*Se aplică pentru :

Facultatea de Inginerie și Tehnologia Informației; Facultatea de Științe și Litere „Petru Maior"; Facultatea de Economie și Drept

Avizat
Comisia de verificare a îndeplinirii standardelor
Preşedinte: _____
Membri: _____
_____
_____

Standardele minimale:
- sunt îndeplinite;
- nu sunt îndeplinite.

Fişă de verificare

a îndeplinirii standardelor minimale necesare şi obligatorii pentru conferirea titlurilor didactice din învăţământul superior şi a gradelor profesionale de cercetare-dezvoltare prevăzute în Anexa nr. _2 – Comisia de Informatică_ din Ordinul Ministerului Educaţiei Naţionale şi Cercetării Ştiinţifice nr. 6129/2016

I. DATE DESPRE CANDIDAT

Nume ____GENGE _____Prenume ____BÉLA_____
Gradul didactic pentru care candidează ___PROFESOR UNIVERSITAR_____
Domeniul ştiinţific ___INFORMATICĂ_____ Poziţia în statul de funcţii ____4_____
Departamentul ___INGINERIE ELECTRICĂ ȘI TEHNOLOGIA INFORMAȚIEI_____
Facultatea___INGINERIE ȘI TEHNOLOGIA INFORMAȚIEI_____

Gradul didactic actual __CONFERENȚIAR UNIVERSITAR___ Poziţia în statul de funcţii _____7_____
Domeniul ştiinţific ___ INFORMATICĂ _____ Departamentul___ INGINERIE ELECTRICĂ ȘI TEHNOLOGIA INFORMAȚIEI _____
Facultatea___ INGINERIE ȘI TEHNOLOGIA INFORMAȚIEI _____ Universitatea ___DE MEDICINĂ, FARMACIE, ȘTIINȚE ȘI TEHNOLOGIE "GEORGE EMIL PALADE" DIN TÂRGU MUREȘ__

II. DATE PRIVIND ÎNDEPLINIREA CONDIŢIILOR DE CONCURS

Doctor __în Știința Calculatoarelor, titlu teză: Contribuții la compunerea și implementarea protocoalelor de securitate, Univ. Tehnică din Cluj-Napoca, Data susținerii: 22 Mai 2009.

Confirmat prin ordinul nr. ___4698 din 14 August 2009_

Atestat de abilitare _în Informatică, titlu teză: Contributions to improving the cyber security and resilience of networked critical infrastructures, Univ. Babes-Bolyai din Cluj-Napoca, Data susținerii: 23 Iunie 2016.

Confirmat prin ordinul nr. ___5961 din 8 Decembrie 2016_

III. DATE PRIVIND ÎNDEPLINIREA STANDARDELOR MINIMALE NAŢIONALE

• Facultatea de Inginerie și Tehnologia Informației și Tehnologia Informației;

1-Condiţii minimale

Nr. crt.	Domeniul de activitate	Categoria Condiţii profesor/ CS I / Abilitare	Punctaj realizat
		Conform standardelor minimale din Metodologia proprie pentru ocuparea posturilor didactice și de cercetare	
1.	**Activitatea didactică şi profesională (A1) CNATDCU Comisia Informatică: performanța academică – perspectiva d**	Min 60 puncte Praguri: Minim un proiect cu echipă de cel puțin 2 (doi) membri, obținut prin competiție la nivel national sau internațional	**171.83 puncte** Praguri: **3 proiecte cu echipă de cel puțin 2 membri** obținute prin competiție națională/internațională (detalii la evaluarea perspectivei)
2.	**Activitatea de cercetare (A2) CNATDCU Comisia Informatică: producția științifică – perspectiva b**	Min 56 puncte Praguri: A*+A ≥ 24 puncte, A*+A+B ≥ 40 puncte	**165.66 puncte** Praguri: **A*+A = 100 puncte** **A*+A+B = 138.66 puncte**
3.	**Recunoaşterea şi impactul activităţii (A3) CNATDCU Comisia Informatică: impactul rezultatelor – perspectiva c**	Min 120 puncte Praguri: A*+A+B ≥ 40 puncte	**1332 puncte** **A*+A+B = 1010 puncte**
	TOTAL	Min 236 puncte	**1669.49 puncte**

***La realizarea acestui punctaj se iau în considerare şi rezultatele aferente criteriilor opţionale dacă este cazul**

IV. DATE PRIVIND ÎNDEPLINIREA CERINŢELOR:

• Facultatea de Inginerie și Tehnologia Informației și Tehnologia Informației; Facultatea de Științe și Litere „Petru Maior"

Nr. crt.	Tipul activităţilor, categorii şi restricţii		Nr. dovezii* (pag.)	Punctaj acordat	Punctaj realizat
ACTIVITATEA DIDACTICĂ ŞI PROFESIONALĂ (A1) CNATDCU Comisia Informatică: performanța academică – perspectiva d					
1.	**A1.1.1 Cărţi de autor/editate în edituri de categoria (conform SENSE): A: 16 / max(1,n-2) B: 8 / max(1,n-2) C: 4 / max(1,n-2) D, E, nelistate: 2 / max(1,n-2)**	B. Genge: Introducere în implementarea aplicatiilor criptografice. Editura Univ. "Petru Maior", Tirgu Mures, 2013, 190 pagini, ISBN 978-606-581-094-5. Categ: nelistat	1-8	**2**	
		B. Genge, P. Haller: Proiectarea sistemelor dedicate si incorporate cu microcontrolerul PIC. Editura Univ. "Petru Maior", Tirgu Mures, 2008, 188 pagini, ISBN 978-973-7794-79-6. Categ: nelistat	9-14	**2**	
		A.V. Duka, B. Genge, P. Haller: Sisteme cu microprocesoare. Microcontrolerul PIC 18F4455. Editura Univ. "Petru Maior", Tirgu Mures, 2013, 305	15-22	**2**	

		pagini, ISBN 978-973-7794-99-4. Categ: nelistat			
		TOTAL		**6**	
2.	**A1.1.2 Capitole publicate în edituri de categoria (conform SENSE)** **A: 8 / max(1,n-2)** **B: 4 / max(1,n-2)** **C: 2 / max(1,n-2)** **D, E, nelistate: 1/max(1,n-2)**	P. Haller, B. Genge, A. Duka: Engineering Edge Security in Industrial Control Systems, Critical Infrastructure Security and Resilience. Springer, Cham, pp. 185-200, 2019. Capitol carte Springer	23-29	**4**	
		A.-V. Duka, B. Genge, P. Haller, B. Crainicu: Enforcing End-To-End SecurityWith Application-Level Cryptography in SCADA Systems, Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Arlington, Virginia, USA, March 13-15, Appears in Critical Infrastructure Protection XI: 11th IFIP WG 11.10 International Conference, ICCIP 2017, Arlington, VA, USA, March 13-15, 2017, Revised Selected Papers, pp. 139-155, 2017. Capitol carte Springer	30-36	**2**	
		H. Sandor, B. Genge, P. Haller, F. Graur: Software Defined Response and Network Reconfiguration for Industrial Control Systems, Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Arlington, Virginia, USA, March 13-15, Appears in Critical Infrastructure Protection XI: 11th IFIP WG 11.10 International Conference, ICCIP 2017, Arlington, VA, USA, March 13-15, 2017, Revised Selected Papers, pp. 157-173, 2017. Capitol carte Springer	30-36	**2**	
		B. Genge, H. Sandor, P. Haller, A. Beres, I. Kiss: Using Software Defined Networking to Mitigate Cyber Attacks in Industrial Control Systems. Securing Cyber-Physical Systems, CRC Press, Taylor & Francis, USA, pp. 305-330, 2015. Capitol carte CRC Press	37-44	**1.33**	
		B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera: Analyzing Cyber-Physical Attacks on Networked Industrial Control Systems. Hannover, New Hampshire, USA, 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection V, vol. 367, Revised Selected Papers, Springer, pp. 167-183, 2011. Capitol carte Springer	45-50	**2**	
		C. Siaterlis, B. Genge, M. Hohenadel, and M. Del Pra:	51-57	**2**	

		Enabling the Experimental Exploration of Operating Procedures in Critical Infrastructures. Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Marshall Hall, National Defense University, Fort McNair, Washington, DC, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection VI, Springer, pp. 217-233, 2012. Capitol carte Springer			
		B. Genge, P. Haller, and O. Ratoi: Constructing Security Protocol Specifications for Web Services. 2nd International Symposium on Intelligent and Distributed Computing, in Studies In Computational Intelligence, vol. 162, Intelligent Distributed Computing, Springer-Verlag Berlin Heidelberg, pp. 245-250, 2008. Capitol carte Springer	58-60	**4**	
		TOTAL		**17.33**	
3.	**A1.2 Editor proceedings la conferințe de tip: A*|A|B|C|D (12|8|4|2|1)/max(1,n-2)**	2017 IEEE International Conference on Digital Forensic and Security, Tîrgu Mureș, Romania Editori: Genge Béla și Haller Piroska Link IEEE Xplore: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7916490 Indexare IEEE	61	**1**	
		TOTAL		**1**	
4.	**A1.3 Publicarea unui curs universitar în format electronic**				
5.	**A1.4 Director/editor al unei reviste de tip: A*|A|B|C|D 36|24|12|6|3**	International Journal of Critical Infrastructure protection, Elsevier https://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection/editorial-board UEFISCDI 2019	62	**12**	
		Security and Communication Networks, Wiley (Hindawi) https://www.hindawi.com/journals/scn/editors/ UEFISCDI 2019	63	**6**	
		Journal of Cyber Security and Mobility http://riverpublishers.com/journal.php?j=JCSM/2/2/jeb Indexare SCOPUS	64	**6**	
		International Journal of Computer Networks & Communications (IJCNC) http://airccse.org/journal/j2editorial.html Indexare Ebsco, CiteSeer	65	**3**	
		TOTAL		**27**	
6.	**A1.5 Director**	2014-2018: FP7 Marie Curie Career Integration	66-71	**6**	

	(coordinator/responsabil) sau membru al unui grant/proiect/contract/ program de cercetare național/internațional Director/membru cu valoarea intrată în instituție: >= 500.000 EUR | 200.000 EUR-499.999 EUR | 100.000-199.999 EUR | 50.000-99.999EUR | <50.000 EUR: 10/5|8/4|6/3|4/2|2/1	Grant intitulat "SERENITI: Cyber security and resilience of networked critical infrastructures", PCIG14-GA-2013-631128. 100.000 EUR **DIRECTOR (4 Membrii)** https://nislab.umfst.ro/projects/sereniti/team.html			
		2016-2018: Proiectul finanțat PNIII, UEFISCDI Bridge Grant intitulat "PROTECT-G: Protejarea comunicațiilor în sistemele de transport a gazelor naturale", nr. PN-III-P2-2.1-BG-2016-0013. 456.250 RON **DIRECTOR (6 Membrii)** https://nislab.umfst.ro/projects/protect-g/en/team.html	72-75	**6**	
		2016 (Ianuarie/Februarie – Iunie/Iulie): Grant de cercetare intitulat "SDIIT: Software Defined Industrial Internet of Things" finanțat de "Accenture Industrial Software Solutions (AISS) grant program for Universities for IoT activity", nr. 899/05.04.2016, 22.000 RON **DIRECTOR (5 Membrii)**	76-79	**2**	
		2010-2013: Grant de cercetare post-doctoral intitulat "Network security in industrial settings" acordat de Institute for the Protection and Security of the Citizen, Joint Research Centre, Ispra, Italy, IPSC-G06-13. 130.000 EUR **DIRECTOR**	80-82	**6**	
		2019-2022: Smart Adaptive Remote Diagnostic Antitampering Systems (DIAS), Horizon 2020, Call identifier: H2020-MG-2018-2019-2020 (2018-2020 Mobility for Growth), nr. 814951. 259.500 EUR (UMFST) **Membru** https://dias-project.com/	83-86	**4**	
		2017-2020: Proiect intitulat "Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control" (GHOST), European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement No 740923, Call identifier: H2020-DS-2016-2017 Digital Security Focus Area. 457.625 EUR (THI) **Membru** https://www.ghost-iot.eu/ghost-project	87-92	**4**	
		2012-2014: Proiectul intitulat „Security of Energy Systems" finanțat de DG-HOME, European Commission (HOME/2011/CIPS/AG/4000002096, 30-CE-0488214/00-30). 179.871 EUR (GCSEC) **Membru**	93-102	**3**	
		TOTAL		**31**	
7.	**A1.6 Membru în comitetul științific (de program) al unor conferințe,**	IEEE/IFIP Networking 2018, Zurich, Elveția CORE2018	103	**4 (A)**	
		IEEE/IFIP Networking 2017, Stockholm, Suedia CORE2017	103	**4 (A)**	

	simpozioane, workshop-uri de tip: A*|A|B|C|D 6|4|2|1|0,5	First ACM Workshop on Cyper-Physical Systems Security & Privacy (CPS-SPC), In conjunction with 22nd ACM Conference on Computer and Communications Security (CCS), Denver, Colorado, USA, Oct. 2015. Workshop ACM CCS (A*) CORE2017	103	**4 (A)**	
		Second ACM Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC), in Conjunction with 23rd ACM CCS, Vienna, Austria, 2016. Workshop ACM CCS (A*) CORE2017	104	**4 (A)**	
		Third IEEE International Workshop on Cloud Security and Forensics (WCSF), Sydney, Australia, 2017. Workshop TrustCom (A) CORE2017	104	**2 (B)**	
		Fourth IEEE International Workshop on Cloud Security and Forensics (WCSF), New York, SUA, 2018. Workshop TrustCom (A) CORE2017	104	**2 (B)**	
		8th International Workshop on Cyber Crime (IWCC 2019) Workshop ARES (B) CORE2018	105	**1 (C)**	
		1st International Workshop on Information Security Methodology and Replication Studies Workshop ARES (B) CORE2018	105	**1 (C)**	
		The 2nd Special Session on High Performance Mission Critical System Development (HiPMiC 2019) Workshop HPCS (B) CORE2018	106	**1 (C)**	
		International Workshop on Cyber Crime (IWCC), Toulouse, France, 2015. Workshop ARES (B) CORE2017	106	**1 (C)**	
		International Workshop on Cyber Crime (IWCC), Salzburg, Austria, 2016. Workshop ARES (B) CORE2017	106	**1 (C)**	
		International Workshop on Cyber Crime (IWCC), Salzburg, Austria, 2017. Workshop ARES (B) CORE2017	106	**1 (C)**	
		International Workshop on Cyber Crime (IWCC), Hamburg, Germania, 2018. Workshop ARES (B) CORE2017	107	**1 (C)**	
		WORLDCOMP 2013, The 2013 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2013	107-108	**1 (C)**	
		WORLDCOMP 2014, The 2014 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2014	107-108	**1 (C)**	
		WORLDCOMP 2015, The 2015 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2015	107-108	**1 (C)**	
		WORLDCOMP 2016, The 2016 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2017	107-108	**1 (C)**	

