Lecture Notes in Networks and Systems 531

Pablo García Bringas · Hilde Pérez García ·
Francisco Javier Martinez-de-Pison ·
José Ramón Villar Flecha · Alicia Troncoso Lora ·
Enrique A. de la Cal · Álvaro Herrero ·
Francisco Martínez Álvarez · Giuseppe Psaila ·
Héctor Quintián · Emilio S. Corchado Rodriguez *Editors*

17th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2022)

Salamanca, Spain, September 5–7, 2022, Proceedings

Springer

Lecture Notes in Networks and Systems

Volume 531

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

More information about this series at https://link.springer.com/bookseries/15179

Pablo García Bringas · Hilde Pérez García ·
Francisco Javier Martinez-de-Pison ·
José Ramón Villar Flecha ·
Alicia Troncoso Lora · Enrique A. de la Cal ·
Álvaro Herrero · Francisco Martínez Álvarez ·
Giuseppe Psaila · Héctor Quintián ·
Emilio S. Corchado Rodriguez
Editors

17th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2022)

Salamanca, Spain, September 5–7, 2022
Proceedings

Springer

International Conference on
SOCO
Soft Computing Models in Industrial and Environmental Applications

Editors
Pablo García Bringas
Faculty of Engineering
University of Deusto
Bilbao, Spain

Francisco Javier Martinez-de-Pison
Mechanical Engineering Department
University of La Rioja
Logroño, La Rioja, Spain

Alicia Troncoso Lora
Data Science and Big Data Lab
Pablo de Olavide University
Sevilla, Spain

Álvaro Herrero
Department of Civil Engineering
University of Burgos
Burgos, Spain

Giuseppe Psaila
DIGIP
University of Bergamo
Dalmine, Bergamo, Italy

Emilio S. Corchado Rodriguez
Department of Computing Science
University of Salamanca
Salamanca, Spain

Hilde Pérez García
University of León
León, Spain

José Ramón Villar Flecha
Inteligencia Artificial
University of Oviedo
A Coruña, La Coruña, Spain

Enrique A. de la Cal
University of Oviedo
Oviedo, Spain

Francisco Martínez Álvarez
School of Engineering
Pablo Olavide University
Seville, Spain

Héctor Quintián
Department of Industrial Engineering
University of A Coruña
Ferrol, Spain

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-3-031-18049-1 ISBN 978-3-031-18050-7 (eBook)
https://doi.org/10.1007/978-3-031-18050-7

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

This volume of Lecture Notes in Networks and Systems contains accepted papers presented at the *17th International Conference on Soft Computing Models in Industrial and Environmental Applications* (SOCO 2022). This conference was held in the beautiful city of Salamanca, Spain, in September 2022.

Soft computing represents a collection or set of computational techniques in machine learning, computer science, and some engineering disciplines, which investigate, simulate, and analyze very complex issues and phenomena.

After a peer-review process, the SOCO 2022 International Program Committee selected 64 papers published in these conference proceedings, representing an acceptance rate of 60%. In this relevant edition, a particular emphasis was put on the organization of special sessions. Seven special sessions were organized related to relevant topics such as Machine Learning and Computer Vision in Industry 4.0; Time Series Forecasting in Industrial and Environmental Applications; Optimization, Modeling, and Control by Soft Computing Techniques; Soft Computing Applied to Renewable Energy Systems; Preprocessing Big Data in Machine Learning; and Tackling Real-World Problems with Artificial Intelligence.

The selection of papers was extremely rigorous to maintain the high quality of the conference. We want to thank the members of the Program Committees for their hard work during the reviewing process. This is a crucial process for creating a high-standard conference; the SOCO conference would not exist without their help.

SOCO 2022 enjoyed outstanding keynote speeches by distinguished guest speakers: Prof. Ajith Abraham, Director of Machine Intelligence Research Labs (MIR Labs), and Prof. Guy De Tré head of the research group on Database, Document, and Content Management (DDCM) at Ghent University (Belgium), and Felix Barrio General Director at INCIBE (Spain).

SOCO 2022 has teamed up with “Neurocomputing” (Elsevier), “Logic Journal of the IGPL” (Oxford University Press), and Cybernetics & Systems (Taylor & Francis) for a suite of special issues, including selected papers from SOCO 2022.

Particular thanks go as well to the conference’s main sponsors, Startup Olé, the CYL-HUB project financed with next-generation funds from the European Union; the Ministry of Labor and Social Economy; the Recovery, Transformation, and

Resilience Plan; and the State Public Employment Service, channeled through the Junta de Castilla y León, BISITE research group at the University of Salamanca, CTC research group at the University of A Coruña, and the University of Salamanca. They jointly contributed in an active and constructive manner to the success of this initiative.

We would like to thank all the special session organizers, contributing authors, as well as the members of the Program Committees and the Local Organizing Committee for their hard and highly valuable work. Their work has helped to contribute to the success of the SOCO 2022 event.

