Advances in Industrial Control

Zhe Wu
Panagiotis D. Christofides

Process Operational Safety and Cybersecurity

A Feedback Control Approach

AIC

Springer

Advances in Industrial Control

Series Editors

Michael J. Grimble, Industrial Control Centre, University of Strathclyde, Glasgow, UK

Antonella Ferrara, Department of Electrical, Computer and Biomedical Engineering, University of Pavia, Pavia, Italy

Editorial Board

Graham Goodwin, School of Electrical Engineering and Computing, University of Newcastle, Callaghan, NSW, Australia

Thomas J. Harris, Department of Chemical Engineering, Queen’s University, Kingston, ON, Canada

Tong Heng Lee, Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Singapore

Om P. Malik, Schulich School of Engineering, University of Calgary, Calgary, AB, Canada

Kim-Fung Man, City University Hong Kong, Kowloon, Hong Kong

Gustaf Olsson, Department of Industrial Electrical Engineering and Automation, Lund Institute of Technology, Lund, Sweden

Asok Ray, Department of Mechanical Engineering, Pennsylvania State University, University Park, PA, USA

Sebastian Engell, Lehrstuhl für Systemdynamik und Prozessführung, Technische Universität Dortmund, Dortmund, Germany

Ikuo Yamamoto, Graduate School of Engineering, University of Nagasaki, Nagasaki, Japan

Advances in Industrial Control is a series of monographs and contributed titles focusing on the applications of advanced and novel control methods within applied settings. This series has worldwide distribution to engineers, researchers and libraries.

The series promotes the exchange of information between academia and industry, to which end the books all demonstrate some theoretical aspect of an advanced or new control method and show how it can be applied either in a pilot plant or in some real industrial situation. The books are distinguished by the combination of the type of theory used and the type of application exemplified. Note that "industrial" here has a very broad interpretation; it applies not merely to the processes employed in industrial plants but to systems such as avionics and automotive brakes and drivetrain. This series complements the theoretical and more mathematical approach of Communications and Control Engineering.

Indexed by SCOPUS and Engineering Index.

Proposals for this series, composed of a proposal form downloaded from this page, a draft Contents, at least two sample chapters and an author cv (with a synopsis of the whole project, if possible) can be submitted to either of the:

Series Editors

Professor **Michael J. Grimble**
Department of Electronic and Electrical Engineering, Royal College Building, 204
George Street, Glasgow G1 1XW, United Kingdom
e-mail: m.j.grimble@strath.ac.uk

Professor **Antonella Ferrara**
Department of Electrical, Computer and Biomedical Engineering, University of
Pavia, Via Ferrata 1, 27100 Pavia, Italy
e-mail: antonella.ferrara@unipv.it

or the

In-house Editor

Mr. **Oliver Jackson**
Springer London, 4 Crinan Street, London, N1 9XW, United Kingdom
e-mail: oliver.jackson@springer.com

Proposals are peer-reviewed.

Publishing Ethics

Researchers should conduct their research from research proposal to publication in line with best practices and codes of conduct of relevant professional bodies and/or national and international regulatory bodies. For more details on individual ethics matters please see:
https://www.springer.com/gp/authors-editors/journal-author/journal-author-helpdesk/publishing-ethics/14214

More information about this series at http://www.springer.com/series/1412

Zhe Wu · Panagiotis D. Christofides

Process Operational Safety and Cybersecurity

A Feedback Control Approach

Springer

Zhe Wu
Department of Chemical and Biomolecular Engineering
University of California
Los Angeles, CA, USA

Panagiotis D. Christofides
Department of Chemical and Biomolecular Engineering
University of California
Los Angeles, CA, USA

ISSN 1430-9491 ISSN 2193-1577 (electronic)
Advances in Industrial Control
ISBN 978-3-030-71182-5 ISBN 978-3-030-71183-2 (eBook)
https://doi.org/10.1007/978-3-030-71183-2

Mathematics Subject Classification (2010): 93C83, 49J15, 93C10

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021
This work is subject to copyright. All rights are solely and exclusively licensed 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, expressed 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

Traditionally, the operational safety of chemical processes has been addressed through process design considerations and through a hierarchical, independent design of control and safety systems. By developing safety systems including alarms, emergency shutdown, and further emergency response systems to be activated when control systems fail to operate chemical processes in a normal operating region, process operational safety has been improved to prevent incidents that can lead to property damage, human injuries, and environmental impact. However, the consistent accidents throughout chemical process plant history (including several high-profile disasters in the last decade) have motivated researchers to design control systems that explicitly account for process operational safety considerations. In particular, a new design of control systems such as model predictive controllers (MPC) that incorporates safety considerations and can be coordinated with safety systems has the potential to significantly improve process operational safety and avoid unnecessary triggering of alarm systems. However, the rigorous design of safety-based control systems poses new challenges that cannot be addressed with traditional process control methods, including, for example, proving simultaneous closed-loop stability and safety. On the other hand, cybersecurity has become increasingly important in chemical process industries in recent years as cyber-attacks that have grown in sophistication and frequency have become another leading cause of process safety incidents. While the traditional methods of handling cyber-attacks in control systems still rely partly on human analysis and mainly fall into the area of fault diagnosis, the intelligence of cyber-attacks and their accessibility to control system information have recently motivated researchers to develop cyber-attack detection and resilient operation control strategies to address directly cybersecurity concerns.

The book covers several rigorous methods for the design of MPC systems that improve process operational safety and cybersecurity for chemical processes described by nonlinear dynamic models. Beginning with the motivation and organization of this book, a background on nonlinear systems analysis, Lyapunov-based control techniques, and MPC designs is first presented. Then, two MPC schemes that use a Safeness Index function and a control Lyapunov-barrier function, respectively, are presented with rigorous analysis provided on their closed-loop stability, operational safety, and recursive feasibility properties, followed by case studies of large-scale chemical processes under integrated process control and safety systems. Subsequently, the use of machine learning techniques to develop data-driven nonlinear dynamic process models to be used in the MPC schemes is presented with closed-loop stability and safety analysis as well as discussion on computational implementation issues. Next, the development of an integrated detection and control system for process cybersecurity is developed, in which several types of intelligent cyber-attacks, machine learning detection methods, and resilient control strategies are presented. The book closes with a two-tier control architecture that possesses inherent cybersecurity properties and could provide a blueprint for the design of cybersecure industrial process control systems. Throughout the book, the control methods are applied to numerical simulations of nonlinear chemical process examples and Aspen simulations of large-scale chemical process networks to demonstrate their effectiveness and performance.

The book requires some knowledge of nonlinear systems, nonlinear control theory, and nonlinear programming methods, and is intended for researchers, graduate students, and process control and safety engineers.