		WORLDCOMP 2017, The 2017 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2017	107-108	**1 (C)**	
		WORLDCOMP 2018, The 2018 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2018	107-108	**1 (C)**	
		WORLDCOMP 2019, The 2019 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2018	107-108	**1 (C)**	
		WORLDCOMP 2020, The 2020 International Conference on Security and Management (SAM2013), Las Vegas, USA. CORE2018	107-108	**1 (C)**	
		The Second International Conference on Advances in Computing and Information Technology, Chennai, India, 2012. Indexare Springer	109	**0.5 (D)**	
		3rd International Symposium for ICS & SCADA Cyber Security Research, Ingolstadt, Germany, 2015. Indexare ACM	109	**0.5 (D)**	
		5th International Symposium for ICS & SCADA Cyber Security Research, Hamburg, Germany, 2018. Indexare ACM	109	**0.5 (D)**	
		6th International Symposium for ICS & SCADA Cyber Security Research 2019 Indexare ACM	110	**0.5 (D)**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2013. Indexare Elsevier Science	110	**0.5 (D)**	
		The 5th International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics, MACRO 2015, Tirgu Mures, Romania, 2015. Indexare DeGruyter	111	**0.5 (D)**	
		The 6th International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics, MACRO 2017, Tirgu Mures, Romania, 2017. Indexare DeGruyter	111	**0.5 (D)**	
		The 7th International Conference on Computer Science and its Applications (CSA-15), Cebu, Philippines, 2015. Indexare Springer	112	**0.5 (D)**	
		9th EAI International Wireless Internet Conference, December 19–21, Sanya, People's Republic of China, 2016. Indexare DBLP	112	**0.5 (D)**	
		2018 Central European Cyber Security Conference, Ljubliana, Slovenia Indexare ACM	112	**0.5 (D)**	

		2018 7th International conference on smart cities and green ICT systems, Portugal Indexare INSTICC	113	**0.5 (D)**	
		TOTAL		**40.5**	
8.	**A1.7 Organizare evenimente științifice/școli de vară în calitate de: director (2) / membru (1)**	International Symposium on Digital Forensics and Security (ISDFS), Tg. Mures, Romania, 2017	113	**1**	
		International Symposium on Digital Forensics and Security (ISDFS), Antalya, Turkey, 2018	114	**1**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2014	114	**1**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2015	114	**1**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2016	114	**1**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2017	114	**1**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2018	115	**1**	
		International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2019	115	**1**	
		2019 Central European Cyber Security Conference, Munich, Germany	115	**1**	
		TOTAL		**9**	
9.	**A1.8 Keynote/invited speaker/professor la evenimente/universități** **A*/top 20: 12** **A/top 100: 8** **B, școli de vară internaționale/top 200: 4** **C, școli de vară naționale, conferințe ale Academiei Române/top 500: 2** **D, evenimente locale/> 500: 1**	International Conference on Interdisciplinarity in Engineering (Inter-Eng), Tg. Mures, Romania, 2014 https://inter-eng.umfst.ro/2014/keynote-speakers.html	116	**1 (D)**	
		2018 Central European Cyber Security Conference, Ljubliana, Slovenia Indexare ACM https://www.fvv.um.si/cecc2018/	117	**1 (D)**	
		TOTAL		**2**	
10.	**A1.9 Profesor/cercetător asociat/visiting la o universitate** **Top 20: 12*nr. luni** **Top 100: 8*nr. luni** **Top 200: 4*nr. luni** **Top 500: 2*nr. luni** **> 500: nr. luni**	Universitatea din Debrecen, Cercetător asociat (contract finanțat de Universitatea Debrecen pentru a desfășura activități de cercetare în cadrul laboratorului Internet of Things), Iunie și Noiembrie 2014 – 2 luni (>500)	118-119	**2**	
		TOTAL		**2**	

11.	**A1.10 Consolidarea de echipe de cercetare International (acreditări) | național (acreditări) | în instituție (recunoscute official): 4|2|1*nr. ani**	Echipă de cercetare: Network and Information Security Laboratory, recunoscută oficial în cadrul UMFST (2014-2019): https://nislab.umfst.ro/team.html	On-line	**6**	
		TOTAL		**6**	
12.	**A1.11 Membru în comisii de evaluare a tezelor de doctorat la o universitate conform**				
13.	**A1.12 Membru în comisii de îndrumare a doctoranzilor (dovedit prin decizia școlii doctorale)**				
14.	**A1.13 Brevete și invenții active (OSIM, ORDA, etc.)**				
15.	**A1.14 Dezvoltarea de pachete și instrumente software, dezvoltarea de resurse și colecții de date de largă utilitate (probate prin număr de accesări, publicarea pe site-uri open source, etc.) 2/max(1,n-2)**	AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. http://sourceforge.net/projects/amici/	On-line	**2**	
		SPEAR: A Connection Pattern-based Approach to Detect Network Traffic Anomalies in Critical Infrastructures. https://nislab.umfst.ro/projects/sereniti/Connpat.html	On-line	**2**	
		Cyber-security-aware network design tool-suite for Networked Critical Infrastructures. https://nislab.umfst.ro/projects/sereniti/netdesign.html	On-line	**2**	
		OptimalFlow: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems. https://nislab.umfst.ro/projects/sereniti/optimalflow.html	On-line	**2**	
		AMICI Extension with IEC61850 https://nislab.umfst.ro/projects/sereniti/AMICIExt.html	On-line	**2**	
		Cross-Association and Cyber Attack Impact Assessment tool https://nislab.umfst.ro/projects/sereniti/CrossCAIA.html	On-line	**2**	
		Clustering-based anomaly detection engine. https://nislab.umfst.ro/projects/sereniti/ADSS.html	On-line	**2**	
		Resilient IDS design for NCI. https://nislab.umfst.ro/projects/sereniti/ResDesign.html	On-line	**1**	

		TOTAL		**15**	
16.	**A1.15 Poziții de conducere în organizații profesionale**				
17.	**A1.16 Premii și alte merite**	2015 – Best Paper Award: 13th International Conference on Industrial Informatics, Cambridge, UK (I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, Cambridge, UK). 2015 – Best paper Award: The 5th International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics, MACRO 2015, Tirgu Mures, Romania (B. Genge, C. Enachescu: Non-Intrusive Historical Assessment of Internet-Facing Services in the Internet of Things, Proc. of MACRO 2015, Univ. of Sapientia, Tg. Mures, Romania) 2015 – Top 5 Best Papers: Ninth IFIP WG 11.10 Int'l Conf. on Critical Infrastructure Protection, SRI, Arlington, Washington DC, USA, 2015 – paper was selected for publication in the International Journal of Critical Infrastructure Protection, Elsevier (B. Genge, I. Kiss, P. Haller: A System Dynamics Approach to Assess the Impact of Cyber Attacks on Critical Infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, 2015 Volume 10, pp. 3-17, 2015) 2014 – 2019 UEFISCDI Premierea rezultatelor Științifice Premiul pentru Excelență în Cercetare acordat de EDU Manager pentru proiectul SERENITI – 2016, București Recenzor invitat reviste: - International Journal of Critical Infrastructure Protection, Elsevier - Computers & Security, Elsevier - Future Generation Computer Systems, Elsevier - Ad Hoc Networks, Elsevier - Expert Systems With Applications, Elsevier - Computers and Electrical Engineering, Elsevier - IEEE Transactions on Emerging Topics in Computing - IEEE Transactions on Smart Grid - IEEE Access - Journal of Information Processing - IEEE Computer Magazine - Mobile Networks and Applications - International Journal of Computer Networks & Communications - International Journal of New Computer Architectures and their Applications	120-128	**15**	

Punctaj obținut (perspectiva A1, CNATDCU Informatică: performanța academică – perspectiva d)		**171.83**	

Nr. crt.	Tipul activităţilor, categorii şi restricţii		Nr. dovezii * (pag.)	Punctaj acordat	Punctaj realizat
ACTIVITATEA DE CERCETARE (A2) **CNATDCU Comisia Informatică: producția științifică – perspectiva b**					
1.	**A2.1 Publicații categoria A* 12/max(1,n-2)**	C. Siaterlis, and B. Genge: Cyber-physical testbeds. Communications of the ACM, vol. 57, no. 6, pp. 64-73, June 2014. UEFISCDI 2014	129-138	**12**	
		C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013. UEFISCDI 2013	139-152	**12**	
		B. Genge, P. Haller, and I. Kiss: Cyber Security-Aware Network Design of Industrial Control Systems, IEEE Systems Journal, IEEE Systems Council, vol. 11, no. 3, pp. 1373 – 1384, 2017. UEFISCDI 2017	153-164	**12**	
		TOTAL		**36**	
2.	**A2.2 Publicații categoria A 8/max(1,n-2)**	B. Genge, P. Haller, A. Duka: Engineering security-aware control applications for data authentication in smart industrial cyber–physical systems, Future Generation Computer Systems, Volume 91, pp. 206-222, 2019. UEFISCDI 2019	165-181	**8**	
		B. Genge, P. Haller, C. Enachescu: Anomaly Detection in Aging Industrial Internet of Things, IEEE Access, Vol. 7, 2019. UEFISCDI 2019	182-195	**8**	
		B. Genge, P. Haller, C.D. Dumitru, C. Enăchescu: Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids, IEEE Transactions on Smart Grid, vol. 8, nr. 5, pp. 2440 – 2451, 2017. UEFISCDI 2017	196-207	**4**	
		P. Haller, B. Genge: Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection	208-219	**8**	

		Systems in Industrial Cyber-Physical Systems, IEEE Access, vol. 5, pp. 9336 – 9347, 2017. UEFISCDI 2017			
		B. Genge, P. Haller: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016. CORE2017	220-228	**8**	
		B. Genge, and C. Siaterlis: An Experimental Study on the Impact of Network Segmentation to the Resilience of Physical Processes. Networking 2012, Prague, Czech Republic, Lecture Notes in Computer Science 7289 Springer 2012, pp. 121-134, 2012. CORE2013	229-242	**8**	
		B. Genge, and P. Haller: Middleware for Automated Implementation of Security Protocols. 6th European Semantic Web Conference, Heraklion, Greece, 31 May - 4 June, Lecture Notes in Computer Science (LNCS 5554), L. Aroyo et al. (Eds.), Springer-Verlag, pp. 476-490, 2009. CORE2013	243-257	**8**	
		B. Genge, and P. Haller: Towards Automated Secure Web Service Execution. Networking 2009, Aachen, Germany, May 11-15, Lecture Notes in Computer Science (LNCS 5550), L. Fratta et al. (Eds.), Springer-Verlag, pp. 943-954, 2009. CORE2013	258-269	**8**	
		B. Genge, C. Siaterlis, and G. Karopoulos: Data Fusion-Based Anomaly Detection in Networked Critical Infrastructures. 43th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013), Workshop on Reliability and Security Data Analysis (RSDA 2013), Budapest, Hungary, pp. 1-8, 2013. Workshop DSN(A*) CORE2013	270-277	**4**	
		TOTAL		**64**	
3.	**A2.3 Publicații categoria B**	P. Haller, B. Genge, A. Duka: On the practical integration of anomaly	278-298	**4**	

	4/max(1,n-2)	detection techniques in industrial control applications, International Journal of Critical Infrastructure Protection, Volume 24, pp. 48-68, 2019. UEFISCDI 2019			
		H Sándor, B Genge, Z Szántó, L Márton, P Haller: Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems, International Journal of Critical Infrastructure Protection, vol. 25, pp. 152-168, 2019. UEFISCDI 2019	299-315	**1.33**	
		C Enăchescu, H Sándor, B Genge: A Multi-Model-based Approach to Detect Cyber Stealth Attacks in Industrial Internet of Things. 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1-6, 2019. CORE2018	316-320	**4**	
		H. Sandor, B. Genge, P. Haller, A.-V. Duka, B. Crainicu: Cross-Layer Anomaly Detection in Industrial Cyber-Physical Systems, 25th International Conference on Software, Telecommunications and Computer Networks, SoftCom2017, Split, Croatia, pp. 1-5, 2017. CORE2017	321-326	**1.33**	
		B. Genge, P. Haller, and I. Kiss: A Framework for Designing Resilient Intrusion Detection Systems for Critical Infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, vol. 15, pp. 3-11, 2016. UEFISCDI 2016	327-335	**4**	
		B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, vol. 10, pp. 3-17, 2015. UEFISCDI 2015	336-350	**4**	
		B. Genge, F. Graur, and P. Haller: Experimental Assessment of Network Design Approaches for Protecting Industrial Control Systems, International Journal of Critical Infrastructure	351-365	**4**	