September 2022

Pablo García Bringas
Hilde Pérez García
Francisco Javier Martinez-de-Pison
José Ramón Villar Flecha
Alicia Troncoso Lora
Enrique A. de la Cal
Álvaro Herrero
Francisco Martínez Álvarez
Giuseppe Psaila
Héctor Quintián
Emilio S. Corchado Rodriguez

Organization

General Chair

Emilio Corchado	University of Salamanca, Spain

International Advisory Committee

Ashraf Saad	Armstrong Atlantic State University, USA
Amy Neustein	Linguistic Technology Systems, USA
Ajith Abraham	Machine Intelligence Research Labs—MIR Labs, Europe
Jon G. Hall	The Open University, UK
Paulo Novais	Universidade do Minho, Portugal
Amparo Alonso Betanzos	President Spanish Association for Artificial Intelligence (AEPIA), Spain
Michael Gabbay	King's College London, UK
Aditya Ghose	University of Wollongong, Australia
Saeid Nahavandi	Deakin University, Australia
Henri Pierreval	LIMOS UMR CNRS 6158 IFMA, France

Program Committee Chairs

Pablo García Bringas	University of Deusto, Spain
Hilde Pérez García	University of León, Spain
Francisco Javier Martínez de Pisón	University of La Rioja, Spain
José Ramón Villar Flecha	University of Oviedo, Spain
Alicia Troncoso Lora	Pablo Olavide University, Spain
Enrique A. de la Cal	University of Oviedo, Spain
Álvaro Herrero	University of Burgos, Spain
Francisco Martínez Álvarez	Pablo Olavide University, Spain
Giuseppe Psaila	University of Bergamo, Italy

Héctor Quintián	University of A Coruña, Spain
Emilio Corchado	University of Salamanca, Spain

Program Committee

Agustina Bouchet	University of Oviedo, Spain
Akemi Galvez-Tomida	University of Cantabria, Spain
Alfredo Jimenez	KEDGE Business School, Spain
Álvaro Herrero Cosio	University of Burgos, Spain
Álvaro Michelena Grandío	University of A Coruña, Spain
Andreea Vescan	Babes-Bolyai University, Cluj-Napoca, Romania
Andres Fuster-Guillo	University of Alicante, Spain
Andres Iglesias Prieto	University of Cantabria, Spain
Angel Arroyo	University of Burgos, Spain
Anna Bartkowiak	University of Wroclaw, Poland
Anna Kamińska-Chuchmała	Wrocław University of Technology, Poland
Anton Koval	Luleå University of Technology, Sweden
Antonio Bahamonde	University of Oviedo at Gijón, Spain
Antonio Sala	Polytechnique University of Valencia, Spain
Bartosz Krawczyk	Virginia Commonwealth University, USA
Beatriz De La Iglesia	University of East Anglia, UK
Bogdan Okreša Đurić	University of Zagreb, Croatia
Borja Sanz	University of Deusto, Spain
Carlos Cambra	University of Burgos, Spain
Carlos Pereira	ISEC, Portugal
Carmen Benavides	University of León, Spain
Damian Krenczyk	Silesian University of Technology, Poland
Daniel Honc	University of Pardubice, Czechia
Daniel Urda	University of Burgos, Spain
Daniela Perdukova	Technical University of Kosice, Slovakia
David Griol	University of Granada, Spain
Dragan Simic	University of Novi Sad, Serbia
Eduardo Solteiro Pires	UTAD University, Portugal
Eleni Mangina	UCD, Ireland
Eloy Irigoyen	University of the Basque Country, Spain
Enrique De La Cal Marín	University of Oviedo, Spain
Enrique Onieva	University of Deusto, Spain
Esteban Jove	University of A Coruña, Spain
Fernando Ribeiro	EST, Portugal
Fernando Sanchez Lasheras	University of Oviedo, Spain
Florentino Fdez-Riverola	University of Vigo, Spain
Francisco Martínez-Álvarez	Pablo de Olavide University, Spain
Francisco Zayas-Gato	University of A Coruña, Spain
Franjo Jovic	University of Osijek, Croatia

