An evaluation framework for industrial control system

International Journal of Critical Infrastructure Protection
36, 100487
DOI: 10.1016/j.ijcip.2021.100487

Citation Report

#	Article	IF	Citations
1	Cybersecurity Risk Assessment of Industrial Control Systems Based on Order-Î± Divergence Measures Under an Interval-Valued Intuitionistic Fuzzy Environment. IEEE Access, 2022, 10, 43751-43765.	4.2	3
2	Risk of cascading effects in digitalized process systems. Methods in Chemical Process Safety, 2022, , .	1.0	1
3	Memory forensics tools: a comparative analysis. Journal of Cyber Security Technology, 2022, 6, 149-173.	2.9	3
4	The Risk of Cyber Security for Power Stability Control System and Its Test Platform. , 2022, , .		1
5	Cybersecurity Analysis of Wind Farm Industrial Control System Based on Hierarchical Threat Analysis Model Framework. , 2022, , .		0
6	The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System. Electronics (Switzerland), 2023, 12, 591.	3.1	4
7	A Comparative Study of Time Series Anomaly Detection Models for Industrial Control Systems. Sensors, 2023, 23, 1310.	3.8	15
8	Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems, 2023, 7, 1-33.	2.5	2
9	A Mixed Clustering Approach for Real-Time Anomaly Detection. Applied Sciences (Switzerland), 2023, 13, 4151.	2.5	0
10	Time-Series Load Data Analysis for User Power Profiling. , 2023, , .		1
11	Overview of Network Security Defense Technologies for Power Systems. , 2022, , .		0
12	Real-Time Anomaly Detection with Subspace Periodic Clustering Approach. Applied Sciences (Switzerland), 2023, 13, 7382.	2.5	1
13	CAPTAIN: Community-based Advanced Persistent Threat Analysis in IT Networks. International Journal of Critical Infrastructure Protection, 2023, 42, 100620.	4.6	1
14	A Low-Cost Environment for Teaching Fundamental Cybersecurity Concepts in CPS. Communications in Computer and Information Science, 2023, , 356-365.	0.5	1
15	Parent process termination: an adversarial technique for persistent malware. Journal of Cyber Security Technology, 0, , 1-26.	2.9	0
16	A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects. Sensors, 2023, 23, 7999.	3.8	2
17	Threat Attribution and Reasoning for Industrial Control System Asset. International Journal of Ambient Computing and Intelligence, 2023, 15, 1-27.	1.1	0
18	Safety monitoring under stealthy sensor injection attacks using reachable sets. IFAC-PapersOnLine, 2023, 56, 1833-1840.	0.9	0

#	Article	IF	Citations
19	A Security Situation Prediction Model for Industrial Control Network Based on EP-CMA-ES. IEEE Access, 2023, 11, 135449-135462.	4.2	0
21	Detecting IoT Anomalies Using Fuzzy Subspace Clustering Algorithms. Applied Sciences (Switzerland), 2024, 14, 1264.	2.5	0
22	Cyber resilience assessment and enhancement of cyber-physical systems: structural controllability perspective. International Journal of Systems Science, 2024, 55, 1224-1242.	5.5	0