		Protection, Elsevier, vol. 11, pp. 24-38, 2015. UEFISCDI 2015			
		B. Genge, and C. Siaterlis: Physical process resilience-aware network design for SCADA systems. Computers and Electrical Engineering, Elsevier, vol. 40, no. 1, pp. 142-157, 2014. UEFISCDI 2014	366-381	**4**	
		B. Genge, P. Haller, and I. Kiss: A Linear Programming Approach for K-Resilient and Reliability-Aware Design of Large-Scale Industrial Networks. AdHoc-Now 2015, Athens, Greece, Lecture Notes in Computer Science, Springer, LNCS 9143, pp. 1-15, 2015. CORE2017	382-396	**4**	
		B. Genge, D.A. Rusu, and P. Haller: A Connection Pattern-based Approach to Detect Network Traffic Anomalies in Critical Infrastructures. 2014 ACM European Workshop on System Security (EuroSec2014), Amsterdam, The Netherlands, pp. 1-6, 2014, ISBN 978-1-4503-2715-2 Workshop EuroSys (A) CORE2014	397-402	**4**	
		B. Genge, and C. Siaterlis: Using Soft Real-Time Simulation in a Hybrid Environment for Cyber-Physical Security Experiments. International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Paris, France, pp. 285-290, 2011. CORE2011	403-408	**4**	
		TOTAL		**38.66**	
4.	**A2.4 Publicații categoria C 2/max(1,n-2)**	B Genge, P Haller, AV Duka, H Sándor: A lightweight key generation scheme for end-to-end data authentication in Industrial Control Systems. at-Automatisierungstechnik 67 (5), 417-428, 2019. UEFISCDI 2019	409-420	**1**	
		B. Genge, and C. Enachescu: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks, Wiley, vol. 9, no. 15, pp. 2696-2714, 2016.	421-439	**2**	

		UEFISCDI 2016			
		B. Genge, and C. Siaterlis: Analysis of the Effects of Distributed Denial-of-Service Attacks on MPLS Networks. International Journal of Critical Infrastructure Protection, Elsevier, vol. 6, no. 2, pp. 87-95, 2013. SCOPUS 2013	440-448	**2**	
		B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera: A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. Computers and Electrical Engineering, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012. UEFISCDI 2012	449-464	**1**	
		B. Genge, C. Siaterlis, and M. Hohenadel: Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems. International Journal of Computers, Communications & Control, vol. 7, no. 4, pp. 673-686, 2012. Indexare ISI	465-478	**2**	
		I. Kiss, B. Genge, P. Haller, and G. Sebestyen: A Framework for Testing Stealthy Attacks in Energy Grids. IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 553 – 560, 2015. CORE2017	479-486	**1**	
		H. Sandor, B. Genge, and G. Sebestyen: Resilience in the Internet of Things: The Software Defined Networking Approach, IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 545 – 552, 2015. CORE2017	487-494	**2**	
		I. Kiss, B. Genge, P. Haller, and G. Sebestyen: Data clustering-based anomaly detection in industrial control systems. 2014 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September, pp.	495-501	**1**	

		275-281, 2014. CORE2014			
		B. Genge, C. Siaterlis, and M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228-239, 2012. CORE2013	502-513	**2**	
		B. Genge, and C. Siaterlis: Investigating the Effect of Network Parameters on Coordinated Cyber Attacks Against a Simulated Power Plant. 6th International Conference on Critical Information Infrastructure Security, Luzerne, Switzerland, Lecture Notes in Computer Science 6983, pp. 140-151, 2011. CORE2013	514-525	**2**	
		B. Genge, P. Haller: Using Planetlab To Implement Multicast at the Application Level. International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.1, January 2011, pp. 67-80, ISSN 0974-9322, 2011. Indexare SCOPUS	526-539	**2**	
		B. Genge, and P. Haller: Resource Usage Prediction for Application-Layer Multicast Networks. 2010 IEEE International Conference on Intelligent Communication and Processing (ICCP 2010), Cluj-Napoca, Romania, pp. 473-478, 2010. CORE2013	540-545	**2**	
		B. Genge, I. Ignat, and P. Haller: Automated Composition of Security Protocols. 2009 IEEE International Conference on Intelligent Communication and Processing (ICCP 2009), Cluj-Napoca, Romania, pp. 251-258, 2009. CORE2013	546-553	**2**	
		B. Genge, and P. Haller: A Modeling Framework for Generating Security Protocol Specifications. 10th	554-557	**2**	

		International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC'08), Timisoara, Romania, pp. 362-365, 2008. CORE2013			
		B. Genge, P. Haller, I. Ignat, and O. Ratoi: Informal specification-based performance evaluation of security protocols. 4th IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, Romania, pp. 193-200, 2008. CORE2013	558-565	**1**	
		B. Genge, and I. Ignat: Verifying the Independence of Security Protocols. 3rd IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, Romania, pp. 155-163, 2007. CORE2013	566-573	**2**	
		TOTAL		**27**	
Punctaj obținut (perspectiva A2, CNATDCU Informatică: producția științifică – perspectiva b)				**165.66**	

Nr. crt.	**Tipul activităţilor, categorii şi restricţii**		**Nr. dovezii * (pag.)**	**Punctaj acordat**	**Punctaj realizat**
RECUNOAŞTEREA ŞI IMPACTUL ACTIVITĂŢII (A3) **CNATDCU Comisia Informatică: impactul rezultatelor – perspectiva c**					
1.	**A3.1 Citări provenind din publicații categoria A* 12/max(1,n-2)**				
	C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013.		574-587		
	K. Mets, J.A. Ojea, and C. Develder: Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis. Communications Surveys & Tutorials, IEEE , vol.16, no.3, pp.1771,1796, Third Quarter 2014. UEFISCDI 2014			**12**	
	U. Goel, M.P. Wittie, K.C. Claffy, A. Le: Survey of End-to-End Mobile Network Measurement Testbeds, Tools, and Services. IEEE Communications Surveys & Tutorials, vol. 18, no. 1, 2016. UEFISCDI 2016			**12**	
	MC Smarter, C Insecurity, C Libertarianism: Who Owns the Social Web?, Communications of the ACM, 2017. UEFISCDI 2017			**12**	
	B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera: A Cyber-Physical		588-		

	Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. Computers and Electrical Engineering, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012.	603		
	W Li, L Xie, Z Wang: Two-Loop Covert Attacks against Constant-Value Control of Industrial Control Systems, IEEE Transactions on Industrial Informatics, 2018. UEFISCDI 2018		**6**	
	B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015	604-617		
	X Li, C Zhou, YC Tian, N Xiong: Asset-based Dynamic Impact Assessment of Cyberattacks for Risk Analysis in Industrial Control Systems, IEEE Transactions on Industrial Informatics, vol 14. pp. 608-618, 2018. UEFISCDI 2018		**12**	
	H Zhang, B Qin, T Tu, Z Guo, F Gao: An Adaptive Encryption-as-a-Service Architecture Based on Fog Computing for Real-time Substation Communications, IEEE Transactions on Industrial Informatics, 2019 UEFISCDI 2019		**12**	
	I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, 2015	618-627		
	Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell, A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. ACM Computing Surveys, vol 51, 4, 2018 UEFISCDI 2018		**12**	
	David I. Urbina, Jairo A. Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Limiting the Impact of Stealthy Attacks on Industrial Control Systems. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). ACM, New York, NY, USA, 1092-1105, 2016 CORE2017		**12**	
	B Yang, L Guo, F Li, J Ye: Vulnerability Assessments of Electric Drive Systems due to Sensor Data Integrity Attacks, IEEE Transactions on Industrial Informatics, 2019 UEFISCDI 2019		**12**	
	W Aoudi, M Iturbe, M Almgren: Truth will out: Departure-based process-level detection of stealthy attacks on control systems, CCS '18 Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018 CORE2018		**12**	
	B. Genge, C. Enachescu: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks, Wiley, Volume 9, Issue 15, pp. 2696-2714, 2016.	644-650		
	Q Li, X Feng, R Wang, Z Li, L Sun: Towards fine-grained fingerprinting of firmware in online embedded devices, IEEE INFOCOM 2018 CORE2018		**12**	
	B. Genge, C. Siaterlis, and M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228-	657-662		

	239, 2012.			
	S. Ntalampiras: Detection of Integrity Attacks in Cyber-Physical Critical Infrastructures Using Ensemble Modeling. Industrial Informatics, IEEE Transactions on, vol. 11, no. 1, pp. 104-111, Feb. 2015. UEFISCDI 2016		**12**	
	B. Genge, P. Haller, I. Kiss: Cyber Security-Aware Network Design of Industrial Control Systems, IEEE Systems Journal, 11(3), pp.1373-1384, 2017.	663-668		
	J Yang, C Zhou, S Yang, H Xu: Anomaly detection based on zone partition for security protection of industrial cyber-physical systems, IEEE Transactions on Industrial Electronics, vol65(5), pp. 4257 – 4267, 2018 UEFISCDI 2018		**12**	
	B. Genge, A. Beres, and P. Haller: A Survey on Cloud-based Software Platforms to Implement Secure Smart Grids. 49th IEEE International Universities' Power Engineering Conference, Cluj-Napoca, Romania, September, pp. 1-6, 2014	701-704		
	M. H. Cintuglu, O. A. Mohammed, K. Akkaya and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 446-464, Firstquarter 2017. UEFISCDI 2017		**12**	
	N Popovic, D Popovic, I Seskar: A Novel Cloud-Based Advanced Distribution Management System Solution, IEEE Transactions on Industrial Informatics, vol 14 iss 8, pp. 3469 – 3476, 2018. UEFISCDI 2018		**12**	
	B. Genge, P. Haller: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016.	705-708		
	MH Rehmani, A Davy, B Jennings: Software Defined Networks based Smart Grid Communication: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, 2019		**12**	
	H. Sandor, B. Genge, G. Sebestyen: Resilience in the Internet of Things: The Software Defined Networking Approach, IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 545-552, 2015.	715-717		
	S Bera, S Misra, AV Vasilakos: Software-Defined Networking for Internet of Things: A Survey, IEEE Internet of Things Journal, 2017. UEFISCDI 2017		**12**	
	B. Genge, and I. Ignat: Verifying the Independence of Security Protocols. 3rd IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, Romania, pp. 155-163, September 2007.	727-726		
	F. Bergsma, B. Dowling, F. Kohlar, J. Schwenk, and D. Stebila: Multi-Ciphersuite Security of the Secure Shell (SSH) Protocol. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 369-381, 2014. CORE2014		**12**	

	A. Beres, B. Genge, and I. Kiss: A Brief Survey on Smart Grid Data Analysis in the Cloud. 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Tirgu Mures, Romania, vol. 19, Procedia Technology, pp. 858–865, 2015.	729-730		
	S Tan, D De, WZ Song, J Yang: Survey of security advances in smart grid: A data driven approach, IEEE Communications Surveys & Tutorials, 2017 UEFISCDI 2017		**12**	
	TOTAL		**222**	
2.	**A3.2 Citări provenind din publicații categoria A 8/max(1,n-2)**			
	C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013.	574-587		
	A Furfaro, A Piccolo, A Parise, L Argento: A Cloud-based platform for the emulation of complex cybersecurity scenarios, Future Generation Computer Systems Volume 89, December 2018, Pages 791-803.		**8**	
	A. Furfaro, L. Argento, A. Parise, A. Piccolo: Using virtual environments for the assessment of cybersecurity issues in IoT scenarios, Simulation Modelling Practice and Theory, 2017.		**8**	
	T Varisetty, D Dietrich: Client-side Bandwidth Estimation Technique for Adaptive Streaming of a Browser Based Free-Viewpoint Application, HotEdgeVideo'19 Proceedings of the 2019 Workshop on Hot Topics in Video Analytics and Intelligent Edges. Workshop MobiCom (A*) CORE2018		**8**	
	B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera: A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. Computers and Electrical Engineering, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012.	588-603		
	S Nazir, S Patel, D Patel: Assessing and augmenting SCADA cyber security: A survey of techniques, Computers & Security, 2017. UEFISCDI 2017		**4**	
	C. Baham and V. Kisekka: Applying Cyber Range Concepts of Operation to Disaster Recovery Testing. A Case Study, 2015 Americas Conference on Information Systems (AMCIS), Puerto Rico, August 13-15, 2015. CORE2017		**4**	
	S.K. Khaitan, and J.D. McCalley: Design Techniques and Applications of Cyberphysical Systems: A Survey. Systems Journal, IEEE , vol. 9, no. 2, pp.1-16, 2015. CORE2014		**4**	
	M Azimi, A Sami, and A Khalili: A security test-bed for industrial control systems. Proceedings of the 1st International Workshop on Modern Software Engineering Methods for Industrial Automation, pp. 26-31, 2014. Workshop ICSE (A*) CORE2014		**4**	
	MR Asghar, Q Hu, S Zeadally: Cybersecurity in industrial control systems: Issues, technologies, and challenges, Computer Networks, 2019		**4**	