Giuseppe Psaila	University of Bergamo, Italy
Grzegorz Ćwikła	Silesian University of Technology, Poland
Hector Cogollos Adrián	University of Burgos, Spain
Héctor Quintián	University of A Coruña, Spain
Henri Pierreval	LIMOS-IFMA, France
Humberto Bustince	UPNA, Spain
Ioana Zelina	Technical University of Cluj-Napoca, North Center in Baia Mare, Romania
Isabel Sofia Sousa Brito	Polytechnic Institute of Beja, Portugal
Isaias Garcia	University of León, Spain
Jaroslav Marek	University of Pardubice, Czechia
Jaume Jordán	Polytechnique University of Valencia, Spain
Javier Díez-González	University of León, Spain
Javier Sanchis Saez	Polytechnique University of Valencia, Spain
Jesús D. Santos	University of Oviedo, Spain
Jiri Pospichal	University of Ss. Cyril and Methodius, Slovakia
Jorge Barbosa	ISEC, Portugal
Jorge García-Gutiérrez	University of Seville, Spain
Jose Carlos Metrolho	IPCB, Portugal
Jose Dorronsoro	Autonomous University of Madrid, Spain
José Francisco Torres Maldonado	Pablo de Olavide University, Spain
Jose Luis Calvo-Rolle	University of A Coruña, Spain
José Luis Casteleiro-Roca	University of A Coruña, Spain
Jose M. Molina	University Carlos III of Madrid, Spain
Jose Manuel Lopez-Guede	Basque Country University, Spain
José Ramón Villar	University of Oviedo, Spain
José Valente de Oliveira	University of Algarve, Portugal
Juan Albino Mendez	University of La Laguna, Spain
Juan Gomez Romero	University of Granada, Spain
Juan M. Alberola	Polytechnique University of Valencia, Spain
Julio César Puche Regaliza	University of Burgos, Spain
Laura Melgar-García	Pablo de Olavide University, Spain
Lidia Sánchez-González	Universidad de León, Spain
Luis Alfonso Fernández Serantes	FH-Joanneum University of Applied Sciences, Spain
Luis Paulo Reis	University of Porto, Portugal
Manuel Castejón-Limas	University of León, Spain
Manuel Graña	University of the Basque Country, Spain
Marcin Paprzycki	IBS PAN and WSM, Poland
Maria Fuente	University of Valladolid, Spain
Maria Teresa Godinho	Polytechnic Institute of Beja, Portugal
Matilde Santos	Complutense University of Madrid, Spain
Mehmet Emin Aydin	University of the West of England, UK
Michal Wozniak	Wroclaw University of Technology, Poland

Míriam Timiraos Díaz	University of A Coruña, Spain
Nashwa El-Bendary	Arab Academy for Science, Technology, and Maritime Transport, Egypt
Noelia Rico	University of Oviedo, Spain
Nuño Basurto	University of Burgos, Spain
Oscar Castillo	Tijuana Institute of Technology, Mexico
Ovidiu Cosma	Technical University of Cluj-Napoca, Romania
Pablo García Bringas	University of Deusto, Spain
Panagiotis Kyratsis	University of Western Macedonia, Greece
Paulo Moura Oliveira	UTAD University, Portugal
Pavel Skrabanek	Brno University of Technology, Czechia
Petr Dolezel	University of Pardubice, Czechia
Petrica Pop	Technical University of Cluj-Napoca, North University Center at Baia Mare, Romania
Qing Tan	Athabasca University, Canada, Canada
Reggie Davidrajuh	University of Stavanger, Norway
Robert Burduk	University Wroclaw, Poland
Rogério Dionísio	Polytechnic Institute of Castelo Branco, Portugal
Santiago Porras Alfonso	University of Burgos, Spain
Sebastian Saniuk	University of Zielona Gora, Poland
Stefano Pizzuti	Energy New Technologies and Sustainable Economic Development Agency (ENEA), Italy
Valeriu Manuel Ionescu	University of Pitesti, Romania
Vladimir Ilin	Fakultet Tehničkih Nauka, Serbia
Wei-Chiang Hong	Asia Eastern University of Science and Technology, Taiwan
Wilfried Elmenreich	Alpen-Adria-Universität Klagenfurt, Austria
Wojciech Bozejko	Wroclaw University of Technology, Poland
Zita Vale	GECAD—ISEP/IPP, Portugal
Andre D. L. Batako	Liverpool John Moores University, UK
Anna Burduk	Wroclaw University of Science and Technology, Poland
Antoon Bronselaer	University of Ghent, Belgium
Bożena Skołud	Silesian University of Technology, Poland
Gloria Bordogna	CNR IREA, Italy
Guy De Tré	University of Ghent, Belgium
Iker Pastor-López	University of Deusto, Spain
Javier Del Ser	University of the Basque Country, Spain
Javiwer Diaz	Aingura IoT, Spain
Katarzyna Antosz	Rzeszow University of Technology, Poland
Krzysztof Kalinowski	Silesian University of Technology, Poland
Marek Placzek	Silesian University of Technology, Poland

Pablo Garcia Bringas	University of Deusto, Spain
Paolo Fosci	University of Bergamo, Italy
Wojciech Bożejko	Wroclaw University of Science and Technology, Poland

Special Sessions

Machine Learning and Computer Vision in Industry 4.0

Program Committee

Enrique Dominguez (Organizer)	University of Málaga, Spain
Jose Garcia Rodriguez (Organizer)	University of Alicante, Spain
Ramón Moreno Jiménez (Organizer)	Grupo Antolin, Spain
Andres Fuster-Guillo	University of Alicante, Spain
Esteban José Palomo	University of Malaga, Spain
Ezequiel López-Rubio	University of Málaga, Spain
Jorge Azorín-López	University of Alicante, Spain
Jorge García-González	University of Málaga, Spain
Jose Luis Calvo-Rolle	University of A Coruña, Spain
Karl Thurnhofer-Hemsi	University of Málaga, Spain
Marcelo Saval-Calvo	University of Alicante, Spain
Miguel A. Molina-Cabello	University of Málaga, Spain
Miguel Cazorla	University of Alicante, Spain
Rafael M. Luque-Baena	University of Extremadura, Spain

