.3	Mental Models	44
4.3.1	Rational Model	45
4.3.2	Intuitive Model	46
4.3.3	Pragmatic Mental Model (PMM)	47
4.4	Cyber Models	48
4.5	Models of Time	50
4.6	Assumption Coverage Versus Model Complexity	51
4.7	Points to Remember	52
5	Multi-Level Hierarchies	55
5.1	Introduction	55
5.2	Hierarchy Levels	56
5.2.1	Holons	57
5.3	Hierarchy Types	59
5.3.1	Formal Hierarchy	60
5.3.2	Information Hierarchy	60
5.3.3	Control Hierarchy	61
5.4	Emergence	62
5.4.1	Supervenience	65
5.5	Points to Remember	66
6	Cyber-Physical Systems Are Different	69
6.1	Introduction	69
6.2	Autonomous Operation in the Physical World	70
6.3	Timeliness	70
6.3.1	Pacing	71
6.3.2	Execution Time of Algorithms	71
6.3.3	Simultaneity	72
6.4	Safety-Criticality	72
6.5	Cyber Security	73
6.6	Points to Remember	74
7	Simplification	77
7.1	Introduction	77
7.2	Divide and Conquer	77
7.2.1	Partitioning in Space	79
7.2.2	Segmentation in Time	81
7.2.3	Abstraction	83
7.3	Static Structures	85
7.4	Emergence—New Conceptualization	85
7.5	Points to Remember	87

8	Communication Systems	89
8.1	Introduction	89
8.2	Classification of Data	89
8.2.1	Real-Time Data (RT Data)	90
8.2.2	Non-Real-Time Data (NRT Data)	92
8.3	Communication Protocols	92
8.3.1	Global Time	93
8.3.2	Time-Triggered Protocols	93
8.3.3	Time-Triggered Protocol (TTP)	94
8.3.4	Time-Triggered Ethernet (TTEthernet)	95
8.4	Communication with the Controlled Object	95
8.4.1	Sensor Inputs	96
8.4.2	Actuator	96
8.5	Real-Time Transfer of Alarm Data	96
8.6	Points to Remember	98
9	Interface Design	101
9.1	Introduction	101
9.2	Architectural Style	102
9.3	Interface Component	103
9.4	Interface Types	104
9.4.1	Service Interface	104
9.4.2	Configuration and Control Interface	105
9.4.3	Maintenance Interface	105
9.5	Interface Model	106
9.6	Human Machine Interface (HMI)	106
9.6.1	Alignment of Contexts	108
9.7	Points to Remember	110
10	Simplification of a Design	113
10.1	Introduction	113
10.2	Purpose Analysis	113
10.3	System Evolution	115
10.4	Architecture Design	116
10.4.1	Top-Level System Structure	116
10.4.2	Independent Components	117
10.4.3	Scheduling Slack	118
10.4.4	Peak Load Behavior	118
10.4.5	Fault Management	118
10.5	Multi-Level Hierarchy	119
10.6	Safety-Critical Control System	121
10.7	Points to Remember	124

11 Annex: Basic System Concepts 127

 11.1 Introduction 127

 11.2 Entities, Time, and Systems 127

 11.3 Component 130

 11.4 Communication 132

 11.5 Failures, Errors and Faults 133

 11.5.1 Software Errors 134

List of Abbreviations 135

References 137

Subject Index 141

Author Index 147