	UEFISCDI 2019			
	R Bitton, T Gluck, O Stan, M Inokuchi, Y Ohta: Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation, European Symposium on Research in Computer Security, ESORICS, 2018. CORE2018		**4**	
	B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015	604-617		
	G Gonzalez-Granadillo, J Rubio-Hernan: Using an Event Data Taxonomy to Represent the Impact of Cyber Events as Geometrical Instances, IEEE Access, 2017. UEFISCDI 2017		**8**	
	R Lanotte, M Merro, R Muradore: A formal approach to cyber-physical attacks, Computer Security Foundations Symposium (CSF), 2017 IEEE 30th, 2017 CORE2017		**8**	
	Palleti, V. R., Joseph, J. V., & Silva, A., A contribution of axiomatic design principles to the analysis and impact of attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 23, pp. 21-32, 2018 UEFISCDI 2018		**8**	
	Leszczyna, R., Standards on cyber security assessment of smart grid. International Journal of Critical Infrastructure Protection, 22, pp. 70-89, 2018 UEFISCDI 2018		**8**	
	L Cazorla, C Alcaraz, J Lopez: Cyber Stealth Attacks in Critical Information Infrastructures, IEEE Systems Journal, vol. 12(2), pp. 1778 – 1792, 2018 UEFISCDI 2018		**8**	
	R Ramirez, N Choucri: Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review, IEEE Access, vol 4, pp. 2216 – 2243, 2016. UEFISCDI 2016		**8**	
	J Zhang, X Liu, P Zhu: Securing Power System State Estimation, Trustcom/BigDataSE/I?SPA, 2016 IEEE, 2016. CORE2017		**8**	
	A Ameli, A Hooshyar, E El-Saadany: Attack Detection and Identification for Automatic Generation Control Systems, IEEE Transactions on Power Systems, vol 33(5), pp. 4760 – 4774, 2018. UEFISCDI 2018		**8**	
	Hamed Orojlo, Mohammad Abdollahi Azgomi: A method for evaluating the consequence propagation of security attacks in cyber–physical systems, Future Generation Computer Systems, vol. 67, pp. 57-71, 2017. UEFISCDI 2017		**8**	
	R Alguliyev, Y Imamverdiyev, L Sukhostat: Cyber-physical systems and their security issues, Computers in industry, 2018. UEFISCDI 2018		**8**	
	N Vodopivec, E Miller-Hooks: Transit system resilience: Quantifying the impacts of disruptions on diverse populations, Reliability Engineering & System Safety, 2019		**8**	

	UEFISCDI 2019			
	HS Sánchez, D Rotondo, T Escobet, V Puig: Bibliographical review on cyber attacks from a control oriented perspective, Annual reviews in control, 2019 UEFISCDI 2019		**8**	
	Q Zhu, Y Qin, C Zhou, L Fei: Hierarchical Flow Model-Based Impact Assessment of Cyberattacks for Critical Infrastructures, IEEE Systems Journal, 2019 UEFISCDI 2019		**8**	
	I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, 2015	618-627		
	Hamid Reza Ghaeini and Nils Ole Tippenhauer. 2016. HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC '16), 2016 Workshop CCS (A*) CORE2017		**8**	
	N Tuptuk, S Hailes: Security of smart manufacturing systems, Journal of Manufacturing Systems, 2018 UEFISCDI 2018		**8**	
	CY Lin, S Nadjm-Tehrani: Timing Patterns and Correlations in Spontaneous {SCADA} Traffic for Anomaly Detection, 22nd International Symposium on Research in Attacks, Intrusions and Defenses ({RAID} 2019) CORE2018		**8**	
	C Wressnegger, A Kellner: Zoe: Content-based anomaly detection for industrial control systems, 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) CORE2018		**8**	
	Y Hu, Y Sun, Y Wang, Z Wang: An Enhanced Multi-Stage Semantic Attack Against Industrial Control Systems, IEEE Access, 2019		**8**	
	I. Kiss, B. Genge, P. Haller, and G. Sebestyen: Data clustering-based anomaly detection in industrial control systems. 2014 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September, pp. 275-281, 2014	628-635		
	M Wan, W Shang, P Zeng: Double Behavior Characteristics for One-Class Classification Anomaly Detection in Networked Control Systems, IEEE Transactions on Information Forensics and Security, 2017. UEFISCDI 2017		**4**	
	Q Chen, A Zhang, T Huang, Q He, Y Song: Imbalanced dataset-based echo state networks for anomaly detection, Neural Computing and Applications, 2018 UEFISCDI 2018		**4**	
	C. Siaterlis, B. Genge, and M. Hohenadel: EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 319-330, 2013.	636-643		
	S. Ntalampiras, Y. Soupionis, and G. Giannopoulos: A fault diagnosis system for interdependent critical infrastructures based on HMMs.		**8**	

	Reliability Engineering & System Safety, vol. 138, pp. 73-81, 2015. UEFISCDI 2015			
	G. Koutsandria, R. Gentz, M. Jamei, A. Scaglione, S. Peisert, C. McParland: A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid, Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, pp. 67-78, 2015. Workshop CCS (A*) CORE2017		**8**	
	P Gunathilaka, D Mashima, B Chen: SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions, CPS-SPC '16 Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pp. 113-124, Vienna, Austria, 2016. Workshop CCS (A*) CORE2017		**8**	
	X Zhou, X Gou, T Huang, S Yang: Review on Testing of Cyber Physical Systems: Methods and Testbeds, IEEE Access, 2018 UEFISCDI 2018		**8**	
	T Alves, R Das, A Werth, T Morris: Virtualization of SCADA testbeds for cybersecurity research: A modular approach, Computers & Security, 2018 UEFISCDI 2018		**8**	
	B. Genge, C. Siaterlis, and M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228-239, 2012.	657-662		
	S. Ntalampiras, Y. Soupionis, and G. Giannopoulos: A fault diagnosis system for interdependent critical infrastructures based on HMMs. Reliability Engineering & System Safety, vol. 138, pp. 73-81, 2015. UEFISCDI 2015		**8**	
	P Gunathilaka, D Mashima, B Chen: SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions, CPS-SPC '16 Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pp. 113-124, Vienna, Austria, 2016. Workshop CCS (A*) CORE2017		**8**	
	T Alves, T Morris: OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research, Computers & Security, 2018 UEFISCDI 2018		**8**	
	A Ashok, S Sridhar, T Becejac, T Rice: A multi-level fidelity microgrid testbed model for cybersecurity experimentation, 12th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 19) Workshop USENIX Security (A*) CORE2018		**8**	
	MM Yamin, B Katt, V Gkioulos: Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture, Computers & Security, 2019 UEFISCDI 2019		**8**	
	B. Genge, P. Haller, I. Kiss: Cyber Security-Aware Network Design of Industrial Control Systems, IEEE Systems Journal, 11(3), pp.1373-1384,	663-668		

	2017.			
	Jiang, X., Chen, X., Hu, J., Yan, H. and Ge, M., 2019. On the achievable tracking performance of NCSs over SNR limited channels. Journal of the Franklin Institute Vol. 356, Issue 6, pp. 3353-3367, 2019 UEFISCDI 2019		**8**	
	Hassani, H., Zarei, J., Razavi-Far, R. and Saif, M., 2019. Robust Interval Type-2 Fuzzy Observer for Fault Detection of Networked Control Systems Subject to Immeasurable Premise Variables. IEEE Systems Journal, 2019 UEFISCDI 2019		**8**	
	B. Chen; D. W. C. Ho; W. A. Zhang; L. Yu, Distributed Dimensionality Reduction Fusion Estimation for Cyber-Physical Systems Under DoS Attacks, in IEEE Transactions on Systems, Man, and Cybernetics: Systems , vol.49, no.2, pp.1-14, 2017 UEFISCDI 2017		**8**	
	J Yang, C Zhou, YC Tian, SH Yang: A software-defined security approach for securing field zones in industrial control systems, IEEE Access 2019 UEFISCDI 2019		**8**	
	B. Genge, C. Siaterlis, and M. Hohenadel: Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems. International Journal of Computers, Communications & Control, vol. 7, no. 4, pp. 673-686, 2012.	675-680		
	M. Krotofil, A. Cárdenas, and J. Larsen: CPS: driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals. ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference, pp. 146-155, 2014. CORE2014		**8**	
	Hamed Orojlo, Mohammad Abdollahi Azgomi: A method for evaluating the consequence propagation of security attacks in cyber–physical systems, Future Generation Computer Systems, vol. 67, pp. 57-71, 2017. UEFISCDI 2017		**8**	
	R Alguliyev, Y Imamverdiyev, L Sukhostat: Cyber-physical systems and their security issues, Computers in Industry, 2018. UEFISCDI 2018		**8**	
	B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera: Analyzing Cyber-Physical Attacks on Networked Industrial Control Systems. Hannover, New Hampshire, USA, 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection V, vol. 367, Revised Selected Papers, Springer, pp. 167-183, 2011.	681-685		
	S.K. Khaitan, and J.D. McCalley: Design Techniques and Applications of Cyberphysical Systems: A Survey, Systems Journal, IEEE , vol. 9, no. 2, pp. 1-16, 2015. UEFISCDI 2015		**4**	
	B Bordel, R Alcarria, T Robles, Á Sánchez-Picot: Stochastic and information theory techniques to reduce large datasets and detect		**4**	

	cyberattacks in Ambient Intelligence Environments, IEEE Access, 2018 UEFISCDI 2018			
	B. Genge, C. Siaterlis, and G. Karopoulos: Data Fusion-Based Anomaly Detection in Networked Critical Infrastructures. 43th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013), Workshop on Reliability and Security Data Analysis (RSDA 2013), Budapest, Hungary, pp. 1-8, 2013.	686-690		
	A. Khalili, and A. Sami: SysDetect: A systematic approach to critical state determination for Industrial Intrusion Detection Systems using Apriori algorithm, Volume 32, Journal of Process Control, pp. 154–160, August 2015. UEFISCDI 2015		**8**	
	B. Chen; D. W. C. Ho; W. A. Zhang; L. Yu, "Distributed Dimensionality Reduction Fusion Estimation for Cyber-Physical Systems Under DoS Attacks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems , vol.PP, no.99, pp.1-14, 2017 UEFISCDI 2017		**8**	
	A Khalili, A Sami, A Khozaei, S Pouresmaeeli: SIDS: State-based intrusion detection for stage-based cyber physical systems, International Journal of Critical Infrastructure Protection, 2018 UEFISCDI 2018		**8**	
	M Eckhart, A Ekelhart: Towards security-aware virtual environments for digital twins, CPSS '18 Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, 2018 Workshop CCS (A*) CORE2018		**8**	
	B. Genge, F. Graur, P. Haller: Experimental Assessment of Network Design Approaches for Protecting Industrial Control Systems, International Journal of Critical Infrastructure Protection, Elsevier, vol. 11, pp. 24-38, 2015.	696-700		
	J. P. Chapman, S. Ofner and P. Pauksztelo, Key Factors in Industrial Control System Security, 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, pp. 551-554, 2016 CORE2017		**8**	
	EN Yilmaz, S Gönen: Attack detection/prevention system against cyber attack in industrial control systems, Computers & Security, vol. 77, pp. 94-105, 2018 UEFISCDI 2018		**8**	
	Jie, X., Wang, H., Fei, M., Du, D., Sun, Q., & Yang, T. C. (2018). Anomaly behavior detection and reliability assessment of control systems based on association rules. International Journal of Critical Infrastructure Protection, vol. 22, pp. 90-99, 2018 UEFISCDI 2018		**8**	
	T Cherifi, L Hamami: A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol, International Journal of Critical Infrastructure Protection, vol. 20, pp68-84, 2018 UEFISCDI 2018		**8**	

	MR Asghar, Q Hu, S Zeadally: Cybersecurity in industrial control systems: Issues, technologies, and challenges, Computer Networks, 2019 UEFISCDI 2019		**8**	
	CV Martinez, B Vogel-Heuser: A Host Intrusion Detection System architecture for embedded industrial devices, Journal of the Franklin Institute, 2019 UEFISCDI 2019		**8**	
	B. Genge, A. Beres, and P. Haller: A Survey on Cloud-based Software Platforms to Implement Secure Smart Grids. 49th IEEE International Universities' Power Engineering Conference, Cluj-Napoca, Romania, September, pp. 1-6, 2014	701-704		
	K Zhou, S Yang: A framework of service-oriented operation model of China's power system, Renewable and Sustainable Energy Reviews, Volume 50, October 2015, pp. 719–725, 2015. UEFISCDI 2015		**8**	
	B. Genge, D.A. Rusu, and P. Haller: A Connection Pattern-based Approach to Detect Network Traffic Anomalies in Critical Infrastructures. 2014 ACM European Workshop on System Security (EuroSec2014), Amsterdam, The Netherlands, pp. 1-6, 2014.	691-695		
	J. P. Chapman, S. Ofner and P. Pauksztelo, "Key Factors in Industrial Control System Security," 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, pp. 551-554, 2016 CORE2017		**8**	
	Hamid Reza Ghaeini and Nils Ole Tippenhauer. 2016. HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC '16), 2016 Workshop CCS (A*) CORE2017		**8**	
	B. Genge, P. Haller: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016.	705-708		
	JA Puente Fernández, LJ García Villalba, TH Kim: Clustering and Flow Conservation Monitoring Tool for Software Defined Networks, SENSORS, vol 18(4), 2018 UEFISCDI 2018		**8**	
	K Zheng, X Wang, J Liu: DISCO: Distributed traffic flow consolidation for power efficient data center network, IFIP Networking Conference (IFIP Networking) and Workshops, 2017. CORE2017		**8**	
	MA Togou, DA Chekired, L Khoukhi: A Hierarchical Distributed Control Plane for Path Computation Scalability in Large Scale Software-Defined Networks, IEEE Transactions on Network and Service Management, 2019 UEFISCDI 2019		**8**	
	J Yang, C Zhou, YC Tian, SH Yang: A software-defined security approach for securing field zones in industrial control systems, IEEE Access 2019		**8**	