In conclusion, we would like to acknowledge Prof. Helen Durand, Prof. Fahad Albalawi, Dr. Anas Alanqar, Dr. Anh Tran, Dr. David Rincon, Dr. Zhihao Zhang, and Ms. Scarlett Chen, all at UCLA, who have contributed substantially to the research efforts and results included in this book. We would like to thank them for their hard work and contributions. We would also like to thank all the other people who contributed in some way to this project. In particular, we would like to thank our colleagues at UCLA, and the United States National Science Foundation and Department of Energy for financial support. Last but not the least, we would like to express our deepest gratitude to our families for their dedication, encouragement, and support over the course of this project. We dedicate this book to them.

Los Angeles, CA, USA

Zhe Wu
Panagiotis D. Christofides

Contents

1 Introduction 1
1.1 Motivation 1
1.2 Background 3
1.3 Operational Safety and Cybersecurity of Chemical Processes 6
1.3.1 Continuously Stirred Tank Reactor 7
1.3.2 Case Study: Process Operational Safety in EMPC 8
1.3.3 Case Study: Cybersecurity in Tracking MPC 10
1.4 Objectives and Organization of the Book 11

2 Background 15
2.1 Notation 15
2.2 Stability of Nonlinear Systems 16
2.2.1 Lyapunov's Direct Method 18
2.2.2 LaSalle's Invariance Principle 18
2.3 Control of Nonlinear Systems 19
2.3.1 Control Lyapunov Functions and Stabilization 19
2.3.2 Model Predictive Control 23
2.3.2.1 Main Components of MPC 23
2.3.2.2 Process Model 24
2.3.2.3 Receding Horizon Implementation 25
2.3.2.4 Sample-and-Hold Implementation of Controllers 25
2.3.2.5 MPC Formulation 26
2.3.3 Lyapunov-Based MPC 27
2.3.3.1 Closed-Loop Stability Under LMPC 28
2.3.3.2 Feasibility Analysis 31
2.3.4 Lyapunov-Based Economic MPC 32
2.3.4.1 Closed-Loop Stability Under LEMPC 34

3 Safeness Index-Based MPC and EMPC . . . 35
3.1 Introduction . . . 35
3.1.1 Class of Nonlinear Systems . . . 35
3.2 Process Operational Safety . . . 37
3.2.1 Safeness Index . . . 38
3.2.2 Choosing Thresholds for Safeness Index . . . 41
3.3 Safeness Index-Based MPC and EMPC . . . 43
3.3.1 Stability, Safety, and Feasibility Analyses . . . 46
3.4 Application to a Chemical Process Example . . . 50
3.4.1 Process Description . . . 50
3.4.2 Simulation Results . . . 53
3.5 Conclusions . . . 58

4 Operational Safety Via Control Lyapunov-Barrier Function-Based MPC . . . 59
4.1 Introduction . . . 59
4.1.1 Class of Nonlinear Systems . . . 60
4.1.2 Characterization of Unsafe Regions . . . 60
4.2 Control Barrier Function . . . 61
4.3 Control Lyapunov-Barrier Function . . . 63
4.3.1 Stabilization and Safety via Control Lyapunov-Barrier Function . . . 64
4.3.1.1 Stabilizability Assumptions . . . 64
4.3.1.2 Stabilization and Safety via CLBF . . . 64
4.3.1.3 Closed-Loop Stability and Safety Under CLBF-Based Controller . . . 66
4.3.2 Design of Constrained CLBF . . . 70
4.4 CLBF-Based Model Predictive Control . . . 72
4.4.1 Sample-and-Hold Implementation of CLBF-Based Controller . . . 72
4.4.2 Formulation of CLBF-MPC . . . 75
4.4.3 Application to a Chemical Process Example . . . 78
4.4.3.1 Case Study: Bounded Unsafe Region . . . 79
4.4.3.2 Case Study: Unbounded Unsafe Region . . . 84
4.5 CLBF-Based Economic Model Predictive Control . . . 85
4.5.1 CLBF-Based EMPC Formulation . . . 85
4.5.2 Application to a Chemical Process Example . . . 91
4.6 Conclusions . . . 94

5 Integration of Safety Systems with Control Systems . . . 95
5.1 Introduction . . . 95
5.2 Integration of Safety and Control Systems . . . 96
5.2.1 Case Study: Thermal Runaway in a CSTR System . . . 96
5.2.1.1 MIC Reaction and CSTR Process Description . . . 97
5.2.1.2 Lyapunov-Based MPC Design . . . 98

5.2.1.3 Simulation Results Under Disturbances 99
5.2.1.4 Integration of MPC with Safety System 101
5.2.1.5 Integration of Control and Safety Systems 102
5.2.1.6 Closed-Loop Simulation Results 103
5.2.2 Case Study: High Pressure in a Flash Drum 105
5.2.2.1 Flash Drum Process Description and Relief Valve Design 105
5.2.2.2 Feedback Controller Design 107
5.2.2.3 Closed-Loop Simulation Results 109
5.3 Safeness Index-Based MPC 113
5.3.1 Case Study: Flash Drum 113
5.3.1.1 Flash Drum Process Description and Control Objective 113
5.3.1.2 Safeness Index-Based MPC 114
5.3.1.3 Formulation of Safeness Index-Based MPC 116
5.3.1.4 Closed-Loop Simulation Results 117
5.3.2 Case Study: Ammonia Process 121
5.3.2.1 Ammonia Process Descriptions and Simulations 121
5.3.2.2 Safeness Index-Based MPC 125
5.3.2.3 Closed-Loop Simulation Results 128
5.3.3 Case Study: Ammonia Process Network 130
5.3.3.1 Ammonia Process Description 130
5.3.3.2 Disturbance and Process Operational Safety 132
5.3.3.3 Feedback Controller Design 133
5.3.3.4 Closed-Loop Simulation Results 138
5.4 Conclusions 142

6 Machine Learning in Process Operational Safety 143
6.1 Introduction 143
6.1.1 Class of Nonlinear Systems 144
6.1.2 Stabilizability Assumption 145
6.2 Recurrent Neural Network Modeling 146
6.2.1 RNN Learning Algorithm 148
6.2.2 Development of RNN Model 151
6.2.2.1 Data Generation 151
6.2.2.2 Training Process 151
6.2.3 Ensemble Regression Modeling 153
6.3 CLBF-MPC Using RNN Models 156
6.3.1 Stabilization and Safety via CLBF-Based Control 156
6.3.2 CLBF-based MPC Using an Ensemble of RNN Models 159
6.3.2.1 CLBF-Based Control Using RNN Models 161
6.3.2.2 Sample-and-Hold Implementation of CLBF-Based Controller 164
6.3.2.3 Formulation of CLBF-MPC 166