Time Series Forecasting in Industrial and Environmental Applications

Program Committee

Federico Divina (Organizer)	Pablo de Olavide University, Spain
José F. Torres (Organizer)	Pablo de Olavide University, Spain
José Luis Vázquez Noguera (Organizer)	Universidad Nacional de Asunción, Paraguay
Mario Giacobini (Organizer)	University of Torino, Italy
Miguel García Torres (Organizer)	Pablo de Olavide University, Spain
Antonio Morales-Esteban	University of Seville, Spain

David Gutiérrez-Avilés	University of Seville, Spain
Diego Pedro Pinto Roa	Universidad Nacional de Asunción, Paraguay
Elvira Di Nardo	University of Torino, Italy
Jorge Reyes	NT2 Labs, Chile
José-Lázaro Amaro-Mellado	University of Seville, Spain
Laura Melgar-García	Pablo de Olavide University, Spain
Laura Sacerdote	University of Torino, Italy
Luís Filipe Domingues	Polytechnic Institute of Beja, Portugal
Manuel Jesús Jiménez Navarro	Pablo de Olavide University, Spain
Zeyar Aung	Khalifa University of Science and Technology, United Arab Emirates

Optimization, Modeling, and Control by Soft Computing Techniques

Program Committee

Ahmed Al-Jumaily (Organizer)	Auckland University of Technology, New Zealand
Eloy Irigoyen (Organizer)	University of the Basque Country, Spain
Jose Luis Calvo-Rolle (Organizer)	University of A Coruña, Spain
Maria Tomas-Rodriguez (Organizer)	University of London, UK
Matilde Santos Peñas (Organizer)	Complutense University of Madrid, Spain
Mikel Larrea Sukia (Organizer)	University of the Basque Country, Spain
Anna Burduk	Wrocław University of Technology, Poland
Antonio Javier Barragán	University of Huelva, Spain
Antonio Robles Alvarez	University of Oviedo, Spain
Antonio Sala	Polytechnique University of Valencia, Spain
Camelia-M. Pintea	Technical University of Cluj-Napoca, North University Center at Baia Mare, Romania
Davide Carneiro	Polytechnic Institute of Porto, Portugal
Eukene Imatz-Ojanguren	Tecnalia Research and Innovation, Spain
Fábio Silva	University of Minho, Portugal
Fernando Matia	Polytechnic University of Madrid, Spain
Ignacio Trojaola Bolinaga	IKERLAN, Spain
Javier Sanchis Saez	Polytechnique University of Valencia, Spain
Jesus Lozano	University of Extremadura, Spain
Jose Manuel Lopez-Guede	University of the Basque Country, Spain
Jose Luis Diez	Polytechnic University of Valencia, Spain

Juan Albino Mendez	University of La Laguna, Spain
Luciano Alonso	University of Cantabria, Spain
Luis Magdalena	Polytechnic University of Madrid, Spain
María José Pérez-Ilzarbe	UPNA, Spain
Pavel Brandstetter	VSB-Technical University of Ostrava, Czechia
Petr Dolezel	Polytechnique University of Valencia, Czechia
Ramon Vilanova	Autonomous University of Barcelona, Spain
Vicente Gomez-Garay	University of the Basque Country, Spain
Xabier Basogain Olabe	University of the Basque Country, Spain

Soft Computing Applied to Renewable Energy Systems

Program Committee

Fares M'Zoughi (Organizer)	University of the Basque Country, Spain
Jesus Enrique Sierra Garcia (Organizer)	University of Burgos, Spain
Matilde Santos Peñas (Organizer)	Complutense University of Madrid, Spain
Paweł Martynowicz (Organizer)	AGH University of Science and Technology, Poland
Payam Aboutalebi (Organizer)	University of the Basque Country, Spain
Asier Ibeas	Autonomous University of Barcelona, Spain
Hugo Diaz-Martínez	University of Lisbon, Portugal
Izaskun Garrido	University of the Basque Country, Spain
Jesus Fernandez-Lozano	University of Málaga, Spain
Ravi Pandit	University of Exeter, UK

Preprocessing Big Data in Machine Learning

Program Committee

Antonio J. Tallón-Ballesteros (Organizer)	University of Huelva, Spain
Luís Cavique (Organizer)	University of Aberta, Portugal
Simon Fong (Organizer)	University of Macau, Macao
Akash Punhani	SRM Institute of Science and Technology, India
David Glass	University of Ulster, UK
Elsa Rodrigues	Polytechnique Institute of Beja, Portugal
Hamidah Jantan	Universiti Teknologi MARA, Malaysia
Marcin Szpyrka	AGH University of Science and Technology, Poland
María José Ginzo Villamayor	University of Santiago de Compostela, Spain
Mohamed Ali Hadj Taieb	University of Sfax, Tunisia

Tatsuo Nakajima	Waseda University, Japan
Antonio J. Tallón-Ballesteros	University of Huelva, Spain
Luís Cavique	University of Aberta, Portugal