	UEFISCDI 2019			
	P. Haller, B. Genge: Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems, IEEE Access, vol. 5, pp. 9336-9347, 2017.	709-711		
	C Jiang, F Zhang, Z Wang: Image Processing of Aluminum Alloy Weld Pool for Robotic VPPAW Based on Visual Sensing, IEEE Access, 2017 UEFISCDI 2017		**8**	
	PK Muhuri, AK Shukla, A Abraham: Industry 4.0: A bibliometric analysis and detailed overview, Engineering Applications of Artificial Intelligence Volume 78, February 2019, Pages 218-235 UEFISCDI 2019		**8**	
	R Fu, X Huang, Y Xue, Y Wu, Y Tang, D Yue: Security assessment for cyber physical distribution power system under intrusion attacks, IEEE Access, 2019 UEFISCDI 2019		**8**	
	P Schneider, K Böttinger: High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks, CPS-SPC '18 Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy Workshop CCS (A*) CORE2018		**8**	
	Y Hu, Y Sun, Y Wang, Z Wang: An Enhanced Multi-Stage Semantic Attack Against Industrial Control Systems, IEEE Access, 2019 UEFISCDI 2019		**8**	
	J Yang, C Zhou, YC Tian, SH Yang: A software-defined security approach for securing field zones in industrial control systems, IEEE Access 2019 UEFISCDI 2019		**8**	
	B. Genge, P. Haller, I. Kiss: A Framework for Designing Resilient Intrusion Detection Systems for Critical Infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, Volume 15, December, pp. 3-11, 2016.	712-714		
	Palleti, V. R., Joseph, J. V., & Silva, A., A contribution of axiomatic design principles to the analysis and impact of attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 23, pp. 21-32, 2018. UEFISCDI 2018		**8**	
	H. Sandor, B. Genge, G. Sebestyen: Resilience in the Internet of Things: The Software Defined Networking Approach, IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 545-552, 2015.	715-717		
	T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh and H. C. Chao, "Defending Against New-Flow Attack in SDN-Based Internet of Things," in IEEE Access, vol. 5, no. , pp. 3431-3443, 2017. UEFISCDI 2017		**8**	
	M Ge, JB Hong, SE Yusuf, DS Kim: Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities, Future Generation Computer Systems, 2018 UEFISCDI 2018		**8**	
	O Salman, I Elhajj, A Chehab, A Kayssi: IoT survey: An SDN and fog computing perspective, Computer Networks, 2018 UEFISCDI 2018		**8**	
	B. Genge, and C. Siaterlis: Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future Smart Grid. IEEE PES Innovative Smart Grid Technologies, Manchester, UK, pp. 1-7, 2011.	721-722		

	Prageeth Gunathilaka, Daisuke Mashima, and Binbin Chen. 2016. SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC '16). ACM, New York, NY, USA, 113-124. Workshop CCS (A*) CORE2017		**8**	
	S.K. Khaitan, and J.D. McCalley: Design Techniques and Applications of Cyberphysical Systems: A Survey, Systems Journal, IEEE , vol. 9, no. 2, pp.1-16, 2015. UEFISCDI 2015		**8**	
	Angelo Furfaro, Luciano Argento, Andrea Parise, Antonio Piccolo, Using virtual environments for the assessment of cybersecurity issues in IoT scenarios, Simulation Modelling Practice and Theory, Volume 73, April 2017, Pages 43-54. UEFISCDI 2017		**8**	
	B. Genge, and C. Siaterlis: An Experimental Study on the Impact of Network Segmentation to the Resilience of Physical Processes. Networking 2012, Prague, Czech Republic, Lecture Notes in Computer Science 7289 Springer 2012, pp. 121-134, 2012.	727-728		
	M. Krotofil, A. Cárdenas, and J. Larsen: CPS: driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals. ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference, pp. 146-155, 2014. CORE2014		**8**	
	Hamed Orojloo, Mohammad Abdollahi Azgomi, A method for evaluating the consequence propagation of security attacks in cyber–physical systems, Future Generation Computer Systems, Volume 67, February 2017, Pages 57-71 UEFISCDI 2017		**8**	
	A. Beres, B. Genge, and I. Kiss: A Brief Survey on Smart Grid Data Analysis in the Cloud. 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Tirgu Mures, Romania, vol. 19, Procedia Technology, pp. 858–865, 2015.	729-730		
	Maria Lorena Tuballa, Michael Lochinvar Abundo, A review of the development of Smart Grid technologies, Renewable and Sustainable Energy Reviews, Volume 59, June 2016, Pages 710-725 UEFISCDI 2016		**8**	
	Baling Fang, Xiang Yin, Yi Tan, Canbing Li, Yunpeng Gao, Yijia Cao, Jianliang Li, The contributions of cloud technologies to smart grid, Renewable and Sustainable Energy Reviews, Volume 59, 2016, Pages 1326-1331. UEFISCDI 2016		**8**	
	H. Sandor, B. Genge, Z. Gal: Security Assessment of Modern Data Aggregation Platforms in the Internet of Things, International Journal Of Information Security Science, Vol.4, No.3, 2017	735		
	B Pourghebleh, NJ Navimipour: Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research, Journal of Network and Computer Applications 2017 UEFISCDI 2017		**8**	
	Z. Gal, H. Sandor, B. Genge: Information flow and complex event processing of the sensor network communication, 2015 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Gyor, Hungary, pp. 1-6, 2015.	736		

	G White, V Nallur, S Clarke: Quality of service approaches in IoT: A systematic mapping, Journal of Systems and Software, 2017. UEFISCDI 2017		**8**	
	B Genge, F Graur, C Enăchescu: Non-intrusive Techniques for Vulnerability Assessment of Services in Distributed Systems, Procedia Technology 19, 12-19, 2015	744		
	A Ahmad, J Webb, KC Desouza, J Boorman: Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack, Computers & Security, 2019 UEFISCDI 2019		**8**	
	H Sandor, B Genge, P Haller, F Graur: Software defined response and network reconfiguration for industrial control systems, International Conference on Critical Infrastructure Protection, 157-173, 2017	740		
	J Puente Fernández, L García Villalba, TH Kim: Clustering and Flow Conservation Monitoring Tool for Software Defined Networks, Sensors, 2018 UEFISCDI 2018		**4**	
	TOTAL		**644**	
3.	**A3.3 Citări provenind din publicații categoria B 4/max(1,n-2)**			
	C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013.	574-587		
	M. Tiloca, F. Racciatti and G. Din: Simulative evaluation of security attacks in networked critical infrastructures, SafeComp 2015, Computer Safety, Reliability, and Security, Lecture Notes in Computer Science Volume 9338, pp 314-323, 2015. CORE2017		**4**	
	Pang-Wei Tsai, Francesco Piccialli, Chun-Wei Tsai, Mon-Yen Luo, Chu-Sing Yang: PControl frameworks in network emulation testbeds: A survey, Journal of Computational Science, 2017. UEFISCDI 2017		**4**	
	R. Sanchez-Iborra, M.D. Cano, J. P. C. Rodrigues and J. Garcia-Haro1: An Experimental QoE Performance Study for the Efficient Transmission of High Demanding Traffic over an Ad Hoc Network Using BATMAN, Mobile Information Systems, Volume 2015 (2015), Article ID 217106, 14 pages. UEFISCDI 2015		**4**	
	N Andreadou, Y Soupionis, F Bonavitacola, G Prettico: A DSM Test Case Applied on an End-to-End System, from Consumer to Energy, Sustainability, 2018. UEFISCDI 2018		**4**	
	KR Dandekar, S Begashaw, M Jacovic: Grid Software Defined Radio Network Testbed for Hybrid Measurement and Emulation, 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2019.		**4**	
	B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera: A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. Computers and Electrical Engineering, Elsevier,	588-603		

	vol. 38, no. 5, pp. 1146-1161, 2012.			
	Han Honggui, Li Ying, and Qiao Junfei: A fuzzy neural network approach for online fault detection in waste water treatment process. Computers and Electrical Engineering, vol. 40, no. 7, pp. 2216-2226, 2014. UEFISCDI 2014		**2**	
	W. Knowles, D. Prince, D. Hutchison, J. F. Pagna Disso, and K. Jones: A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, vol. 9, pp. 52-80, June 2015. UEFISCDI 2015		**2**	
	Matthias Wachs, Nadine Herold, Stephan-A. Posselt, Florian Dold, Georg Carle: GPLMT: A Lightweight Experimentation and Testbed Management Framework, Passive and Active Measurement (PAM), pp 165-176, 2016. CORE2017		**2**	
	AF Murillo, LF Cómbita, AC Gonzalez: A Virtual Environment for Industrial Control Systems: A Nonlinear Use-Case in Attack Detection, Identification, and Response, Proceedings of the 4th Annual Industrial Control System Security Workshop, Pages 25-32, 2018. Workshop ACSAC (A) CORE2018		**2**	
	R Leszczyna: Standards on cyber security assessment of smart grid, International Journal of Critical Infrastructure Protection, 2018. UEFISCDI 2018		**2**	
	SD Anton, S Kanoor, D Fraunholz: Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/tcp data set, ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018 CORE2018		**2**	
	B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015	604-617		
	Zhu, Q., Qin, Y., Zhou, C., & Gao, W., Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems. *International Journal of Distributed Sensor Networks*, *14*(6), 2018. UEFISCDI 2018		**4**	
	R Alguliyev, Y Imamverdiyev, L Sukhostat: Cyber-physical systems and their security issues, Computers in Industry, vol 100, pp. 212-223, 2018. UEFISCDI 2018		**4**	
	Shi, L., Dai, Q., & Ni, Y., Cyber–physical interactions in power systems: A review of models, methods, and applications. Electric Power Systems Research, 163, pp. 396-412, 2018 UEFISCDI 2018		**4**	
	Siwar Kriaa, Marc Bouissou, Youssef Laarouchi: A new safety and security risk analysis framework for industrial control systems, Proceedings of the Institution of Mechanical Engineers Part O-Journal of Risk and Reliability, 2018. UEFISCDI 2018		**4**	
	D Hayes, F Cappa: Open-source intelligence for risk assessment, Business Horizons, vol 61(5), pp. 689-697, 2018 UEFISCDI 2018		**4**	
	NSV Rao, CYT Ma, F He: Defense strategies for multi-site cloud		**4**	

	computing server infrastructures, ICDCN '18 Proceedings of the 19th International Conference on Distributed Computing and Networking, 2018 CORE2017			
	JW Galbraith, L Iuliani: Measures of Robustness for Networked Critical Infrastructure: an Empirical Comparison on Four Electrical Grids, International Journal of Critical Infrastructure Protection, 2019 UEFISCDI 2019		**4**	
	H Esquivel-Vargas, M Caselli, E Tews, D Bucur: BACRank: Ranking building automation and control system components by business continuity impact, International Conference on Computer Safety, Reliability, and Security (SafeComp), 2019 CORE2018		**4**	
	R Lanotte, M Merro, S Tini: Towards a formal notion of impact metric for cyber-physical attacks, International Conference on Integrated Formal Methods (IFM), 2018 CORE2018		**4**	
	A Sardi, E Sorano: Dynamic Performance Management: An Approach for Managing the Common Goods, Sustainability, 2019 UEFISCDI 2019		**4**	
	I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, 2015	618-627		
	Ghaeini, H.R., Antonioli, D., Brasser, F., Sadeghi, A.R. and Tippenhauer, N.O., State-aware anomaly detection for industrial control systems. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1620-1628, 2018. CORE2018		**4**	
	M. Iturbe, J. Camacho, I. Garitano, U. Zurutuza and R. Uribeetxeberria, "On the Feasibility of Distinguishing Between Process Disturbances and Intrusions in Process Control Systems Using Multivariate Statistical Process Control," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), Toulouse, pp. 155-160, 2016 Workshop DSN (A) CORE2017		**4**	
	Y Hu, A Yang, H Li, Y Sun: A survey of intrusion detection on industrial control systems, International Journal of Distributed Sensor Networks, 2018 UEFISCDI 2018		**4**	
	J Liu, L Yin, Y Hu, S Lv, L Sun: A Novel Intrusion Detection Algorithm for Industrial Control Systems Based on CNN and Process State Transition, 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC) CORE2018		**4**	
	PHN Rajput, P Rajput, M Sazos: Process-Aware cyberattacks for thermal desalination plants, Asia CCS '19 Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019 CORE2018		**4**	
	I. Kiss, B. Genge, P. Haller, and G. Sebestyen: Data clustering-based	628-		

	anomaly detection in industrial control systems. 2014 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September, pp. 275-281, 2014	635		
	Hu, Y., Yang, A., Li, H., Sun, Y. and Sun, L., 2018. A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks, 14(8), 2018. UEFISCDI 2018		**2**	
	Xing, B., Jiang, Y., Liu, Y. and Cao, S., Risk Data Analysis Based Anomaly Detection of Ship Information System. Energies, 11(12), pp.3403, 2018. UEFISCDI 2018		**2**	
	I Bermudez, A Tongaonkar, M Iliofotou, M Mellia: Towards automatic protocol field inference, Computer Communications, vol. 84, pp. 40-51, 2016. UEFISCDI 2018		**2**	
	C. Siaterlis, B. Genge, and M. Hohenadel: EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 319-330, 2013.	636-643		
	G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, D. Gritzalis: Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. International Journal of Critical Infrastructure Protection, vol. 12, pp. 46-60, 2016. UEFISCDI 2016		**4**	
	SD Anton, S Kanoor, D Fraunholz: Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/tcp data set, ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018 CORE2018		**4**	
	B. Genge, C. Enachescu: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks, Wiley, Volume 9, Issue 15, pp. 2696-2714, 2016.	644-650		
	Simon K. (2016) Vulnerability Analysis Using Google and Shodan. In: Foresti S., Persiano G. (eds) Cryptology and Network Security. CANS 2016. Lecture Notes in Computer Science, vol 10052. Springer, Cham CORE2017		**4**	
	H Kim, T Kim, D Jang: An Intelligent Improvement of Internet-Wide Scan Engine for Fast Discovery of Vulnerable IoT Devices, Symmetry, 2018 UEFISCDI 2017		**4**	
	B. Genge, C. Siaterlis, and M. Hohenadel: Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems. International Journal of Computers, Communications & Control, vol. 7, no. 4, pp. 673-686, 2012.	675-680		
	H Orojloo, MA Azgomi: A Stochastic Game Model for Evaluating the Impacts of Security Attacks Against Cyber-Physical Systems, Journal of Network and Systems Management, 2018 UEFISCDI 2018		**4**	
	B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera: Analyzing Cyber-Physical Attacks on Networked Industrial Control Systems. Hannover, New	681-685		