6.3.3 Parallel Computing and Ensemble of RNN Models 168
6.3.3.1 Training Multiple RNNs in Parallel 169
6.3.3.2 Parallel Operation of CLBF-MPC Using an Ensemble of RNNs 169
6.3.4 Online Learning of RNN Models 171
6.3.4.1 Implementation Strategy For Online RNN Learning within CLBF-MPC 173
6.3.5 Computational Implementation Issues of RNN Models 175
6.3.5.1 Long Prediction Horizon 175
6.3.5.2 Approximation Via Numerical Methods 176
6.3.6 Application to a Chemical Process Example 177
6.3.6.1 Development of RNN Models 178
6.3.6.2 Closed-Loop Simulation Results 179
6.3.6.3 Comparison with A Linear State-Space Model 182
6.3.6.4 Real-Time CLBF-MPC with Online Learning of RNN Models 183
6.4 CLBF-EMPC Using RNN Models 185
6.4.1 Stability and Safety Under CLBF-EMPC 186
6.4.1.1 Online Learning of RNN Models 190
6.4.2 Application to a Chemical Process Example 191
6.4.2.1 Closed-Loop Simulation Results 191
6.4.2.2 Real-Time CLBF-EMPC with Online Learning of RNN Models 196
6.5 Conclusions 198

7 Process Cybersecurity Via Machine Learning Detection 201
7.1 Introduction 201
7.1.1 Class of Nonlinear Systems 202
7.1.2 Lyapunov-Based MPC and EMPC 203
7.2 Intelligent Cyber-Attacks 205
7.2.1 Types of Intelligent Cyber-Attacks 206
7.2.1.1 Min-Max Cyber-Attack 206
7.2.1.2 Geometric Cyber-Attack 207
7.2.1.3 Replay Cyber-Attack 207
7.2.1.4 Surge Cyber-Attack 207
7.2.1.5 Simulation Design Guide 209
7.3 Detection of Cyber-Attacks Targeting MPC Systems 211
7.3.1 Choice of Detection Input Variable 214
7.3.2 Sliding Detection Window 215
7.4 Cyber-Attack Resilient Control Systems 217
7.4.1 Redundant Sensors 217
7.4.2 Attack-Resilient Operation Combining Open-Loop and Closed-Loop Control 218
7.4.3 Post Cyber-Attack State Reconstruction 222

7.4.3.1 Recurrent Neural Network 222
7.4.3.2 Online Reconstruction 224
7.4.3.3 Closed-Loop Control with Reconstructed States 224
7.5 Application to a Chemical Process Example 227
7.6 Conclusions 240

8 A Two-Tier Control Architecture For Cybersecurity and Operational Safety 241
8.1 Introduction 241
8.1.1 Class of Nonlinear Systems 242
8.2 Cyber-Secure Two-Tier Control Architecture 243
8.2.1 Lower-Tier Control System 243
8.2.2 Upper-Tier Model Predictive Control System 244
8.3 Cyber-Attack Design and Detection 247
8.3.1 Attack Scenarios 248
8.3.2 Mitigation Measures via Reconfiguration of Control System 249
8.3.3 Integration of Safety Systems with Two-Tier Control Systems 251
8.4 Application to a Chemical Process Example 252
8.4.1 Cyber-Attacks and Detector Training 257
8.4.2 Cyber-Attack Detection Results 258
8.5 Conclusions 265

References 267

List of Figures

Fig. 1.1 Control/safety system layers [119] 2

Fig. 1.2 Schematic of a CSTR with an irreversible, second-order reaction that converts the reactant A to the desired product B 7

Fig. 1.3 State trajectory in closed-loop simulation of the CSTR under EMPC when the initial condition is at the steady-state, i.e., $(C_A(0) - C_{As}, T(0) - T_s)$=$(0\ \frac{\text{kmol}}{\text{m}^3}, 0K)$ 9

Fig. 1.4 **a** Production rate profile $k_0 e^{-E/RT} C_A^2 (\frac{kmol}{m^3\ h})$ within the safe operating region of the CSTR, and **b** accumulated operating profits for the closed-loop CSTR under EMPC and steady-state operation, respectively 10

Fig. 1.5 Closed-loop state trajectories for the CSTR under tracking MPC when the temperature sensor is under no attack, and under a min-max attack, respectively 11

Fig. 1.6 **a** State and **b** input profiles for the CSTR under tracking MPC when the temperature sensor is under no attack, and under a min-max attack, respectively 12

Fig. 2.1 General concept for model predictive control (MPC) 24

Fig. 2.2 An exemplar closed-loop state trajectory with initial state $x(t_0)$ under LMPC 29

Fig. 2.3 A two-layer paradigm for optimizing process economics within process control 32

Fig. 2.4 An exemplar closed-loop state trajectory under LEMPC, where the red and the blue trajectories are under Mode 1 and Mode 2 constraints, respectively 33

Fig. 3.1 Systematic methodology to construct Safeness Index function $S(x)$ and its thresholds 40

Fig. 3.2 Example of the stability region Ω_ρ partitioned into "safe" $(S(x) < S_{TH})$ and "unsafe" $(S(x) > S_{TH})$ regions, where Ω_{ρ_e} is a subset of Ω_ρ to ensure forward invariance of Ω_ρ in the LEMPC of Eq. 2.35 42

Fig. 3.3 Manipulated input profiles for the closed-loop CSTR under the LEMPC design of Eq. 2.35 and under the Safeness Index-based EMPC design of Eq. 3.7 for the initial condition $x_0^T = [0 \ \frac{\text{kmol}}{\text{m}^3} \ 0 \text{ K}]$ 54

Fig. 3.4 The state profiles for the closed-loop CSTR under the LEMPC design of Eq. 2.35 and under the Safeness Index-based EMPC design of Eq. 3.7 for the initial condition $x_0^T = [0 \ \frac{\text{kmol}}{\text{m}^3} \ 0 \text{ K}]$ 54

Fig. 3.5 The Safeness Index function $S(x)$ for the closed-loop CSTR under the LEMPC design of Eq. 2.35 and under the Safeness Index-based EMPC design of Eq. 3.7 for the initial condition $x_0^T = [0 \ \frac{\text{kmol}}{\text{m}^3} \ 0 \text{ K}]$ 56

Fig. 3.6 The state-space profile for the closed-loop CSTR under the LEMPC design of Eq. 2.35 (black trajectory) and under the Safeness Index-based EMPC design of Eq. 3.7 (dark gray trajectory) for the initial condition $x_0^T = [0 \ \frac{\text{kmol}}{\text{m}^3} \ 0 \text{ K}]$ 56

Fig. 3.7 The Safeness Index function $S(x)$ for the closed-loop CSTR under the Safeness Index-based EMPC design of Eq. 3.7 for the initial condition $x_0^T = [0 \ \frac{\text{kmol}}{\text{m}^3} \ 0 \text{ K}]$ with bounded process disturbances 57

Fig. 3.8 The state-space profile for the closed-loop CSTR under the Safeness Index-based EMPC design of Eq. 3.7 for the initial condition $x_0^T = [0 \ \frac{\text{kmol}}{\text{m}^3} \ 0 \text{ K}]$ with bounded process disturbances 57

Fig. 4.1 A schematic showing an initial condition x_0 from which the state trajectory converges to x_e and passes around a bounded unsafe set $\mathscr{D}_b$ embedded within the operating region either in the up or down direction using a discontinuous control action 67

Fig. 4.2 A schematic representing an unbounded unsafe set $\mathscr{D}_u$ in state-space, where the trajectories start from any initial condition x_0 avoid $\mathscr{D}_u$ and converge to the origin x_s^* 69