Tackling Real-World Problems with Artificial Intelligence

Program Committee

Alberto Gallucci Suárez	University of Oviedo, Spain
Beatriz de la Iglesia	University of East Anglia, UK
Enol García González	University of Oviedo, Spain
Enrique De La Cal Marín	University of Oviedo, Spain
Fernando Moncada	University of Oviedo, Spain
José R. Villar	University of Oviedo, Spain
Mirko Fáñez	University of Oviedo, Spain
Noelia Rico	University of Oviedo, Spain
Paloma Valverde	Technological Institute of Castilla y León, Spain
Petrica Pop	Technical University of Cluj-Napoca, Romania
Samad Barri Khojasteh	University of Oviedo, Spain
Víctor Gonzalez	University of Oviedo, Spain
Víctor M. Álvarez	University of Oviedo, Spain

SOCO 2022 Organizing Committee Chairs

Emilio Corchado	University of Salamanca, Spain
Héctor Quintián	University of A Coruña, Spain

SOCO 2022 Organizing Committee

Álvaro Herrero Cosio	University of Burgos, Spain
Jose Luis Calvo-Rolle	University of A Coruña, Spain
Ángel Arroyo	University of Burgos, Spain
Daniel Urda	University of Burgos, Spain
Nuño Basurto	University of Burgos, Spain
Carlos Cambra	University of Burgos, Spain
Esteban Jove	University of A Coruña, Spain
José Luis Casteleiro-Roca	University of A Coruña, Spain
Francisco Zayas-Gato	University of A Coruña, Spain
Álvaro Michelena	University of A Coruña, Spain
Míriam Timiraos Díaz	University of A Coruña, Spain

Contents

Decision Support and Deep Learning

Evolutionary Computing

Neural Networks and Data Mining

Soft Computing Applications

Special Session on Machine Learning and Computer Vision in Industry 4.0

Special Session on Time Series Forecasting in Industrial and Environmental Applications

Special Session on Optimization, Modeling and Control by Soft Computing Techniques

Special Session on Soft Computing Applied to Renewable Energy Systems

Special Session on Pre-processing Big Data in Machine Learning

Special Session on Tackling Real World Problems with Artificial Intelligence

Decision Support and Deep Learning

Anomaly Detection of Security Threats to Cyber-Physical Systems: A Study

Nicholas Jeffrey[1](✉), Qing Tan[2], and José R. Villar[1]

[1] University of Oviedo, Oviedo, Spain
{uo292630,villarjose}@uniovi.es
[2] Athabasca University, Athabasca, Canada
qingt@athabasca.edu

Abstract. As the presence of Cyber-Physical Systems (CPS) becomes ubiquitous throughout all facets of modern society, malicious attacks by hostile actors have increased exponentially in recent years. Attacks on critical national infrastructure (CNI) such as oil pipelines or electrical power grids have become commonplace, as increased connectivity to the public internet increases the attack surface of CPS. This paper presents a study of the current academic literature describing the state of the art for anomaly detection of security threats to Cyber-Physical Systems, with a focus on life safety issues for industrial control networks (ICS), with the goal of improving the accuracy of anomaly detection. As a new contribution, this paper also identifies outstanding challenges in the field, and maps selected challenges to potential solutions and/or opportunities for further research.

Keywords: Cyber-physical systems security · IoT security · SCADA security · AI/ML in CPS · Human-in-the-loop cyber-physical systems (HitL-CPS) · Anomaly detection in CPS

1 Introduction

Cyber-Physical Systems (CPS) are integrated systems that combine software and physical components [1]. CPS have experienced exponential growth over the past decade, from fields as disparate as telemedicine, smart manufacturing, autonomous vehicles, Internet of Things, industrial control systems, smart power grids, remote laboratory environments, and many more. Academia tends to use the term Cyber-Physical System, while industry tends to use IoT for consumer-grade devices, and IIoT (Industrial Internet of Things) [2] for industrial control systems (manufacturing, process control, etc.).

The rapid growth [3] of CPS has outpaced advancements in cybersecurity, with new threat models and security challenges that lack a unified framework for secure design, malware resistance, and risk mitigations. Much of the attention from academia and industry is focused on consumer-grade IoT devices (smart home automation, etc.). Industrial-grade IoT seems to have less attention from academia and industry, which is unfortunate, as the consequences of IIoT failure are much higher (power grid failure, oil pipeline shutdowns, train switching, etc.) [4].

P. García Bringas et al. (Eds.): SOCO 2022, LNNS 531, pp. 3–12, 2023.
https://doi.org/10.1007/978-3-031-18050-7_1

Threat detection and prevention is a mature industry in enterprise networks, with large and entrenched vendors (Checkpoint, Cisco, F-Secure, Kapersky, Microsoft, Sophos, Trend Micro, etc.) providing host-based and network-based Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS). Cyber-Physical Systems do not yet have similar IDS/IPS capabilities [5].