	Hampshire, USA, 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection V, vol. 367, Revised Selected Papers, Springer, pp. 167-183, 2011.			
	I Ahmed, V Roussev, W Johnson, S Senthivel: A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy, ICSS '16 Proceedings of the 2nd Annual Industrial Control System Security Workshop, pp. 1-9, 2016. Workshop ACSAC (A) CORE2017		**2**	
	HS Kang, JY Lee, SS Choi, H Kim, JH Park: Smart manufacturing: Past research, present findings, and future directions, International Journal of Precision Engineering and Manufacturing-Green Technology, vol. 3, no. 1, pp. 111-128, 2016. UEFISCDI 2016		**2**	
	B. Genge, A. Beres, and P. Haller: A Survey on Cloud-based Software Platforms to Implement Secure Smart Grids. 49th IEEE International Universities' Power Engineering Conference, Cluj-Napoca, Romania, September, pp. 1-6, 2014	701-704		
	Y Xie, J Wu, Y Jiang, H Wen, J Meng, X Guo, A Xu: Three-Layers Secure Access Control for Cloud-based Smart Grids, IEEE 82nd Vehicular Technology Conference, Sept. 2015. CORE2017		**4**	
	B. Genge, D.A. Rusu, and P. Haller: A Connection Pattern-based Approach to Detect Network Traffic Anomalies in Critical Infrastructures. 2014 ACM European Workshop on System Security (EuroSec2014), Amsterdam, The Netherlands, pp. 1-6, 2014.	691-695		
	A Amrein, V Angeletti, A Beitler: Security intelligence for industrial control systems, IBM Journal of Research and Development , vol. 60(4), pp. 1-12, 2016. UEFISCDI 2016		**4**	
	H. Sandor, B. Genge, G. Sebestyen: Resilience in the Internet of Things: The Software Defined Networking Approach, IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 545-552, 2015.	715-717		
	G Knieps: Internet of Things, big data and the economics of networked vehicles, Telecommunications Policy, 2019 UEFISCDI 2019		**4**	
	B. Genge, P. Haller, A. Gligor, A. Beres: An Approach for Cyber Security Experimentation Supporting Sensei/IoT for Smart Grid. Second International Symposium on Digital Forensics and Security, Houston, Texas, USA, pp. 37-42, May 2014	718-720		
	Ming Liu, Yang Xu, Haixiao Hu, and Abdul-Wahid Mohammed: Semantic Agent-Based Service Middleware and Simulation for Smart Cities, Sensors 2016, 16(12). UEFISCDI 2016		**2**	
	P Haller, B Genge, AV Duka: On the practical integration of anomaly detection techniques in industrial control applications, International	738		

	Journal of Critical Infrastructure Protection 24, 48-68, 2019			
	T Karimireddy, S Zhang: A Hybrid Method for Secure and Reliable Transmission on Industrial Automation and Control Networks in Industry 4.0, 2019 25th International Conference on Automation and Computing (ICAC) UEFISCDI 2019		**4**	
	B Genge, P Haller, AV Duka: Engineering security-aware control applications for data authentication in smart industrial cyber–physical systems, Future Generation Computer Systems 91, 206-222, 2019	742		
	Y Liu, X Liu, A Liu, NN Xiong, F Liu: A Trust Computing-based Security Routing Scheme for Cyber Physical Systems, ACM Transactions on Intelligent Systems and Technology (TIST) – Special Section on Intelligent Edge Computing for Cyber Physical and Cloud Systems and Regular Papers Volume 10 Issue 6, December 2019 UEFISCDI 2019		**4**	
	TOTAL		**144**	
4.	**A3.4 Citări provenind din publicații categoria C** **2/max(1,n-2)**			
	C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013.	574-587		
	H. Holm, M. Karresand, A. Vidström, E. Westring: A Survey of Industrial Control System Testbeds. Secure IT Systems, Volume 9417 of the series Lecture Notes in Computer Science, pp. 11-26, 2015. LNCS		**2**	
	K. Borisenko, I. Kholod, A. Shorov: Framework for Infrastructure Attack Modeling in Hybrid Networks, International Journal of Mobile Computing and Multimedia Communications, vol. 6, no. 4, 2014. Indexare SCOPUS		**2**	
	BB Gupta, T Akhtar: A survey on smart power grid: frameworks, tools, security issues, and solutionsm, Annals of Telecommunications, 2017. UEFISCDI 2017		**2**	
	B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera: A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. Computers and Electrical Engineering, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012.	588-603		
	F Baiardi, F Tonelli, L Guidi, D Pestonesi, V. Angeletti: Assessing and managing the information and communication risk of power generation, Computers and Electrical Engineering, vol. 47, pp. 286-298, 2015. UEFISCDI 2015		**1**	
	Ming Wan, Wenli Shang, Linghe Kong, Peng Zeng: Content-based deep communication control for networked control system, Telecommunication Systems, Vol. 65, no. 1, pp. 155-168, 2016. UEFISCDI 2016		**1**	
	M Almgren, P Andersson, G Björkman: RICS-el: Building a National Testbed for Research and Training on SCADA Security (Short Paper), International Conference on Critical Information Infrastructures		**1**	

	Security (CRITIS), pp 219-225, 2018. CORE2018			
	A Gawanmeh, A Alomari: Taxonomy analysis of security aspects in cyber physical systems applications, 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018. Workshop ICC (B) CORE2018		**1**	
	H Gao, J Li, J Cheng: Industrial Control Network Security Analysis and Decision-Making by Reasoning Method Based on Strong Relevant Logic, 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) CORE2018		**1**	
	B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015	604-617		
	Rubio-Hernan, J., De Cicco, L., & Garcia-Alfaro, J., Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems. Transactions on Emerging Telecommunications Technologies, 29(7), e3209, 2018 UEFISCDI 2018		**2**	
	YOO, S. K., & BAIK, D. K., Comprehensive Damage Assessment of Cyberattacks on Defense Mission Systems. IEICE TRANSACTIONS on Information and Systems, 102(2), pp. 402-405, 2019 UEFISCDI 2019		**2**	
	Kang, W., Zhu, P., Zhang, J., & Zhang, J., Critical Nodes Identification of Power Grids Based on Network Efficiency. IEICE TRANSACTIONS on Information and Systems, 101(11), pp. 2762-2772, 2018. UEFISCDI 2019		**2**	
	Y Deng, L Song, Z Zhou, P Liu: Complexity and Vulnerability Analysis of Critical Infrastructures: A Methodological Approach, Mathematical Problems in Engineering, 2017. UEFISCDI 2017		**2**	
	A Marjanian, S Soleymani: Optimal investment in power system for defending against malicious attacks through defender-attacker-defender model and mixed strategy Nash equilibrium, International Journal of Critical Infrastructures, 2017 Indexare SCOPUS		**2**	
	Hemangi Laxman Gawand, Anup Kumar Bhattacharjee, Kallol Roy: Investigation of control theoretic cyber attacks on controllers, International Journal of Systems, Control and Communications, 2016. Indexare SCOPUS		**2**	
	H Moga, M Boscoianu, D Ungureanu: Using BDI Agents in Flexible Patterns for Cyber-Attacks over Electrical Power Infrastructures, Applied Mechanics & Materials . 2016, Vol. 841, p97-104. Indexare SCOPUS		**2**	
	H Orojloo, M Abdollahi Azgomi: Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems, Security and Communication Networks, vol 9, (18), pp 6111-6136, 2016. UEFISCDI 2016		**2**	
	I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber	618-		

	Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, 2015	627		
	Hu, Y., Li, H., Yang, H., Sun, Y., Sun, L. and Wang, Z., 2019. Detecting stealthy attacks against industrial control systems based on residual skewness analysis. EURASIP Journal on Wireless Communications and Networking, pp. 74, 2019. UEFISCDI 2019		**2**	
	Maliszewski, M., Pristerjahn, S. and Boryczka, U., DBSCAN Algorithm as a means to protect the ATM Systems. In 2018 Innovations in Intelligent Systems and Applications (INISTA), pp. 1-6, 2018. CORE2018		**2**	
	Rauter, T., Iber, J. and Kreiner, C., 2018. Integrating Integrity Reporting Into Industrial Control Systems: A Reality Check. In Solutions for Cyber-Physical Systems Ubiquity, pp. 358-382, 2018. Indexare SCOPUS		**2**	
	Durand H. A Nonlinear Systems Framework for Cyberattack Prevention for Chemical Process Control Systems †. Mathematics, vol. 6(9), pp. 169, 2018. Indexare SCOPUS		**2**	
	Hemangi Laxman Gawand, Anup Kumar Bhattacharjee, Kallol Roy: Investigation of control theoretic cyber attacks on controllers, International Journal of Systems, Control and Communications, 2016. Indexare SCOPUS		**2**	
	M Maliszewski, U Boryczka: Basic clustering algorithms used for monitoring the processes of the ATM's OS, INnovations in Intelligent SysTems and Applications (INISTA), 2017 IEEE International Conference on, 2017 CORE2017		**2**	
	M Iturbe, I Garitano, U Zurutuza: Towards Large-Scale, Heterogeneous Anomaly Detection Systems in Industrial Networks: A Survey of Current Trends, Security and Communication Networks, Volume 2017, 2017 UEFISCDI 2017		**2**	
	M Wan, Y Song, Y Jing, J Wang: Function-Aware Anomaly Detection Based on Wavelet Neural Network for Industrial Control Communication, Security and Communication Networks, 2018 UEFISCDI 2018		**2**	
	I. Kiss, B. Genge, P. Haller, and G. Sebestyen: Data clustering-based anomaly detection in industrial control systems. 2014 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September, pp. 275-281, 2014	628-635		
	Saneja, B. and Rani, R., An integrated framework for anomaly detection in big data of medical wireless sensors. Modern Physics Letters B, 32(24), 2018. Indexare SCOPUS		**1**	
	Chen, Q., Zhang, A., Huang, T., He, Q. and Song, Y., Imbalanced dataset-based echo state networks for anomaly detection. Neural Computing and Applications, pp.1-10, 2018. Indexare SCOPUS		**1**	
	Win, T.Y., Tianfield, H. and Mair, Q., Big data based security analytics for protecting virtualized infrastructures in cloud computing. IEEE		**1**	

	Transactions on Big Data, 4(1), pp.11-25, 2018. Indexare SCOPUS			
	Hemangi Laxman Gawand, Anup Kumar Bhattacharjee, Kallol Roy: Investigation of control theoretic cyber attacks on controllers, International Journal of Systems, Control and Communications, 2016. Indexare SCOPUS		**1**	
	M Iturbe, I Garitano, U Zurutuza: Towards Large-Scale, Heterogeneous Anomaly Detection Systems in Industrial Networks: A Survey of Current Trends, Security and Communication Networks, Volume 2017 UEFISCDI 2017		**1**	
	B Wang, Z Mao: One-class classifiers ensemble based anomaly detection scheme for process control systems, Transactions of the Institute of Measurement and Control, 2017 UEFISCDI 2017		**1**	
	C. Siaterlis, B. Genge, and M. Hohenadel: EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 319-330, 2013.	636-643		
	Hiecheol Kim, Won-Kee Hong, Joonhyuk Yoo, and Seong-eun Yoo: Experimental Research Testbeds for Large-Scale WSNs: A Survey from the Architectural Perspective. International Journal of Distributed Sensor Networks, Article ID 630210, 2015. UEFISCDI 2015		**2**	
	Jose Rubio-Hernan, Luca De Cicco and Joaquin Garcia-Alfaro: On the use of watermark-based schemes to detect cyber-physical attacks, EURASIP Journal on Information Security, 2017 Indexare SCOPUS		**2**	
	S Ntalampiras, Y Soupionis: Gaussian Mixture Modeling for Detecting Integrity Attacks in Smart Grids, Electronics, 5(4), 2016. Indexare SCOPUS		**2**	
	R Keidel, S Wendzel, S Zillien, ES Conner, G Haas: WoDiCoF-A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J. UCS, 2018 UEFISCDI 2018		2	
	M Almgren, P Andersson, G Björkman: RICS-el: Building a National Testbed for Research and Training on SCADA Security (Short Paper), International Conference on Critical Information Infrastructures Security (CRITIS), pp 219-225, 2018. CORE2018		**2**	
	B. Genge, C. Enachescu: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks, Wiley, Volume 9, Issue 15, pp. 2696-2714, 2016.	644-650		
	E Ko, T Kim, H Kim: Management platform of threats information in IoT environment, Journal of Ambient Intelligence and Humanized Computing, 2017 UEFISCDI 2017		**2**	
	S. Samtani, S. Yu, H. Zhu, M. Patton and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment		**2**	

	techniques," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, 2016, pp. 25-30. CORE2017			
	K Simon, C Moucha, J Keller: Contactless Vulnerability Analysis using Google and Shodan, Journal of universal computer science, vol. 23, no. 4, pp. 404-430, 2017. UEFISCDI 2017		**2**	
	Sang-Yong Choi; Daehyeok Kim; Yong-Min Kim: Journal of Information Processing Systems . Sep2016, Vol. 12 Issue 3, p422-435. Indexare SCOPUS		**2**	
	Chu Huang, Sencun Zhu, Quanlong Guan, Yongzhong He, A software assignment algorithm for minimizing worm damage in networked systems, Journal of Information Security and Applications, Volume 35, August 2017, Pages 55-67 Indexare SCOPUS		**2**	
	D Wang, X Zhang, T Chen, J Li: Discovering Vulnerabilities in COTS IoT Devices through Blackbox Fuzzing Web Management Interface, Security and Communication Networks, 2019 UEFISCDI 2019		**2**	
	A Zimba, Z Wang, M Mulenga: Cryptojacking injection: A paradigm shift to cryptocurrency-based web-centric internet attacks, J of Organizational Computing and Electronic Commerce, 2019 UEFISCDI 2019		**2**	
	S Na, T Kim, H Kim: Service Identification of Internet-Connected Devices Based on Common Platform Enumeration, Journal of Information Processing Systems, 2018 Indexare SCOPUS		**2**	
	B. Genge, C. Siaterlis, and M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228-239, 2012.	657-662		
	E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa: Using Software Defined Networking to manage and control IEC 61850-based systems. Computers and Electrical Engineering, vol. 43, pp. 142-154, 2015. UEFISCDI 2015		**2**	
	M Tiloca, F Racciatti, G Dini: Simulative Evaluation of Security Attacks in Networked Critical Infrastructures, Computer Safety, Reliability, and Security, Volume 9338 of the series Lecture Notes in Computer Science pp 314-323, 2015. LNCS		**2**	
	S Ntalampiras, Y Soupionis: Gaussian Mixture Modeling for Detecting Integrity Attacks in Smart Grids, Electronics, 5(4), 2016. Indexare SCOPUS		**2**	
	B. Genge, P. Haller, I. Kiss: Cyber Security-Aware Network Design of Industrial Control Systems, IEEE Systems Journal, 11(3), pp.1373-1384,	663-668		