Fig. 4.3 A schematic showing the relationship among the sets ϕ_{uc}, $\mathscr{D}$, $\mathscr{D}_H$, and H, where $\mathscr{U}_{\rho_c}$ is the invariant set shown as an ellipse subtracting $\mathscr{D}_H$ 71

Fig. 4.4 A schematic representing the sets $\mathscr{U}_{\rho_c}$, $\mathscr{U}_{\rho_{\min}}$, and $\mathscr{U}_{\rho_s}$, where an example of the state trajectory (dotted line) for the closed-loop system under the sample-and-hold implementation of $u = \Phi(x) \in U$ is shown to ultimately enter and remain in $\mathscr{U}_{\rho_{\min}}$ while avoiding the unsafe region $\mathscr{D}$ at all times from the initial state $x_0 \in \mathscr{U}_{\rho_c}$ 74

Fig. 4.5 Closed-loop state trajectories for four different initial conditions $(-0.19, 5.5)$ (red line), $(0.2, -5)$ (green line), $(-0.235, 6.5)$ (blue line), and $(-0.35, 7)$ (black line) under CLBF-MPC. The set $\mathscr{U}_\rho$ is the region between the set H and the largest ellipse, and the set of unsafe states $\mathscr{D}$ is represented by the solid black ellipse 80

Fig. 4.6 Closed-loop state profiles under the MPC with state constraints (dashed line) and the CLBF-MPC of Eq. 4.27 (solid line) with the same initial condition $(-0.235, 6.5)$, where the unsafe region $\mathscr{D}$ is represented by the solid black ellipse 81

Fig. 4.7 Closed-loop state profile for the disturbed system under CLBF-MPC (solid line) with the initial condition $(-0.235, 6.5)$ 82

Fig. 4.8 Manipulated input profiles ($u_1 = \Delta C_{A0}$ and $u_2 = \Delta Q$) for the disturbed system under CLBF-MPC with the initial condition $(-0.235, 6.5)$ 82

Fig. 4.9 Closed-loop state profiles under the CLBF-based controller of Eq. 4.11 (dashed line) and the CLBF-MPC of Eq. 4.27 (solid line) for the initial condition $(-0.235, 6.5)$ 83

Fig. 4.10 Manipulated input profiles ($u_1 = \Delta C_{A0}$ and $u_2 = \Delta Q$) under the CLBF-based controller of Eq. 4.11 (dashed line) and the CLBF-MPC of Eq. 4.27 (solid line) for the initial condition $(-0.235, 6.5)$ 83

Fig. 4.11 Closed-loop state trajectories (with different initial conditions marked by stars) for the system of Eq. 4.28 under CLBF-MPC, where the unbounded unsafe region $\mathscr{D}_u$ is represented by the red area on the top 84

Fig. 4.12 Closed-loop state trajectories for the CSTR under the CLBF-EMPC of Eq. 4.33 and the standard LEMPC of Eq. 2.35 with the same initial condition $(0, 0)$ 92

Fig. 4.13 Manipulated input profiles ($u_1 = \Delta C_{A0}$, $u_2 = \Delta Q$) for the CSTR under the CLBF-EMPC of Eq. 4.33 and the standard LEMPC of Eq. 2.35 with the same initial condition $(0, 0)$ 93

Fig. 5.1 State-space profile (top) and input trajectory (bottom) under a small disturbance 100

Fig. 5.2 State-space profile (top) and input trajectory (bottom) under a large disturbance 100

Fig. 5.3 Safety system for the CSTR with an MIC hydrolysis reaction 102

Fig. 5.4 A schematic showing, in the $C_A - T$ state-space, the stability region (white region), unsafe operating region (light gray region), and the thermal runaway region (dark gray region), together with an example trajectory starting from the origin 103

Fig. 5.5 State-space plot and input plot of LMPC integrated with the safety system for the MIC hydrolysis reaction in a CSTR 104

Fig. 5.6 A schematic of the flash process with a heat exchanger, flash drum, pump (from left to right), valves, and controllers that control the temperature and liquid level. The temperature controller (marked by "Designing") is designed to account for the safety system activation for handling vapor effluent valve failure (marked by "Device failure") 106

Fig. 5.7 Manipulated input and controlled output profiles for the temperature controller with varying tuning parameters to account for the activation of the safety system in a flash drum 110

Fig. 5.8 Drum pressure profile under the temperature controller with varying tuning parameters to account for the activation of the safety system in a flash drum 110

Fig. 5.9 Flash drum temperature profile under the temperature controllers with fixed parameters, and varying tuning parameters to account for the activation of the safety system, respectively 111

Fig. 5.10 Drum temperature and heating duty profiles under the temperature controller with varying tuning parameters to account for the activation of the relief valve with the reseating pressure of 9.2 bar in a flash drum 111

Fig. 5.11 Drum pressure profile under the temperature controller with varying tuning parameters to account for the activation of the relief valve with the reseating pressure of 9.2 bar in a flash drum 112

Fig. 5.12 **a** Drum pressure and **b** temperature profiles under Safeness Index-based MPC with a device failure that changes the top vapor valve opening from 50% to 45% 118

Fig. 5.13 **a** Manipulated input and **b** Safeness Index profiles under Safeness Index-based MPC with a device failure that changes the top vapor valve opening from 50% to 45% 118

Fig. 5.14 **a** Drum pressure and **b** temperature profiles under Safeness Index-based MPC with a device failure that changes the top vapor valve opening from 50% to 35%.when the top vapor valve is closed from 50% to 35% 118

Fig. 5.15 **a** Manipulated input and **b** Safeness Index profiles under Safeness Index-based MPC with a device failure that changes the top vapor valve opening from 50% to 35% 119
Fig. 5.16 **a** Drum pressure and **b** temperature profiles under Safeness Index-based MPC with a device failure that changes the top vapor valve opening from 50% to 10% 120
Fig. 5.17 **a** Manipulated input and **b** Safeness Index profiles under Safeness Index-based MPC with a device failure that changes the top vapor valve opening from 50% to 10% 121
Fig. 5.18 A schematic of an ammonia process 122
Fig. 5.19 A schematic of all simulated units, where the high-temperature shift reactor, heat exchanger, low-temperature shift reactor, CO_2 removal, and methanator are denoted by HT-SHIFT, HE, LT-SHIFT, CO_2 REMOVAL, and METHANATOR, respectively 123
Fig. 5.20 Methanator outlet temperature profiles, from which it is shown that $T - T_{ss}$ increases more than **a** 80 °C after the catalyst activity decreases from 1 to 0.1 in 300 s, and **b** 60 °C after the feed temperature decreases from 380 °C to 280 °C in 300 s, respectively, in the high-temperature shift reactor 126
Fig. 5.21 Close-loop methanator **a** outlet temperature and **b** feed temperature profiles when the catalyst activity decreases from 1 to 0.1 within 300 s in the high-temperature shift reactor 129
Fig. 5.22 Close-loop methanator **a** outlet temperature and **b** feed temperature profiles when the feed temperature decreases from 380 °C to 280 °C within 300 s in the high-temperature shift reactor 129
Fig. 5.23 A schematic of the entire ammonia process network 131
Fig. 5.24 A schematic of the control structure that uses two control loops, where C_1 and C_2 represent controller 1 and controller 2 132
Fig. 5.25 A schematic of disturbance propagation showing that a reaction thermal runaway may occur due to the increasing concentration of CO in high-temperature shift reactor 133
Fig. 5.26 Open-loop methanator outlet temperature profile for the ammonia process under a decrease of catalyst activity from 1 to 0.2 within 300 s in the high-temperature shift reactor 133
Fig. 5.27 Closed-loop **a** outlet temperature and **b** inlet temperature profiles of the high-temperature shift reactor using the proposed MPC and Safeness Index-based MPC for C_1 and C_2, respectively 139

