# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td>ix</td>
</tr>
<tr>
<td>1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>What Is a Cyber-Physical System?</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Key Features of Cyber-Physical Systems</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>Overview of Topics</td>
<td>5</td>
</tr>
<tr>
<td>1.4</td>
<td>Guide to Course Organization</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>Synchronous Model</td>
<td>13</td>
</tr>
<tr>
<td>2.1</td>
<td>Reactive Components</td>
<td>13</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Variables, Valuations, and Expressions</td>
<td>13</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Inputs, Outputs, and States</td>
<td>14</td>
</tr>
<tr>
<td>2.1.3</td>
<td>Initialization</td>
<td>15</td>
</tr>
<tr>
<td>2.1.4</td>
<td>Update</td>
<td>16</td>
</tr>
<tr>
<td>2.1.5</td>
<td>Executions</td>
<td>18</td>
</tr>
<tr>
<td>2.1.6</td>
<td>Extended-State Machines</td>
<td>19</td>
</tr>
<tr>
<td>2.2</td>
<td>Properties of Components</td>
<td>21</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Finite-State Components</td>
<td>21</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Combinational Components</td>
<td>22</td>
</tr>
<tr>
<td>2.2.3</td>
<td>Event-Triggered Components*</td>
<td>24</td>
</tr>
<tr>
<td>2.2.4</td>
<td>Nondeterministic Components</td>
<td>26</td>
</tr>
<tr>
<td>2.2.5</td>
<td>Input-Enabled Components</td>
<td>29</td>
</tr>
<tr>
<td>2.2.6</td>
<td>Task Graphs and Await Dependencies</td>
<td>30</td>
</tr>
<tr>
<td>2.3</td>
<td>Composing Components</td>
<td>36</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Block Diagrams</td>
<td>36</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Input/Output Variable Renaming</td>
<td>38</td>
</tr>
<tr>
<td>2.3.3</td>
<td>Parallel Composition</td>
<td>38</td>
</tr>
<tr>
<td>2.3.4</td>
<td>Output Hiding</td>
<td>47</td>
</tr>
<tr>
<td>2.4</td>
<td>Synchronous Designs</td>
<td>49</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Synchronous Circuits</td>
<td>50</td>
</tr>
<tr>
<td>2.4.2</td>
<td>Cruise Control System</td>
<td>54</td>
</tr>
<tr>
<td>2.4.3</td>
<td>Synchronous Networks*</td>
<td>58</td>
</tr>
</tbody>
</table>
## Safety Requirements

### 3.1 Invariants of Transition Systems
- 3.1.1 Role of Requirements in System Design
- 3.1.2 Safety Monitors

### 3.2 Verifying Invariants
- 3.2.1 Proving Invariants
- 3.2.2 Automated Invariant Verification
- 3.2.3 Simulation-Based Analysis

### 3.3 Enumerative Search

### 3.4 Symbolic Search
- 3.4.1 Symbolic Transition Systems
- 3.4.2 Symbolic Breadth-First Search
- 3.4.3 Reduced Ordered Binary Decision Diagrams

## Asynchronous Model

### 4.1 Asynchronous Processes
- 4.1.1 States, Inputs, and Outputs
- 4.1.2 Input, Output, and Internal Actions
- 4.1.3 Executions
- 4.1.4 Extended-State Machines
- 4.1.5 Operations on Processes
- 4.1.6 Safety Requirements

### 4.2 Asynchronous Design Primitives
- 4.2.1 Blocking vs. Non-blocking Synchronization
- 4.2.2 Deadlocks
- 4.2.3 Shared Memory
- 4.2.4 Fairness Assumptions

### 4.3 Asynchronous Coordination Protocols
- 4.3.1 Leader Election
- 4.3.2 Reliable Transmission
- 4.3.3 Wait-Free Consensus

## Liveness Requirements

### 5.1 Temporal Logic
- 5.1.1 Linear Temporal Logic
- 5.1.2 LTL Specifications
- 5.1.3 LTL Specifications for Asynchronous Processes
- 5.1.4 Beyond LTL

### 5.2 Model Checking
- 5.2.1 Büchi Automata
- 5.2.2 From LTL to Büchi Automata
- 5.2.3 Nested Depth-First Search
- 5.2.4 Symbolic Repeatability Checking

### 5.3 Proving Liveness
- 5.3.1 Eventuality Properties
5.3.2 Conditional Response Properties 224

6 Dynamical Systems 231
6.1 Continuous-Time Models 231
   6.1.1 Continuously Evolving Inputs and Outputs 231
   6.1.2 Models with Disturbance 241
   6.1.3 Composing Components 242
   6.1.4 Stability 243
6.2 Linear Systems 248
   6.2.1 Linearity 248
   6.2.2 Solutions of Linear Differential Equations 251
   6.2.3 Stability 259
6.3 Designing Controllers 263
   6.3.1 Open-Loop vs. Feedback Controller 263
   6.3.2 Stabilizing Controller 264
   6.3.3 PID Controllers* 269
6.4 Analysis Techniques* 277
   6.4.1 Numerical Simulation 277
   6.4.2 Barrier Certificates 280

7 Timed Model 289
7.1 Timed Processes 289
   7.1.1 Timing-Based Light Switch 289
   7.1.2 Buffer with a Bounded Delay 291
   7.1.3 Multiple Clocks 292
   7.1.4 Formal Model 294
   7.1.5 Timed Process Composition 297
   7.1.6 Modeling Imperfect Clocks* 300
7.2 Timing-Based Protocols 301
   7.2.1 Timing-Based Distributed Coordination 302
   7.2.2 Audio Control Protocol* 305
   7.2.3 Dual Chamber Implantable Pacemaker 310
7.3 Timed Automata 317
   7.3.1 Model of Timed Automata 318
   7.3.2 Region Equivalence* 319
   7.3.3 Matrix-Based Representation for Symbolic Analysis 328

8 Real-Time Scheduling 339
8.1 Scheduling Concepts 339
   8.1.1 Scheduler Architecture 340
   8.1.2 Periodic Job Model 341
   8.1.3 Schedulability 345
   8.1.4 Alternative Job Models 350
8.2 EDF Scheduling 352
   8.2.1 EDF for Periodic Job Model 352
   8.2.2 Optimality of EDF 356
8.2.3 Utilization-Based Schedulability Test .......................... 358
8.3 Fixed-Priority Scheduling ........................................ 362
  8.3.1 Deadline-Monotonic and Rate-Monotonic Policies ....... 362
  8.3.2 Optimality of Deadline-Monotonic Policy * ............. 365
  8.3.3 Schedulability Test for Rate-Monotonic Policy * ....... 372

9 Hybrid Systems ............................................. 381
  9.1 Hybrid Dynamical Models .................................... 381
    9.1.1 Hybrid Processes ....................................... 381
    9.1.2 Process Composition .................................... 388
    9.1.3 Zeno Behaviors .......................................... 391
    9.1.4 Stability .................................................. 395
  9.2 Designing Hybrid Systems .................................... 397
    9.2.1 Automated Guided Vehicle ................................ 397
    9.2.2 Obstacle Avoidance with Multi-robot Coordination ..... 400
    9.2.3 Multi-hop Control Networks * ........................... 408
  9.3 Linear Hybrid Automata * .................................... 415
    9.3.1 Example Pursuit Game ................................. 416
    9.3.2 Formal Model ............................................ 419
    9.3.3 Symbolic Reachability Analysis ......................... 422

Bibliography .................................................. 433

Index ......................................................... 441