Traditional Industrial Control Systems (ICS), also known as Supervisory Control and Data Acquisition (SCADA) have not adjusted to the ubiquitous connectivity of Industry 4.0 [7], and still largely consider security to be an afterthought [7]. Much of this is due to the (no longer accurate) assumption that the ICS/SCADA environment is on an isolated, air-gapped, and trusted network [8, 9]. Historically, the primary design goal of SCADA/ICS systems was extreme reliability and predictability. Basic cybersecurity practices such as complex passwords or onerous authentication requirements were seen as barriers to system accessibility and were therefore avoided by the designers and operators of these systems [8]. Anti-malware programs such as signature-based antivirus tools were similarly avoided, to eliminate the possibility of a false positive inadvertently quarantining critical system files. These historical systems typically ran on fully isolated and trusted networks, without connectivity to corporate networks, and definitely without any connectivity to the public Internet.

Additionally, the lack of standardization [10, 11] of historical SCADA/ICS systems resulted in widespread usage of proprietary communication protocols, leading to "security by obscurity" [12], due to lack of a robust method of peer review. System vendors typically lacked any method of providing updates or bug fixes, so newly discovered vulnerable systems would typically remain in place for the entire lifespan of the system, relying on network isolation for protection from threats. As modern CPS grew out of legacy SCADA/ICS systems, those historical design considerations became untenable, as connectivity to wireless networks became ubiquitous, as well as a rapid abandonment of isolated air-gapped network environments.

Legacy protocols used in SCADA/ICS (Modbus, DNP, Fieldbus, HART, etc.) [13] are increasingly giving way to TCP/IP used in CPS, largely driven by commercial motivations for connectivity to corporate computer networks and the Internet. The modern reality of CPS is a hyper-connected world where threat actors are omnipresent, and a hostile network environment must be assumed. As modern CPS become increasingly interconnected with other networks, the attack surface has increased exponentially, leading to increasingly frequent breaches of critical national infrastructure (CNI) such as oil pipelines [14], power grids [4], etc.

Due to historical design goals of SCADA/ICS, observability of system state [4] has typically been limited to the current real-time status of a particular sensor or actuator, with relatively simple threshold-based alerts for the system operator. The historical assumption of a SCADA/ICS running on an isolated and fully trusted network meant that intrusion detection and intrusion prevention (IDS/IPS) were not design priorities, leading to a lack of observability in the increasingly hostile network layer of the CPS, making it difficult to detect threats and malicious activity in an increasingly connected world. Anomaly detection of security threats to CPS has become more urgent and critical to industry and life safety, as CNI becomes increasingly interconnected to public networks. Therefore, further study is needed to advance the state of academic research on the issue, and to develop and apply preventative solutions for industry to ensure safe and secure implementations of CPS.

This study aims to gather a full understanding of the research issue, and to identify existing gaps in the current state of the art that are opportunities for further research efforts. The remainder of this paper is organized as follows; Sect. 2 provides a statistical analysis of the areas of coverage in existing literature, which will allow identification of gaps in the current research. Section 3 provides a literature analysis for key identified topics. Section 4 illustrates the currently outstanding challenges in the field, with potential solutions for advancing the state of art. Finally, Sect. 5 discusses the conclusions reached in this paper, as well as identifies opportunities for future research.

2 Statistical Analysis

The keywords described previously were used to search literature from the various described sources. A total of 310 papers and online articles were selected and reviewed for this study. As a study done by literature review, this section will provide statistical analysis to describe the existing research presented in the reviewed literature by publisher, publication type, publication year, and country of origin.

The top 5 publishers (IEEE 47%, ScienceDirect 15%, Springer 12%, ACM 9%, MDPI 4%, all others 13%) comprise the bulk of available research in this field and are all well-established academic publishers with robust levels of peer review and quality assurance.

Most of the research in this area is published in academic journals (59%), with academic conferences a close second (39%). The field of CPS security is also heavily influenced by industry, but those efforts are typically for short-term tactical responses to current market threats and opportunities. For competitive advantage and trade secret reasons, industry efforts are rarely shared with the broader community, with “security by obscurity” still a common tactic in industry. There is a noticeable lack of industry and academic collaboration in this field, which is an opportunity for improvement.

To maintain relevance in a rapidly changing field, the reviewed literature in this paper is within the last decade, with most articles from the past 3 years. The term “Cyber-Physical Systems” was coined in 2006 by the US-based National Science Foundation (NSF) [4], so little research exists before that date. Earlier research related to CPS existed in fields of cybernetics, industrial process control, and control logic and engineering.

The USA is the largest single source of research in the area, with the top 5 countries generating more research than all other countries combined. Of the top 5 countries, there are 3 countries (USA, UK, India) with English as an official language, making the overwhelming majority of the published research available in English, often to the exclusion of other languages. The remaining 2 countries in the top 5 (China and Germany) typically publish research in English as well, due to greater availability of reference literature and collaboration opportunities. China and Russia appear to be the only two countries with significant publications in local languages, perhaps due to the large sizes of their domestic industry and academic communities (Fig. 1, Fig. 2 and Fig. 3).