Fig. 5.28 Closed-loop **a** outlet temperature and **b** inlet temperature profiles of the methanator using the proposed MPC and Safeness Index-based MPC for C_1 and C_2, respectively 139
Fig. 5.29 Closed-loop **a** outlet mole fraction of carbon monoxide of the methanator, and **b** Safeness Index profiles using the proposed MPC and Safeness Index-based MPC for C_1 and C_2, respectively, where the solid line is the actual process threshold, and the dashed line is the threshold used in the controller 139
Fig. 5.30 Methanator outlet temperature profiles under C_2 only, and under both C_1 and C_2 140
Fig. 5.31 Comparison of methanator outlet temperature under MPC (both C_1 and C_2) and under PI (both C_1 and C_2) control schemes 141
Fig. 5.32 Methanator outlet temperature profiles under the MPC with and without Safeness Index constraints 142
Fig. 6.1 A recurrent neural network (left) and its unfolded structure (right), where x, u, o, and Θ are the input vector, the state vector, the output vector, and the weight matrix, respectively 147
Fig. 6.2 The top figure shows the discretization of the operating region Ω_ρ for open-loop simulations with initial conditions $x_0 \in \Omega_\rho$, and the bottom figure shows the data processing step for the RNNs with a prediction horizon of P_{nn}. Ω_ρ and $\Omega_{\hat{\rho}}$ are the closed-loop stability region for the actual nonlinear system of Eq. 6.1, and the RNN model, respectively 152
Fig. 6.3 A schematic of the implementation of ensemble learning method based on k-fold cross validation, where $u \in \mathbf{R}^m$ and $x \in \mathbf{R}^n$ are the input vector, and the state vector, respectively, and H_1, H_2 are the number of neurons in the two hidden layers 155
Fig. 6.4 Parallel computation of the ensemble of RNN models in CLBF-MPC, where $u^g(t_k)$ represents the guess of control action sent to the RNN models 171
Fig. 6.5 Evolution of CLBF $W_c(x)$ (blue trajectory) under the CLBF-MPC of Eq. 6.34 with error-triggered condition of Eq. 6.37 and event-triggered condition of Eq. 6.35, where the threshold lines in Eq. 6.35 are represented by the dashed lines with the slope $-\varepsilon_w$ 174
Fig. 6.6 The state-space profiles for the open-loop simulation using the first-principles model of Eq. 6.40 and the RNN model, respectively, for various sets of inputs and initial conditions (marked as blue stars) x_0 in the operating region 179

Fig. 6.7 State trajectories for the closed-loop CSTR of Eq. 6.40 under the CLBF-MPC using an ensemble of RNN models. The gray area on the top represents the set of unbounded unsafe states $\mathscr{D}_u$, and the circles represent the initial conditions . . . 180

Fig. 6.8 State trajectories for the closed-loop system of Eq. 6.40 under the CLBF-MPC using an ensemble of RNN models. The gray area embedded within $\mathscr{U}_{\hat{\rho}}$ represents the set of bounded unsafe states, and the circles represent the initial conditions . . . 181

Fig. 6.9 State trajectories for the closed-loop CSTR system the CLBF-MPC using a linear state-space model. The gray ellipse in state-space represents the set of bounded unsafe states $\mathscr{D}_b$, and the circles represent the initial conditions . . . 183

Fig. 6.10 Closed-loop state trajectories under the CLBF-MPC using an ensemble of RNN models (solid trajectory) and a linear state-space model (dashed trajectory), respectively. The gray ellipse in state-space represents the set of bounded unsafe states $\mathscr{D}_b$, and the circles represent the initial conditions . . . 183

Fig. 6.11 The state-space profiles for the closed-loop CSTR subject to time-varying disturbances under the CLBF-MPC of Eq. 6.34 with (red trajectory) and without online RNN update (blue trajectory), respectively, for an initial condition (−1.5,70) . . . 184

Fig. 6.12 Manipulated input profiles ($u_1 = \Delta C_{A0}$, $u_2 = \Delta Q$) for the closed-loop CSTR subject to time-varying disturbances under the CLBF-MPC of Eq. 6.34 with (red profile) and without online RNN update (blue profile), respectively, for an initial condition (−1.5,70) . . . 185

Fig. 6.13 Value of $E_{rnn}(t)$ at each sampling time for the closed-loop CSTR subject to time-varying disturbances under the CLBF-MPC of Eq. 6.34 with (red, right y-axis) and without online RNN update (blue, left y-axis), respectively, where the threshold E_T is set to 0.15 (dashed horizontal line corresponding to the right y-axis) . . . 185

Fig. 6.14 State trajectories for the closed-loop system of Eq. 6.40 within one operating period under LEMPC and CLBF-EMPC, respectively, where the gray area on the top of $\mathscr{U}_\rho$ represents the unbounded set of unsafe states $\mathscr{D}_u$, and the initial condition is (0, 0) . . . 192

Fig. 6.15 Closed-loop state trajectories for the system of Eq. 6.40 within four operating periods under CLBF-EMPC and LEMPC, respectively, where the initial condition is (0, 0) and the unbounded set of unsafe states $\mathscr{D}_u$ is the gray area on the top of $\mathscr{U}_\rho$ 193

Fig. 6.16 Input profiles for the closed-loop system of Eq. 6.40 within four operating periods under CLBF-EMPC, where the unsafe region is the gray area on the top of $\mathscr{U}_\rho$ 194

Fig. 6.17 Closed-loop state trajectories for the system of Eq. 6.40 within four operating periods under CLBF-EMPC and LEMPC, respectively, where the initial condition is (0, 0) and the bounded set of unsafe states $\mathscr{D}_b$ is embedded within $\mathscr{U}_\rho$ 195

Fig. 6.18 Input profiles for the closed-loop system of Eq. 6.40 within four operating periods under CLBF-EMPC, where the bounded set of unsafe states $\mathscr{D}_b$ is embedded within $\mathscr{U}_\rho$ 195