	2017.			
	Mackintosh, M., Epiphaniou, G., Al-Khateeb, H., Burnham, K., Pillai, P. and Hammoudeh, M., Preliminaries of Orthogonal Layered Defence Using Functional and Assurance Controls in Industrial Control Systems. Journal of Sensor and Actuator Networks, 8(1), pp.14, 2019 Indexare SCOPUS		**2**	
	HL Gawand, AK Bhattacharjee, K Roy: Investigation of control theoretic cyber attacks on controllers, International Journal of Systems, Control and Communications, vol. 7, no. 3, 2016. Indexare SCOPUS		**2**	
	Roman Schlegel, Sebastian Obermeier, Johannes Schneider, A security evaluation of IEC 62351, Journal of Information Security and Applications, vol 34(2), pp. 197-204. 2017 Indexare SCOPUS		**2**	
	H Gao, J Li, J Cheng: Industrial Control Network Security Analysis and Decision-Making by Reasoning Method Based on Strong Relevant Logic, 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) CORE2018		**2**	
	B. Genge, and C. Siaterlis: Analysis of the Effects of Distributed Denial-of-Service Attacks on MPLS Networks. International Journal of Critical Infrastructure Protection, Elsevier, vol. 6, no. 2, pp. 87-95, 2013.	669-674		
	M. Kuchaki Rafsanjani, and N. Kazeminejad: Distributed denial of service attacks and detection mechanisms. Journal of Computational Methods in Sciences and Engineering, vol. 14, no. 6, pp. 329-345, 2015. Indexare SCOPUS		**2**	
	E Cambiaso, G Papaleo, M Aiello: Slowcomm: Design, development and performance evaluation of a new slow DoS attack, Journal of Information Security and Applications, Elsevier, vol. 35, pp. 23-31, 2017. Indexare SCOPUS		**2**	
	Rustu Yilmaz, Yildiray Yalman: A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks, TEM Journal, 2016. Indexare SCOPUS		**2**	
	A Irawan, MF Mat Jusoh: Label-QoS switching protocol for quality of service assurance in dynamic swarm robot local network, International Journal of Communication Systems, 2018 UEFISCDI 2017		**2**	
	A Irawan, MF Mat Jusoh: Label-QoS switching protocol for quality of service assurance in dynamic swarm robot local network, International Journal of Communication Systems, 2018 UEFISCDI 2018		**2**	
	B. Genge, and C. Siaterlis: Physical process resilience-aware network design for SCADA systems. Computers and Electrical Engineering, Elsevier, vol. 40, no. 1, pp. 142-157, 2014.	651-656		

	Shuang Huang, Chun-Jie Zhou , Shuang-Hua Yang, Yuan-Qing Qin: Cyber-physical system security for networked industrial processes, International Journal of Automation and Computing, vol 12, no. 6, pp. 567-578, 2015. Indexare SCOPUS		**2**	
	S. Nazir, H. Hamdoun, J. A. Alzubi, O. A. Alzubi: Cyber Attack Challenges and Resilience for Smart Grids, European Journal of Scientific Research, Vol. 134 No 1 August, pp.111-120, 2015. Indexare SCOPUS		**2**	
	B. Genge, C. Siaterlis, and M. Hohenadel: Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems. International Journal of Computers, Communications & Control, vol. 7, no. 4, pp. 673-686, 2012.	675-680		
	M. Krotofil, A. Cárdenas, J. Larsen, and D. Gollmann: Vulnerabilities of cyber-physical systems to stale data—Determining the optimal time to launch attacks. International Journal of Critical Infrastructure Protection, vol. 7, no. 4, Pages 213-232, 2014. UEFISCDI 2014		**2**	
	M. Krotofil, and A. Cárdenas: Resilience of Process Control Systems to Cyber-Physical Attacks. Secure IT Systems Lecture Notes in Computer Science Volume 8208, 2013, pp 166-182, 2013. LNCS		**2**	
	H Orojloo, M Abdollahi Azgomi: Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems, Security and Communication Networks, 2016. UEFISCDI 2016		**2**	
	M Iturbe, I Garitano, U Zurutuza: Towards Large-Scale, Heterogeneous Anomaly Detection Systems in Industrial Networks: A Survey of Current Trends, Security and Communication Networks, Volume 2017, 2017 UEFISCDI 2016		**2**	
	J Hingant, M Zambrano, FJ Pérez, I Pérez: HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection, Security and Communication Networks, 2018 UEFISCDI 2018		**2**	
	B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera: Analyzing Cyber-Physical Attacks on Networked Industrial Control Systems. Hannover, New Hampshire, USA, 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection V, vol. 367, Revised Selected Papers, Springer, pp. 167-183, 2011.	681-685		
	A. Di Pietro, S. Panzieri: Taxonomy of SCADA systems security testbeds, International Journal of Critical Infrastructures, vol. 10, no. 3-4, pp. 288-306, 2014. Indexare SCOPUS		**1**	
	B. Genge, C. Siaterlis, and G. Karopoulos: Data Fusion-Based Anomaly Detection in Networked Critical Infrastructures. 43th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN	686-690		

	2013), Workshop on Reliability and Security Data Analysis (RSDA 2013), Budapest, Hungary, pp. 1-8, 2013.			
	L. Zou, L. Zheng, and X. Zeng: Improving Accuracy of Dempster-Shafer Theory Based Anomaly Detection Systems. Sensors & Transducers, Vol. 175, Issue 7, pp. 88-94, July 2014. Indexare SCOPUS		**2**	
	S Anwar, J Mohamad Zain, MF Zolkipli, Z Inayat: From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions, Algorithms 2017, 10(2), 39. Indexare SCOPUS		**2**	
	M Iturbe, I Garitano, U Zurutuza: Towards Large-Scale, Heterogeneous Anomaly Detection Systems in Industrial Networks: A Survey of Current Trends, Security and Communication Networks, Volume 2017, 2017 UEFISCDI 2017		**2**	
	B. Genge, F. Graur, P. Haller: Experimental Assessment of Network Design Approaches for Protecting Industrial Control Systems, International Journal of Critical Infrastructure Protection, Elsevier, vol. 11, pp. 24-38, 2015.	696-700		
	A Wood, Y He, LA Maglaras: A security architectural pattern for risk management of industry control systems within critical national infrastructure, International Journal of Critical Infrastructures, 13 (2-3), pp. 113-132, 2017 Indexare SCOPUS		**2**	
	Hemangi Laxman Gawand, Anup Kumar Bhattacharjee, Kallol Roy: Investigation of control theoretic cyber attacks on controllers, International Journal of Systems, Control and Communications, vol 7(3), 2016. Indexare SCOPUS		**2**	
	Elias Molina, Eduardo Jacob, Software-defined networking in cyber-physical systems: A survey, Computers & Electrical Engineering, vol. 66, pp. 407-419, 2018. UEFISCDI 2018		**2**	
	B. Genge, D.A. Rusu, and P. Haller: A Connection Pattern-based Approach to Detect Network Traffic Anomalies in Critical Infrastructures. 2014 ACM European Workshop on System Security (EuroSec2014), Amsterdam, The Netherlands, pp. 1-6, 2014.	691-695		
	Wan, M., Song, Y., Jing, Y. and Wang, J., 2018. Function-Aware Anomaly Detection Based on Wavelet Neural Network for Industrial Control Communication. Security and Communication Networks, 2018. Indexare SCOPUS		**2**	
	S Tu, G Liu, Q Lin, L Lin, Z Sun: Security Framework based on Trusted Computing for Industrial Control Systems of CNC Machines, International Journal of Performability Engineering, 2017 Indexare SCOPUS		**2**	
	B. Genge, P. Haller: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016.	705-708		

	Mackintosh, M., Epiphaniou, G., Al-Khateeb, H., Burnham, K., Pillai, P. and Hammoudeh, M., Preliminaries of Orthogonal Layered Defence Using Functional and Assurance Controls in Industrial Control Systems. Journal of Sensor and Actuator Networks, 8(1), pp.14, 2019 Indexare SCOPUS		**2**	
	S Anwar, J Mohamad Zain, MF Zolkipli, Z Inayat: From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions, Algorithms, 10(2), 39, 2017 Indexare SCOPUS		**2**	
	Wan, M., Yao, J., Jing, Y., & Jin, X. (2018). Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. CMC-COMPUTERS MATERIALS & CONTINUA,vol 55(3), pp. 447-463, 2018 UEFISCDI 2018		**2**	
	P. Haller, B. Genge: Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems, IEEE Access, vol. 5, pp. 9336-9347, 2017.	709-711		
	G Hansch, P Schneider, GS Brost: Deriving Impact-driven Security Requirements and Monitoring Measures for Industrial IoT, CPSS '19 Proceedings of the 5th on Cyber-Physical System Security Workshop Workshop AsiaCCS (B) CORE2018		**2**	
	Hu, Y., Li, H., Yang, H., Sun, Y., Sun, L. and Wang, Z., 2019. Detecting stealthy attacks against industrial control systems based on residual skewness analysis. EURASIP Journal on Wireless Communications and Networking, pp. 74, 2019. UEFISCDI 2019		**2**	
	B. Genge, P. Haller, I. Kiss: A Framework for Designing Resilient Intrusion Detection Systems for Critical Infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, Volume 15, December, pp. 3-11, 2016.	712-714		
	Wu, X., Zhang, C., Zhang, R., Wang, Y., & Cui, J., A distributed intrusion detection model via nondestructive partitioning and balanced allocation for big data. CMC-COMPUTERS MATERIALS & CONTINUA, 56(1), 61-72, 2018 UEFISCDI 2018		**2**	
	A Alfaqiri, NUI Hossain, R Jaradat: A systemic approach for disruption risk assessment in oil and gas supply chains, International Journal of Critical Infrastructures, 2019 Indexare SCOPUS		**2**	
	B. Genge, and C. Siaterlis: Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future Smart Grid. IEEE PES Innovative Smart Grid Technologies, Manchester, UK, pp. 1-7, 2011.	721-722		
	IA Siddavatam, S Parekh, T Shah, F Kazi: Testing and Validation of Modbus/TCP Protocol for Secure SCADA Communication in CPS using Formal Methods, Scalable computing: practice and experience, 2017 Indexare SCOPUS		**2**	
	B. Genge, and C. Siaterlis: An Experimental Study on the Impact of	727-		

	Network Segmentation to the Resilience of Physical Processes. Networking 2012, Prague, Czech Republic, Lecture Notes in Computer Science 7289 Springer 2012, pp. 121-134, 2012.	728		
	M. Krotofil, A. Cárdenas, J. Larsen, D. Gollmann: Vulnerabilities of cyber-physical systems to stale data—Determining the optimal time to launch attacks. International Journal of Critical Infrastructure Protection, vol. 7, no. 4, pp. 213-232, 2014. UEFISCDI 2014		**2**	
	M. Krotofil, and A. Cárdenas: Resilience of Process Control Systems to Cyber-Physical Attacks. Secure IT Systems Lecture Notes in Computer Science, vol. 8208, pp. 166-182, 2013. LNCS		**2**	
	H Orojloo, M Abdollahi Azgomi: Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems, Security and communication networks, vol. 9, no. 18, pp. 6111–6136, 2016. UEFISCDI 2016		**2**	
	D. Gollmann, P. Gurikov, A. Isakov, M. Krotofil, J. Larsen, and A. Winnicki: Cyber-Physical Systems Security: Experimental Analysis of a Vinyl Acetate Monomer Plant. Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, pp. 1-12, Singapore, 2015. Workshop AsiaCCS (B) CORE2017		**2**	
	A. Beres, B. Genge, and I. Kiss: A Brief Survey on Smart Grid Data Analysis in the Cloud. 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Tirgu Mures, Romania, vol. 19, Procedia Technology, pp. 858–865, 2015.	729-730		
	JV de Sousa, DV Coury: A Survey on Cloud Computing Applications in Smart Distribution Systems, Electric Power Components and Systems, 2019 UEFISCDI 2019		**2**	
	B. Genge, P. Haller, C.D. Dumitru, C. Enachescu: Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids, IEEE Transactions on Smart Grid, 2017.	731-732		
	Z Uddin, A Ahmad, A Qamar: Recent advances of the signal processing techniques in future smart grids, Human-centric Computing and Information Sciences, 2018 Indexare SCOPUS		**1**	
	C. Siaterlis, and B. Genge: Theory of Evidence-based Automated Decision Making in Cyber-Physical Systems. IEEE International Conference on Smart Measurements for Future Grids, Bologna, Italy, pp.107-112, 2011.	733-734		
	R Santini, C Foglietta, S Panzieri: A graph-based evidence theory for assessing risk, Information Fusion (Fusion), 2015 18th International Conference on, pp. 1467 – 1474, Washington, DC, 2015. CORE2017		**2**	
	H. Sandor, B. Genge, Z. Gal: Security Assessment of Modern Data Aggregation Platforms in the Internet of Things, International Journal Of Information Security Science, Vol.4, No.3, 2017	735		
	M Aydos, Y Vural, A Tekerek: Assessing risks and threats with layered		**2**	

