

# Piroska Haller

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/5082068/publications.pdf>

Version: 2024-02-01

50  
papers

545  
citations

840728

11  
h-index

794568

19  
g-index

53  
all docs

53  
docs citations

53  
times ranked

515  
citing authors

#	ARTICLE	IF	CITATIONS
1	A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 2015, 10, 3-17.	4.6	90
2	Data clustering-based anomaly detection in industrial control systems. , 2014, , .		50
3	Cyber-Security-Aware Network Design of Industrial Control Systems. IEEE Systems Journal, 2017, 11, 1373-1384.	4.6	42
4	A clustering-based approach to detect cyber attacks in process control systems. , 2015, , .		38
5	Experimental assessment of network design approaches for protecting industrial control systems. International Journal of Critical Infrastructure Protection, 2015, 11, 24-38.	4.6	28
6	GHOST - Safe-Guarding Home IoT Environments with Personalised Real-Time Risk Control. Communications in Computer and Information Science, 2018, , 68-78.	0.5	27
7	Anomaly Detection in Aging Industrial Internet of Things. IEEE Access, 2019, 7, 74217-74230.	4.2	27
8	Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems. IEEE Access, 2017, 5, 9336-9347.	4.2	26
9	A connection pattern-based approach to detect network traffic anomalies in critical infrastructures. , 2014, , .		20
10	A framework for designing resilient distributed intrusion detection systems for critical infrastructures. International Journal of Critical Infrastructure Protection, 2016, 15, 3-11.	4.6	20
11	Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. International Journal of Critical Infrastructure Protection, 2019, 25, 152-168.	4.6	19
12	A hierarchical control plane for software-defined networks-based industrial control systems. , 2016, , .		18
13	A survey on cloud-based software platforms to implement secure smart grids. , 2014, , .		17
14	Engineering security-aware control applications for data authentication in smart industrial cyber-physical systems. Future Generation Computer Systems, 2019, 91, 206-222.	7.5	17
15	Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids. IEEE Transactions on Smart Grid, 2017, 8, 2440-2451.	9.0	16
16	Denial of Service Attack Detection in Case of Tennessee Eastman Challenge Process. Procedia Technology, 2015, 19, 835-841.	1.1	13
17	Privacy-Preserving Tampering Detection in Automotive Systems. Electronics (Switzerland), 2021, 10, 3161.	3.1	10
18	On the practical integration of anomaly detection techniques in industrial control applications. International Journal of Critical Infrastructure Protection, 2019, 24, 48-68.	4.6	9

#	ARTICLE	IF	CITATIONS
19	Performance Analysis of Wireless Sensor Networks. <i>Procedia Technology</i> , 2015, 19, 842-849.	1.1	7
20	Communication delay and jitter influence on bilateral teleoperation. , 2014, , .		5
21	Prediction and congestion control algorithm for networked motion tracking. <i>Control Engineering Practice</i> , 2009, 17, 1265-1272.	5.5	3
22	Performance analysis of WLAN based mobile robot teleoperation. , 2013, , .		3
23	Nonlinear PI Rate Control in Bottleneck Links: Application to Teleoperation Systems—This work was supported by a grant of the Romanian National Authority for Scientific Research, CNCS UEFISCDI, project number PN-II-RU-TE-2011-3-0005.. <i>IFAC-PapersOnLine</i> , 2015, 48, 14-19.	0.9	3
24	Cross-layer anomaly detection in industrial cyber-physical systems. , 2017, , .		3
25	A lightweight key generation scheme for end-to-end data authentication in Industrial Control Systems. <i>Automatisierungstechnik</i> , 2019, 67, 417-428.	0.8	3
26	Bilateral Teleoperation of Wheeled Mobile Robots Working in Common Workspace. <i>IAES International Journal of Robotics and Automation</i> , 2013, 3, .	0.3	3
27	Tampering Detection for Automotive Exhaust Aftertreatment Systems using Long Short-Term Memory Predictive Networks. , 2022, , .		3
28	Extending the BOINC architecture using peer-to-peer application code exchange. , 2011, , .		2
29	Passive bilateral teleoperation with bounded control signals. , 2013, , .		2
30	A framework for testing stealthy attacks in energy grids. , 2015, , .		2
31	Bilateral Teleoperation in the Presence of Jitter: Communication Performance Evaluation and Control. <i>Studies in Systems, Decision and Control</i> , 2015, , 291-311.	1.0	2
32	Behavior-based critical cyber asset identification in Process Control Systems under Cyber Attacks. , 2015, , .		2
33	Generating high quality data for the protection of modern critical infrastructures. , 2016, , .		2
34	Data transfer regulator for wireless teleoperation. <i>Transactions of the Institute of Measurement and Control</i> , 2016, 38, 141-149.	1.7	2
35	SOFTWARE DEFINED RESPONSE AND NETWORK RECONFIGURATION FOR INDUSTRIAL CONTROL SYSTEMS. <i>IFIP Advances in Information and Communication Technology</i> , 2017, , 157-173.	0.7	2
36	Term-Based Composition of Security Protocols. , 2008, , .		1

#	ARTICLE	IF	CITATIONS
37	Video supported bilateral teleoperation system: Design and implementation. , 2013, , .		1
38	Optimally scheduled interventions in the presence of vulnerabilities for modern cyber-physical systems. , 2017, , .		1
39	Enabling authenticated data exchanges in industrial control systems. , 2018, , .		1
40	Middleware for Automated Implementation of Security Protocols. Lecture Notes in Computer Science, 2009, , 476-490.	1.3	1
41	Dynamic Filter Based Prediction for Efficient Networked Motion Tracking. Industrial Informatics, 2009 INDIN 2009 7th IEEE International Conference on, 2007, , .	0.0	0
42	Adaptive Transfer Protocol for Networked Motion Tracking. , 2007, , .		0
43	Formal verification and implementation of real time operating system based applications. , 2008, , .		0
44	A syntactic approach for identifying multi-protocol attacks. , 2009, , .		0
45	Design, verification and implementation of a lightweight remote attestation protocol for process control systems. , 2017, , .		0
46	A Security-Enhanced Interoperability Middleware for the Internet of Things. , 2019, , .		0
47	Using Side-Channels to Detect Abnormal Behavior in Industrial Control Systems. , 2019, , .		0
48	Engineering Edge Security in Industrial Control Systems. Advanced Sciences and Technologies for Security Applications, 2019, , 185-200.	0.5	0
49	Towards Automated Secure Web Service Execution. Lecture Notes in Computer Science, 2009, , 943-954.	1.3	0
50	Big Data Processing to Detect Abnormal Behavior in Smart Grids. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 214-221.	0.3	0