Fig. 6.19 The state-space profiles for the closed-loop CSTR subject to time-varying disturbances under CLBF-EMPC with (red trajectory) and without online RNN update (blue trajectory), respectively, for an initial condition (0,0) 196

Fig. 6.20 The state-space profiles for the closed-loop CSTR subject to time-varying disturbances under CLBF-EMPC with (red trajectory) and without online RNN update (blue trajectory), respectively, for two consecutive operating periods with an initial condition (0,0) 197

Fig. 6.21 Manipulated input profiles ($u_1 = \Delta C_{A0}$, $u_2 = \Delta Q$) for the closed-loop CSTR subject to time-varying disturbances under CLBF-EMPC with (red trajectory) and without online RNN update (blue trajectory), respectively, for two consecutive operating periods with an initial condition (0,0) 197

Fig. 6.22 Value of $E_{rnn}(t)$ at each sampling time for the closed-loop CSTR subject to time-varying disturbances under CLBF-EMPC with and without online RNN update, respectively, where the threshold E_T is set to 0.15 198

Fig. 7.1 A two-hidden-layer feedforward neural network structure with inputs $p(\bar{x})$ being a nonlinear function of state measurements within the detection window N_T, and output being the probability of each class label that indicates the status and/or type of cyber-attack 212

Fig. 7.2 The sliding detection window with a length of N_s, where D_i is the indicator for the detection triggered every N_a sampling steps 216

Fig. 7.3 Basic structure of the proposed integrated NN-based detection and LMPC control method . . . 218

Fig. 7.4 A schematic showing an example state trajectory under the integrated cyber-attack detection and control scheme . . . 219

Fig. 7.5 Logic flowchart showing the implementation steps of the attack-resilient operation of LEMPC that combines open-loop and closed-loop control actions together for the system operated in a secure region $\Omega_{\rho_{\text{secure}}}$ . . . 221

Fig. 7.6 Structures of recurrent neural network (left) and of a restruction window (right), where the input vectors are $\bar{x}$, u, the output vector is x, and f_{NN} represents the hidden neurons that incorporate nonlinear activation functions . . . 222

Fig. 7.7 Evolution of measured process states within one material constraint period under resilient LEMPC (blue trajectory) and under LEMPC (red trajectory) . . . 229

Fig. 7.8 Evolution of attacked state measurements (yellow trajectories) and true process states over one material constraint period under resilient LEMPC (red trajectories) and under LEMPC (blue trajectories) when **a** min-max, **b** geometric, **c** replay, and **d** surge attacks are targeting the temperature sensor, where the dashed ellipse is $\Omega_{\rho_{\text{secure}}}$ and the dash-dotted ellipse is the stability region Ω_ρ . . . 231

Fig. 7.9 Time-derivative of the reaction rate r_B of Eq. 7.27 based on measured process states over one material constraint period, when the temperature sensor is under no attack, and under min-max, geometric, replay, and surge attacks, respectively . . . 233

Fig. 7.10 Evolution of attacked state measurements (red trajectories) and true process states (blue trajectories) over two material constraint periods under the resilient LEMPC when **a** min-max, **b** geometric, and **c** surge attacks, targeting the temperature sensor are successfully detected by a NN detector at the end of the first material constraint period, $t = 0.06$ h, where the dashed ellipse is $\Omega_{\rho_{\text{secure}}}$ and the dash-dotted ellipse is the stability region Ω_ρ . . . 235

Fig. 7.11 **a** State-space trajectories, and **b** closed-loop profiles of reconstructed state (marked by colored circles), measured state (red), and true state (blue) for the CSTR system of Eq. 7.26 under LEMPC when the temperature sensor is attacked by a min-max cyber-attack at $t = 0.05$ h . . . 237

Fig. 7.12 **a** State-space trajectories, and **b** closed-loop profiles of reconstructed state (marked by colored circles), measured state (red), and true state (blue) for the CSTR system of Eq. 7.26 under LEMPC when the temperature sensor is attacked by surge cyber-attacks at $t = 0.03$ h, $t = 0.21$ h, and $t = 0.36$ h 238

Fig. 7.13 **a** State-space trajectories, and **b** closed-loop profiles of reconstructed state (marked by colored circles), measured state (red), and true state (blue) for the CSTR system of Eq. 7.26 under LEMPC when the temperature sensor is attacked by geometric cyber-attacks at $t = 0.03$ h, $t = 0.21$ h, and $t = 0.36$ h 239

Fig. 8.1 Two-tier control-detector architecture with the upper-tier controller (i.e., MPC) using both networked and continuous (secure) sensor measurements, and the lower-tier controllers using only continuous (secure) sensor measurements, where the networked sensors are vulnerable to cyber-attacks 246

Fig. 8.2 Schematic of the reactor-reactor-separator process with two CSTRs and a flash drum separator 252

Fig. 8.3 Measured and true state values (in deviation variable form) of x_{A1} when **a** min-max, **b** replay, **c** geometric, and **d** surge cyber-attacks are added on the sensor measurement of concentration x_{A1} at 3.22 h, and no detection or mitigation mechanisms are used 260

Fig. 8.4 Profiles of true process states when all 9 state measurement sensors are attacked at 3.22 h by min-max cyber-attacks, and no detection or reconfiguration of the two-tier control architecture are implemented 261

Fig. 8.5 Profiles of true process states when the six sensors of mass fraction are attacked at 3.22 h by min-max cyber-attacks; the attacks are detected at 3.28 h, and the process is re-stabilized at the steady-state by turning off upper-tier LMPC and using lower-tier PIs 262

Fig. 8.6 Profiles of true process states when the six sensors of mass fraction are attacked at 3.22 h by replay cyber-attacks; the attacks are detected at 3.28 h, and the process is re-stabilized at the steady-state by turning off upper-tier LMPC and using lower-tier PIs 263

Fig. 8.7 Profiles of true process states when the six sensors of mass fraction are attacked at 3.22 h by geometric cyber-attacks; the attacks are detected at 3.28 h, and the process is re-stabilized at the steady-state by turning off upper-tier LMPC and using lower-tier PIs 264

Fig. 8.8 Profiles of true process states when the six sensors of mass fraction are attacked at 3.22 h by surge cyber-attacks; the attacks are detected at 3.28 h, and the process is re-stabilized at the steady-state by turning off upper-tier LMPC and using lower-tier PIs 265

List of Tables

Table 1.1 Process parameters of the CSTR 8
Table 4.1 Parameter values of the CSTR with a first-order reaction 79
Table 5.1 Parameter values for the CSTR with MIC reaction 97
Table 5.2 Parameter values of the empirical model of Eq. 5.5 when the pressure relief valve is open and closed, respectively 108
Table 5.3 Parameter values of a PI temperature controller for the cases when the relief valve is open and closed, respectively 109
Table 5.4 Parameter values of the ammonia process simulation 124
Table 6.1 Parameter values of the CSTR system 178
Table 7.1 Detection accuracies of NN detectors in response to different types of cyber-attacks 234
Table 8.1 Descriptions and values of process parameters. 255