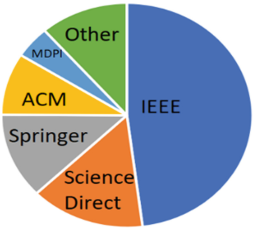

Fig. 1. Publishers

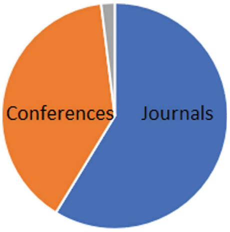

Fig. 2. Publication types

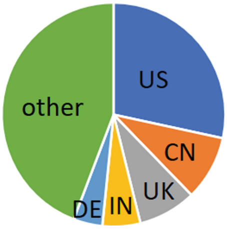

Fig. 3. Countries of Publication

3 Literature Analysis

Two of the commonly recurring themes in the available literature are CPS Security Design, and Anomaly Detection/Threat Detection in CPS, each of which will be discussed further below.

3.1 CPS Security Design

CPS is a broad field, and there is an interesting schism between the traditional SCADA systems used for industrial process control (now commonly referred to as IIoT), and the more consumer-focused IoT industry.

Due to product lifecycles measured in years or decades [15], and the historical design assumptions of operating in a fully trusted and air-gapped isolated environment, the traditional Industrial Control Systems (ICS) are much slower to adopt new technologies than their more agile counterparts in consumer-focused IoT devices that have product lifecycles measured in months to a few years.

Unlike their IIoT-based counterparts, the consumer-focused IoT industry was born in an age when ubiquitous connectivity to an increasingly hostile Internet was assumed, which helped drive adoption of standardized communication protocols around TCP/IP, with integrated authentication and encryption [16] functionality designed for the lightweight messaging protocols of devices assumed to have constrained processing power, battery life, and unreliable network connectivity.

Security design efforts for ICS/IIoT tend to focus on a hardened perimeter firewall separating the CPS from other networks, with little in the way of protection once inside the trusted network, reminiscent of the "hard shell, soft center" security posture of enterprise networks in decades past [17]. Due to historical design assumptions of a fully trusted network environment, there is still considerable resistance to actively blocking Intrusion Prevention Systems (IPS) being deployed with CPS, due to the high cost of false positives. Passive Intrusion Detection Systems (IDS) are seeing increasing acceptance in CPS, but due to the extreme heterogeneity, false positives are still a significant issue, making it difficult for the CPS operators to determine what is truly hostile network activity.

The more modern consumer-focused IoT industry has been quicker to adopt a zero-trust model of information security, accepting the reality that they operate in a potentially hostile network environment, and embedding strong authentication and encryption protocols by default [16]. Unfortunately, the rapid advancement of IoT means that product lifecycles are very short, making devices become obsolete quickly, leaving many "orphaned" devices without ongoing vendor support or upgrades to counter new security threats. While some vendors have included functionality for receiving trusted over-the-air updates to counter newly discovered threats, there are many IoT devices that entirely lack any sort of update functionality, leaving them permanently vulnerable to emerging threats.

Human-in-the-Loop Cyber-Physical Systems (HitL-CPS) are a unique subset of CPS that partially or completely rely on human operator input to control the CPS. This introduces unique security challenges, due to unpredictability from human error, inattentiveness, slower reaction time of humans, susceptibility to social engineering, inconsistent decision-making, etc. The key research in this area is from Nunes [18], who describes the most significant outstanding challenges in this area as gathering a full understanding of the problem domain, improvements in modeling unpredictable human behaviour, autonomic mitigations against intentional and unintentional human-introduced risks, and development of a formal methodology of integrating human feedback in the control loop. Each of these challenges are still in rapid states of development, so the maturity of this area of research is still in its early stages.

3.2 Anomaly Detection/Threat Detection in CPS

Threat detection methodologies can be broadly categorized [19] as signature-based, threshold-based, or behaviour-based. Traditional antivirus programs are an example of a signature-based threat detection methodology, using a centralized and regularly updated database of signatures of malicious files or traffic to trip an alarm on an IDS and/or IPS. Signature-based detection works well on IT networks thanks to standardized communication protocols and low levels of heterogeneity but suffers from high levels of false negatives on OT networks due to their proprietary communication protocols and heterogeneous physical components.

Threshold-based methodologies rely on known ranges of acceptable operation, which are relatively easy to define on IT networks. Examples of threshold-based threat detections for IT networks include network link utilization, communication latency, processor utilization levels, etc. However, OT networks have proven more difficult to accurately define known ranges of acceptable operation, due to real-world environmental fluctuations [20]. For example, a wireless mesh network of air quality sensors in a smart city environment may have communication latency impacted by fog or rain, making the thresholds of acceptable operation differ based on unpredictable weather conditions.

Kabiri and Chavoshi [20] propose a CPS design model that includes a inline hardware device that interrogates all commands sent to actuators, passively relaying all commands until a malicious or anomalous pattern is detected that would run the actuator outside of specified operational tolerances. This provides active protection of physical devices in OT networks, similar to inline IPS that are commonly used for protection of cyber assets in IT networks. IPS products suffer from false positives in IT networks due to complexity and unpredictability of traffic patterns. False positives have a higher impact in OT networks, due to financial implications of shutting down a CPS like a factory line or water treatment plant, so the tolerance for false positives is much lower in OT networks, which is still an outstanding research problem.

