Chapter 4
Enhancing Cyber-Physical System Resilience With Safe Data-Driven Control Strategies

Muhammad Usman Tariq
https://orcid.org/0000-0002-7605-3040
Abu Dhabi University, UAE & University College Cork, Ireland

ABSTRACT

This chapter explores strategies for enhancing the resilience of Cyber-Physical Systems (CPS) through safe and data-driven control mechanisms. As CPS become increasingly reliant on artificial intelligence (AI) and machine learning (ML) for real-time decision-making, ensuring system safety, security, and reliability becomes a critical challenge. The chapter examines various AI-powered control techniques, including Model Predictive Control (MPC), reinforcement learning, and anomaly detection, to optimize system performance while mitigating risks such as adversarial attacks, biases, and unpredictability. Additionally, it highlights the role of edge computing and distributed control architectures in reducing latency and improving fault tolerance. The chapter also addresses cybersecurity threats that impact CPS, including data breaches, cyberattacks, and network vulnerabilities.

INTRODUCTION

Cyber-Physical Systems (CPS) fuse computational procedures with operational procedures. Physical parts function with software programs in these systems which experience system behaviour control through real-world actions as well as computer-

DOI: 10.4018/979-8-3373-1832-5.ch004

based choices. CPS appears as autonomous vehicles, smart grids, industrial robots, medical devices along with Internet of Things (IoT) networks and additional critical examples. Technological systems are becoming prevalent, so their design methods and system maintenance directly impact the operational safety of both physical elements and mathematical components (Aghazadeh Ardebili & Andronie, 2025). CPS describes the necessity of establishing secure control mechanisms as its essential security focus point. The real-time operation of CPS includes physical components meeting complex algorithms which normally function without significant human control. Such tight physical-cyber integration leads to higher failure probabilities together with various possible malicious threat situations. In 2010 Stuxnet malware delivered a direct assault on the supervisory control and data acquisition (SCADA) system that operated Iranian uranium enrichment centrifuges. The malicious software controlled physical equipment operations discreetly as part of standard system activities. The incident demonstrated the harmful consequences of unsecure CPS environments because unidentified system failures could lead to monetary damages and threaten human existence (Gao et al., 2023). Protecting people from such risks becomes absolutely essential for achieving safe operations in CPS. Safety-critical environments represent many of the physical elements found in CPS operations including health services and transport systems and industrial production facilities. Catastrophic results emerge from all security failures and breaches in these critical operational environments. Consider autonomous vehicles, for instance. Autonomous vehicles adopting faulty control systems could generate incidents which lead to vehicle accidents along with injuries and death of occupants. A vehicle needs its communication systems with traffic control along with navigation to be protected against cyber threats (Aghazadeh Ardebili & Andronie, 2025).

Safety and security needs in CPS control systems can be achieved through careful implementation of cybersecurity protocols as well as fault-tolerant algorithms alongside real-time monitoring systems. The technical development of these systems should protect against malicious cyber threats together with protecting against unintentional failures stemming from system overload or environmental conditions (Gao et al., 2023). Data-driven methodologies show promise as a method of enhancing system resilience while increasing robustness in CPS designs. The development of CPS depends on non-stop data acquisition which combines sensor analytics with cyber system analysis to anticipate system evolutions through monitoring capabilities. Machine learning algorithms together with statistical methods and big data analytics enable data-driven methods to detect potential threats as well as system failures and performance anomalies and warn about catastrophic events before their occurrence. The early alert system allows operators to conduct maintenance operations before breakdowns emerge thus improving system operational reliability while ensuring safety measures (Aghazadeh Ardebili & Andronie, 2025). Data-driven techniques

A Bibliometric Analysis of Artificial Intelligence Applications in Global Higher Education

Ming Liand Mohd Isa Rohayati (2025). *International Journal of Information System Modeling and Design (pp. 1-24).*

www.irma-international.org/article/a-bibliometric-analysis-of-artificial-intelligence-applications-in-global-higher-education/365913