Chapter 1
Introduction

1.1 Motivation

Process operational safety has been a long-standing research problem in optimal operation and control of dynamic systems and processes. The traditional approach to process operational safety is to employ a hierarchical approach as shown in Fig. 1.1. Specifically, a complete control and safety system used in industries includes basic process control systems (BPCSs), alarm systems, emergency shutdown systems (ESSs), and safety relief devices. Ideally, BPCS regulates process variables to their set-points, while the layers of the safety system should not be activated regularly. When the BPCS fails to maintain the process variables within acceptable ranges due to, for example, equipment faults or unusually large process disturbances, alarms are triggered that alert operators so that actions can be taken to prevent further unsafe deviations. If the process variables subsequently further exceed allowable values, the ESS is triggered, which takes automatic and extreme actions such as forcing a valve to its fully open position to bring the process to a safer state of operation. Safety relief devices such as relief valves are used on vessels that can become highly pressurized quickly to prevent an explosion. Containments are used to prevent hazardous materials from entering the environment or injuring workers when the other layers of the safety hierarchy fail to prevent the release of the materials. The emergency response plan is used in severe cases that cannot be mitigated by any other layers. The layers are independent of each other and of the control system (i.e., they have separate sensors, computing elements, and actuators) to allow redundancy and improve safety [119]. Design decisions for the location and sizing of the safety systems are aided through qualitative and quantitative studies (e.g., hazards and operability (HAZOP) studies, fault trees, event trees, what-if or worst-case scenarios, security indices, and layers of protection analysis (LOPA)) of the damage that may result from an accident (including life losses, capital equipment loss, and damage to the environment) which is evaluated to determine whether it is within an acceptable level of risk [55, 119, 125, 199].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

Z. Wu and P. D. Christofides, *Process Operational Safety and Cybersecurity*,
Advances in Industrial Control, https://doi.org/10.1007/978-3-030-71183-2_1

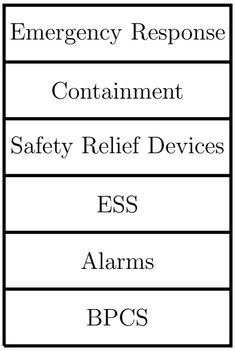

Fig. 1.1 Control/safety system layers [119]

Though safety systems and feedback control systems are critical to safe plant operation, they act fully independently in the hierarchical multilevel system of Fig. 1.1 and are not integrated to yield cooperative actions to ensure both operational safety and economic performance. This has resulted in staggering profit losses for the chemical process industries; for example, it was reported that the 20 major accidents in the hydrocarbon industry from 1974 to 2015 cost over $15 billion, with the total accumulated value of the 100 largest losses at more than $33 billion (estimates in 2015 dollars) [121]. It is clear from these numbers that it is necessary to coordinate the actions of process safety and control systems from both the ethical perspective of saving lives and property, and also from an economics standpoint for the chemical process industry. One potential solution is to incorporate safety considerations and safety system actions within optimization-based control schemes, e.g., model predictive control (MPC). While MPC has been widely used in real-time operation of industrial chemical plants to optimize chemical process performance accounting for closed-loop stability and control actuator constraints [66, 124, 130, 133, 160, 165], current MPC designs do not account for process safety considerations and actions and thus may lead to process operation in certain regions of the state space from which migration to an unsafe state may quickly occur. Therefore, a systematic methodology needs to be developed with rigorous analysis of process stability, operational safety, and recursive feasibility to coordinate MPC systems and safety systems to ensure operational safety while achieving desired operation performance.

In addition to process operational safety, cybersecurity has become crucially important in recent years due to increasing risks of cyber-attacks with the development of modern communication in industrial process controls and operations. Since both process safety and cybersecurity aim to prevent or mitigate events involving a loss of control of safety- and security-critical systems, the layers of protection analysis for safety systems can also be employed in the development of a defense-in-depth strategy for cyber-defense systems, where cybersecurity is incorporated into control network designs. Industrial control systems or supervisory control and data acquisition (SCADA) systems are generally large-scale, geographically dispersed, and life-critical systems in which embedded sensors, actuators, and controller networks are utilized to sense and control the physical devices [59]. The unsafe process operation due to the failure of cybersecurity can lead to catastrophic consequences in chemical process industries, causing environmental damage, capital loss, and human injuries. Cyber-attacks are essentially a series of computer actions that are designed to compromise the integrity, stability, and safety of control systems [58, 64, 152, 230]. Among cyber-attacks, targeted attacks are designed with the aim of modifying the control actions applied to an industrial process (for example, the Stuxnet worm was designed to attack the SCADA system by modifying the data sent to Programmable Logic Controllers [43]). Additionally, since targeted attacks are designed to be process and controller behavior aware and can have access to process operation information such as process state measurement, operating region, and control algorithms, they are stealthy and difficult to detect using conventional detection methods. Nevertheless, as the development of most of the existing detection methods still depends partly on human analysis, intelligent cyber-attacks that are process-aware and stealthy pose great challenges to the development of efficient detection methods with high detection accuracy for modern industrial control system where cyber- and physical components closely interact. Therefore, designing advanced detection systems and integrating them with MPC to handle cyber-attacks in safety-critical systems is a new frontier in control systems that will significantly improve the security of chemical production.

1.2 Background

Chemical process safety has traditionally been addressed through process design decisions (e.g., designing the process to be inherently safe in terms of its chemistry and physics [68, 77]) and control and safety system design decisions (e.g., adding sensors for critical process variables that trigger an alarm when a measurement outside of the desired range is obtained [119]). Inherently safer designs are achieved through four primary principles: minimize (reduce the quantity of hazardous substances used and stored by a process), substitute (utilize less hazardous process chemicals), moderate (dilute chemicals or change operating conditions), and simplify (choose designs with less complexity and less potential to create hazardous conditions when faults or errors occur) [71, 92]. However, it is not possible to eliminate all hazards at a plant, so a safety system, comprised of several independent layers, should be added (Fig. 1.1). While the hierarchical approach that utilizes control and safety systems independently for process safety has been successfully deployed in chemical process industries, the accidents throughout chemical plant history [96, 98, 117] have led some researchers to suggest that the philosophy used in the design of the control and safety system layers (i.e., designing barriers against specific unsafe scenarios using the safety system) is quite limited, particularly as economic considerations drive more optimized and integrated system designs [70, 75, 112, 140], and that a systems approach coordinating directly the actions of control and safety systems and analyzing closed-loop process operational safety should instead be used [7, 27, 54, 84, 109, 116, 195]. One step toward this systems approach is by incorporating safety considerations and safety system actions within the BPCS. However, the single-input/single-output controllers (e.g., proportional–integral–derivative controller (PID controller)) traditionally used within the BPCS cannot account for factors that are important to process safety such as multivariable interactions and state/input constraints. On the other hand, advanced model-based control methodologies such as model predictive control (MPC) can account for these factors and thus can be integrated with safety considerations [109, 124, 130, 160]. A large number of works in the MPC literature have addressed the robustness, performance, and closed-loop stability of MPC (e.g., [42, 62, 76, 82, 124, 128, 133, 146, 233] and the references therein), but have not considered explicit safety considerations and safety system actions in their formulations.