Behaviour-based methodologies are the most difficult to accurately define on IT networks and are even more challenging for OT networks [21]. Defining an accurate baseline of normal behaviour on an IT network requires a deep understanding of what normal system activity looks like, and it is rare that IT networks are completely unchanged over their entire lifecycle, making any definition of normal behaviour a moving target at best. These challenges are exacerbated on OT networks, which tend to be even more dynamic due to environmental factors such as weather-related variations in temperature, humidity, ambient light, etc. Additionally, the negative impact of a false positive or false negative detection on an OT network has more significant consequences, including physical equipment damage and life safety concerns.

There is considerable interest in the use of machine learning (ML) algorithms for automated threat detection in CPS, but few of the proposed frameworks from academia have seen significant adoption in industry. Due to the extreme diversity in CPS, it has proven difficult to generate a useful training model for AI/ML algorithms, which has resulted in unacceptably high levels of false positives and false negatives for automated anomaly detection. This appears to be a significant discontinuity between the efforts of academia and industry, and is an opportunity to improve collaboration.

Manufacturing processes in the so-called “Industry 4.0” have been particularly quick to adopt AI in CPS, both for protection from cybersecurity attacks, and operational efficiency. Alhaidari and AL-Dahasi [22] propose an improved framework for using AI to detect DDoS attacks using multiple machine learning algorithms. Different datasets were analyzed with ML algorithms for rapid detection of DDoS attacks, with preprocessing of raw data to minimize the size of the training model particularly helpful in increasing the mean time to detection of an attack. A significant conclusion drawn was the need for greater collaboration between the operators of individual CPS and broader industry participants for sharing of vulnerability information.

The major strategies, as well as their relative advantages and disadvantages are shown in the table below (Table 1).

Table 1. Comparison of anomaly detection strategies

Detection strategy	Advantages	Disadvantages
Signature	High accuracy for known threats	Wide variation in CPS makes it difficult to develop and maintain signature databases
Threshold	Simple design	External factors such as weather or operational changes can cause thresholds to vary over time, which can cause false positives
Behaviour	Best accuracy for unknown threats	Most difficult to accurately define

4 Outstanding Challenges

A modern CPS can be considered as a combination of corporate computer networks and industrial control networks, sometimes referred to as Information Technology (IT) and Operational Technology (OT), each of which have differing priorities.

Traditional IT networks have used the so-called Confidentiality, Integrity, Availability (CIA) triad to define the organizational security posture, with each facet listed in order of importance. OT networks reverse that order [23], with availability being the most important factor, followed by integrity, with confidentiality the least important facet of overall system security. This difference is largely due to CPS growing out of earlier SCADA/ICS networks used for industrial control processes, where availability was of the utmost importance, with integrity and confidentiality rarely considered due to usage of trusted and air-gapped isolated network environments.

As OT networks merged with IT networks to form modern CPS, those differing priorities have resulted in ongoing challenges that have yet to be fully resolved. IT networks heavily prioritize authentication (who you are) and authorization (what you are allowed to do), which roughly map to the confidentiality and integrity facets of the CIA triad of information security. However, OT networks have traditionally focused so heavily on the availability facet of the CIA triad, that authentication and authorization were assumed to be true [8] by virtue of physical access to the trusted and isolated OT network.

This historical assumption of a fully trusted and isolated environment is no longer true after the interconnection of IT and OT networks, resulting in vulnerability to common network-based attacks such as DDoS, MitM, replay attacks, impersonation, spoofing, false data injection, etc. Compounding the problem, OT networks typically lack integration with antimalware programs, as well as detailed logging capabilities, making it difficult to observe potentially hostile activity on OT networks [24].

There are ongoing efforts [12] to extend the IDS/IPS capabilities of IT networks into OT networks, but the lack of standardized protocols and interfaces to the physical components of CPS makes threat detection very challenging. Those IDS/IPS systems that have been extended into CPS environments struggle with high levels of false positives and false negatives, due to the complexity of CPS.

The single largest challenge facing the secure design and operation of CPS is their lack of standardized communication protocols and proprietary nature [25]. Due to the lack of even rough industry consensus for the system development life cycle of CPS, each system designer essentially builds each new CPS from scratch, without much consideration for multivendor interoperability, secure and robust patching mechanisms, or exposing system telemetry details in a consistent manner for health and security monitoring. This is slowly changing with industry consortiums forming standards bodies such as O-PAS (Open Process Automation Standard) [26], but broad industry consensus has proved elusive.

The highly proprietary nature of CPS products is due to their historical evolution from ICS, which were designed to operate on closed networks without interoperability or communication requirements with external networks. As OT and IT networks merged to become CPS, the open standards and communication protocols used by IT networks have been rapidly adopted by OT networks [27], but there is still significant opportunity for