Several works have looked at coordinating control with safety considerations. For example, safety in the sense of fault/abnormality diagnosis and monitoring has been addressed, e.g., [53, 65, 197], as well as integrating fault tolerance within process control, e.g., [12, 35, 89, 105, 131, 229]; however, these methods do not address system-wide safety considerations and safety system actions in control. Furthermore, the coordination of control and safety systems through a system-wide safety metric (while operating the systems independently) has not been performed, though this has the potential to significantly reduce unnecessary triggering of the safety system and to help in the design of triggers and appropriate actions for automated elements of the ESS and relief systems. Thresholds on a recently developed state-based Safeness Index [8] may be incorporated as triggers for safety system activation that allow the safety system to be aware of system-level safety considerations; the same metric, with different thresholds, can be utilized in MPC design to provide some coordination between the designs. This can be particularly beneficial for mitigating alarm overloading [39, 69, 204], which is the triggering of too many alarms at once, either because of poor alarm design creating frequent alarms that require no operator actions, or too many correct alarms sounding at once triggered by the same root cause. The number of alarms that sound at a chemical process plant each day can be over seven times the recommended number [61, 172], making it difficult for operators to adequately address the alarms, which can lead to environment and plant damage, danger to lives [181, 184], and reduced operator confidence in the alarm system [204]. Industry [172] and academia [14, 20, 38, 44, 134, 137, 186, 203, 204] have addressed alarm issues with techniques based on, for example, models, statistical analysis, and metrics. Despite these efforts, the integration of operational safety considerations such as safeness metrics that characterize the safeness of chemical processes based on the values of the process states, as well as safety system actions (like on/off behavior of relief valves) within control system designs, has received limited attention.

Additionally, industrial process control systems rely heavily on information and communication technologies for automated operations. Particularly, industrial control systems integrate computers, data communications networks, and physical process components to seamlessly combine hardware and software resources for reliable operation and robust control. In more recent years, Internet communication and wireless networks are starting to replace or complement existing wired point-to-point communications in traditional large-scale process operations as well [49]. As these new developments bring efficiency to the existing system by enabling transmission of signals to remote locations without adding or altering the current hardwire infrastructure, heightened concern for security also arises [28]. Each device and communication channel in the control system network expand the possible attack surface that cyber-attacks can exploit, thereby increasing the vulnerability of the industrial cyber-physical system. Due to the connectivity and interaction between physical and cyber-components in these processes, a different strategy from the traditional information technology (IT) approaches is required for operational cybersecurity. Therefore, the design and implementation of cyber-defense in industrial control systems remain an ongoing scientific and practical issue. Moreover, with the increasing sophistication of attacks, they may lead to negative consequences beyond critical asset damage and the net economic loss of the system. Since the attackers may have full access to technical details of the process control system and production processes in the plant, process safety and operational integrity may also be compromised. In recent years, a number of industrial cyber-attacks have caused detrimental physical damage, for example, the Stuxnet worm compromising Iran's nuclear centrifuges, the 2014 cyber-attack attacking a German steel mill, and the 2015 cyber-attack compromising information systems of three energy distribution companies in Ukraine [94]. In light of conducting hazard analysis as part of standard process safety practice, there have been recent calls to incorporate cybersecurity-integrated hazard evaluations, where cyber-vulnerabilities in the production units are assessed and understood, and countermeasures are outlined to reduce these cyber-risks. However, at this stage, no systematic approach has been developed to actively monitor, detect, and mitigate the impact of these intrusions using the data network on the digital platform. Considering this gap, developing detection algorithms and mitigation measures from within the control system is fundamental to addressing the problem.

Recent IT developments such as enhancement of firewalls for guarding network security have given an edge to enterprise cybersecurity. As a huge amount of operational and instrumentation data is generated, collected and archived for process monitoring, control, and troubleshooting in production plants, safeguarding methodologies such as big data analytics may also be used to secure device measurements for safe process operation. With the rapid development of computing power and digital technologies, the potential application of these data goes beyond fault detection and preventative maintenance. One example usage of these process operational data is to detect and predict cyber-attacks in the industrial control systems. In recent years, cybersecurity and cyber-defense have garnered increasing research interests with the rise of virtualization and big data [26, 57, 99], where machine learning techniques that can learn the system pattern from big data provide a powerful tool to analyze industrial process data for the development of cyber-attack detection algorithms. In fact, machine learning has increasingly gained more popularity in classical engineering fields in addition to computer science and engineering [11, 30, 159, 161, 166, 177, 196, 211], and has shown promising potential for use in the detection of cyber-attacks. For example, [136] proposed a model-based fault diagnostic method for fault diagnosis and classification in electric drives, and [208] used hidden Markov models for automated fault detection and diagnosis of heating, ventilation, and air conditioning (HVAC) systems. Additionally, in [78], various machine learning classification methods were used to distinguish cyber-attacks on power systems from process disturbances, and in [86], a behavior-based intrusion detection algorithm was developed to identify the types of attacks. Moreover, an extensive literature review of machine learning methods deployed for attack detection are presented in [40, 147, 173, 192, 209, 236]. While the feasibility of data science and machine learning algorithms in anomaly management has been demonstrated in these recent literature contributions, the development of a protective safeguard through the integration of online machine-learning-based detection algorithms and existing advanced control techniques such as MPC to the multi-layer cyber-defense system that is of significant importance to next-generation smart manufacturing is still in its infancy.

1.3 Operational Safety and Cybersecurity of Chemical Processes

A chemical process example is presented in this section to provide the motivation for developing novel control algorithms that account for operational safety and cybersecurity. In the first case study, the chemical process is operated in an off steady-state manner under economic model predictive control (EMPC) to optimize process economic performance. While the formal definition of EMPC will not be presented until the subsequent chapters, we can think of EMPC as a predictive control scheme that optimizes operating strategy in real time to dynamically operate chemical processes in a bounded operating region in order to maximize process economic benefits accounting for various economic factors such as time-varying material and energy pricing. However, in the case that the economically optimal regions include unsafe operating conditions, the time-varying operation of EMPC without accounting for safety region constraints may lead to unsafe operations when attempting to maximize process economic profits. The second case study considers the same chemical process and demonstrates the impact of cyber-attacks that compromise one of the sensor measurements. Specifically, the system is normally operated at a pre-specified steady-state (either originally at the steady-state or forced to the steady-state from another operating condition) under feedback-based tracking model predictive control (MPC) with secure sensor measurements of process variables, e.g., temperature and species concentration; however, it will be demonstrated that process stability is no longer guaranteed in the sense that the system may deviate from the steady-state and even leave the normal operating region when sensor measurements are tampered by cyber-attacks. The two case studies indicate the importance of having advanced control systems that account for process operational safety and cybersecurity, and have motivated much of the work contained in this book. The chemical process example and the two case studies are provided below.