	approach to Internet of Things security, Measurement and Control, SagePub, 2019 Indexare SCOPUS			
	DA Rusu, B Genge, C Siaterlis: SPEAR: A systematic approach for connection pattern-based anomaly detection in SCADA systems, Procedia Technology 12, 168-173, 2014	741		
	DK Sadhasivan, K Balasubramanian: A novel LWCSO-PKM-based feature optimization and classification of attack types in SCADA network, Arabian Journal for Science and Engineering, August 2017, Volume 42, Issue 8, pp 3435–3449 UEFISCDI 2017		**2**	
	B Genge, C Enăchescu: Non-intrusive historical assessment of internet-facing services in the internet of things, MACRo 2015 1 (1), 25-36, 2015	744		
	SY Choi, D Kim, YM Kim: ELPA: Emulation-Based Linked Page Map Analysis for the Detection of Drive-by Download Attacks., Journal of Information Processing Systems, 2016 Indexare SCOPUS		**2**	
	H Sándor, P Haller, B Genge, Z Kátai: Optimally scheduled interventions in the presence of vulnerabilities for modern cyber-physical systems, 2017 IEEE 15th International Conference on Industrial Informatics	746		
	S Prabavathy, K Sundarakantham, SM Shalinie: Design of Cognitive Fog Computing for Autonomic Security System in Critical Infrastructure, J. UCS, 2018 UEFISCDI 2018		**1**	
	B Genge, C Enachescu: Identifying chains of software vulnerabilities: a passive non-intrusive methodology, Acta Univ Sapientiae, Elect Mech Eng 6, 68-77, 2014	749		
	C Huang, S Zhu, Q Guan, Y He: A software assignment algorithm for minimizing worm damage in networked systems, Journal of Information Security and Applications, Volume 35, August 2017, Pages 55-67 Indexare SCOPUS		**2**	
	TOTAL		**168**	
5.	**A3.5 Citări provenind din publicații categoria D** **1/max(1/n-2)**			
	C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013.	574-587		
	I. Hokelek, H.B. Celebi, R.T. Kuyuk, O. Erturk, F. Kara, and G. Vicil: TÜBİTAK BİLGEM wireless telecommunication technologies research laboratory. Signal Processing and Communications Applications Conference (SIU), 2013 21st , pp. 1-4, 2013. Indexare IEEE		**1**	
	A. Carlsson, R. Gustavsson, L. Truksans, and M. Balodis: Remote Security Labs in the Cloud ReSeLa, Global Engineering Education Conference (EDUCON), 2015 IEEE, Tallin, pp. 199-206, 2015. Indexare IEEE		**1**	
	PW Tsai, WH Fong, KW Huang, MY Luo, and CS Yang: Design and development of virtual nodes in the network testbed for emulation.		**1**	

	Communications, Computers and Signal Processing (PACRIM), 2015 IEEE Pacific Rim Conference on, pp. 101 – 106, Victoria, BC, 2015. Indexare IEEE			
	A. Furfaro, A. Piccolo, D. Saccà, and A. Parise: A virtual environment for the enactment of realistic cyber security scenarios, Cloud Computing Technologies and Applications (CloudTech), 2016 2nd International Conference on, 2016. Indexare IEEE		**1**	
	Y. Soupionis, R. Piccinelli, T. Benoist: Cyber security impact on power grid including nuclear plant, Computer Science and Information Systems (FedCSIS), 2016 Federated Conference on, 2016. Indexare IEEE		**1**	
	J. Davis, S. Magrath: A Survey of Cyber Ranges and Textbeds, DSTO-GD-0771, Technocal Report of the Australian Government, Department of Defense, October 2013. Indexare IEEE		**1**	
	Y. Soupionis, T. Benoist: Experimental platform for Internet contingencies, Security and resilience of cyber-physical infrastructures, London, UK, pp. 16-19, 2016. Workshop conferinta LNCS		**1**	
	Guido Lena Cota: Addressing selfishness in the design of cooperative systems, PhD Thesis, Lyon Franța – Milano Italia, 2017. Teză doctorat		**1**	
	Y. Soupionis, T. Benoist: Cyber-physical testbed — The impact of cyber attacks and the human factor, 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London UK, 2016. Indexare IEEE		**1**	
	MA Walker, A Dubey, A Laszka: PlaTIBART: a platform for transactive IoT blockchain applications with repeatable testing, M4IoT '17 Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things, pp. 17-22, 2017. Indexare ACM		**1**	
	NO Tippenhauer: Design and Realization of Testbeds for Security Research in the Industrial Internet of Things, In: Alcaraz C. (eds) Security and Privacy Trends in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications. Springer, Cham, 2019. Capitol carte Indexare Springer		**1**	
	M Tiloca, G Dini, F Racciatti, A Stagkopoulou: SEA++: A Framework for Evaluating the Impact of Security Attacks in OMNeT++/INET, In: Virdis A., Kirsche M. (eds) Recent Advances in Network Simulation. EAI/Springer Innovations in Communication and Computing. Springer, Cham, 2019. Capitol carte Indexare Springer		**1**	
	O Leps: Hybride Testumgebungen in der Informationssicherheit: Effiziente Sicherheitsanalysen für Industrieanlagen, In: Hybride Testumgebungen für Kritische Infrastrukturen. Springer Vieweg, Wiesbaden, 2018 Capitol carte Indexare Springer		**1**	
	B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera: A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. Computers and Electrical Engineering, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012.	588-603		

	M. Krotofil, and D. Gollmann: Industrial control systems security: What is happening?. Industrial Informatics (INDIN), 2013 11th IEEE International Conference on, pp. 670-675, 2013. Indexare IEEE		**0.5**	
	Cheng Zhi Jiang, Ting Ting Liu, and Xing Chuan Bao: A Security Test and Evaluation Model for Electric Industrial Control Systems. Applied Mechanics and Materials, Vol. 519-520, pp. 1385-1389, 2014. Indexare SCOPUS		**0.5**	
	Gilbert E. Pérez, Ivica Kostanic: Comparing a Real-Life WSN Platform Small Network and its OPNET Modeler Model using Hypothesis Testing, Journal on Systemics, Cybernetics and Informatics: JSCI, Volume 12 - Number 7, pp. 66-73, 2014. Indexare EBSCO		**0.5**	
	Z. Thornton, T. Morris: Enhancing a Virtual SCADA Laboratory Using Simulink. J. Butts and S. Shenoi (Eds.), Critical Infrastructure Protection IX IFIP Advances in Information and Communication Technology, vol. 466, pp. 119-133, Springer, 2015. Capitol carte Springer		**0.5**	
	Dean Wardell, Robert Mills, Gilbert Peterson, Mark Oxley: A Method for Revealing and Addressing Security Vulnerabilities in Cyber-physical Systems by Modeling Malicious Agent Interactions with Formal Verification, Complex Adaptive Systems conference, Los Angeles, 2016. Indexare Procedia Computer Science		**0.5**	
	E Markatos, D Balzarotti, M Almgren: The Red Book - A Roadmap for Systems Security Research, Chalmers publications, 2013. Carte Chalmers		**0.5**	
	M Savtschenko, F Schulte, S Voß: IT Governance for Cyber-Physical Systems: The Case of Industry 4.0, International Conference of Design, User Experience, and Usability, Springer Indexare Springer		**0.5**	
	CT Lin, SL Wu, ML Lee: Cyber attack and defense on industry control systems, Dependable and Secure Computing, 2017 Indexare IEEE		**0.5**	
	J Gardiner, B Craggs, B Green, A Rashid: Oops I did it again: Further adventures in the land of ICS security testbeds, Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, pp. 75-86, 2019. Indexare ACM		**0.5**	
	NO Tippenhauer: Design and Realization of Testbeds for Security Research in the Industrial Internet of Things, In: Alcaraz C. (eds) Security and Privacy Trends in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications. Springer, Cham, 2019. Capitol carte Indexare Springer		**0.5**	
	SD Antón, M Gundall, D Fraunholz: Implementing scada scenarios and introducing attacks to obtain training data for intrusion detection methods, ICCWS 2019 14th International Conference on Cyber Warfare and Security Indexare Google Books		**0.5**	
	KC Lu, IH Liu, JS Li: Venerability and Protection Tool Surveys of Industrial Control System, 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW) Indexare IEEE		**0.5**	

	SD Anton, D Fraunholz, D Krummacker: The Dos and Don'ts of Industrial Network Simulation: A Field Report, ISCSIC '18 Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control Article No. 6 Indexare ACM		**0.5**	
	B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015	604-617		
	Bîrleanu, F. G., Anghelescu, P., Bizon, N., & Pricop, E., Cyber Security Objectives and Requirements for Smart Grid. In Smart Grids and Their Communication Systems, Springer ,pp. 607-634, 2019 Capitol carte Springer		**1**	
	LF Combita, J Giraldo, AA Cardenas, and N. Quijano: Response and reconfiguration of cyber-physical control systems: A survey. Automatic Control (CCAC), 2015 IEEE 2nd Colombian Conference on, pp. 1-6, Manizales, 2015. Indexare IEEE		**1**	
	A Tofani, G D'Agostino, J Martí: Phenomenological Simulators of Critical Infrastructures, Volume 90 of the series Studies in Systems, Decision and Control pp 85-107, 2017. Capitol carte Springer		**1**	
	Asmeret Bier Naugle, Austin Silva, Munaf Aamir: Cooperation and Free Riding in Cyber Security Information-Sharing Programs, International Journal of System Dynamics Applications (IJSDA) 6(2), 2017. Indexare ISI ESCI		**1**	
	N Ghose, L Lazos, J Rozenblit: Multimodal graph analysis of cyber attacks, 2019 Spring Simulation Conference (SpringSim) Indexare IEEE		**1**	
	A Ameli, A Kirakosyan, KA Saleh: Vulnerabilities of Line Current Differential Relays to Cyber-Attacks, 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) Indexare IEEE		**1**	
	I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, 2015	618-627		
	A Rajabi, RB Bobba: False Data Detection in Distributed Oscillation Mode Estimation using Hierarchical k-means, 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) Indexare IEEE		**1**	
	E Zugasti Uriguen, I Garitano Garitano, M Iturbe Urretxa: Null is Not Always Empty: Monitoring the Null Space for Field-Level Anomaly Detection in Industrial IoT Environments, 2018 Global Internet of Things Summit, GIoTS Indexare IEEE		**1**	
	S Paul, MR Haq, A Das, Z Ni: A Comparative Study of Smart Grid Security Based on Unsupervised Learning and Load Ranking, 2019 IEEE International Conference on Electro Information Technology (EIT) Indexare IEEE		**1**	
	RB Benisha, SR Ratna: Prevention of Cyber Attacks in Control Systems: A Review, 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018		**1**	

	Indexare IEEE			
	RB Benisha, SR Ratna: Hierarchical View on Detection of Attacks in Closed Loop Control Systems, ICICI 2018: International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI), 2018 Indexare Springer		**1**	
	I. Kiss, B. Genge, P. Haller, and G. Sebestyen: Data clustering-based anomaly detection in industrial control systems. 2014 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September, pp. 275-281, 2014	628-635		
	S Warsi, Y Rai, S Kushwaha: Selective Iteration based Particle Swarm Optimization (SIPSO) for Intrusion Detection System, Selective Iteration based Particle Swarm Optimization (SIPSO) for Intrusion Detection System, International Journal of Computer Applications, Volume 124 – No.17, pp. 24-30, 2015. Indexare EBSCO		**0.5**	
	K Folkert, M Fojcik: Ontology-Based Integrated Monitoring of Hadoop Clusters in Industrial Environments with OPC UA and RESTful Web Services, Computer Networks Volume 522 of the series Communications in Computer and Information Science, pp. 162-171, 2015. Capitol carte Springer		**0.5**	
	A Maiti, AA Kist, AD Maxwell: Components relationship analysis in distributed remote laboratory apparatus with data clustering, Industrial Electronics (ISIE), 2015 IEEE 24th International Symposium on, Buzios, Rio de Janeiro, Brazil, pp. 797-802, 2015 Indexare IEEE		**0.5**	
	S Wange, SK Sahu, A Mishra: A critical analysis on intrusion detection techniques, International Journal of Advanced Technology and Engineering Exploration, vol. 3(19), pp. 77-81, 2016. Indexare ProQuest		**0.5**	
	MA Butakova, AV Chernov: Complex event processing for network anomaly detection in digital railway communication services, Telecommunication Forum (TELFOR), 2017 IEEE 25th, 2017. Indexare IEEE		**0.5**	
	K Al Jallad, M Aljnidi, MS Desouki: Big data analysis and distributed deep learning for next-generation intrusion detection system optimization, Journal of Big Data, 2019 Indexare Springer		**0.5**	
	KK Wankhade, KC Jondhale: An ensemble clustering method for intrusion detection, International Journal of Intelligent Engineering Informatics, 2019 Indexare DBLP		**0.5**	
	B Peng, Q Wang, X Li, J Cai, J Fei: Research on Abnormal Detection Technology of Real-Time Interaction Process in New Energy Network, 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) Indexare IEEE		**0.5**	

	A Krasov, L Vitkova, I Pestov: Behavioral Analysis of Resource Allocation Systems in Cloud Infrastructure, 2019 International Russian Automation Conference (RusAutoCon) Indexare IEEE		**0.5**	
	A Belkadi, P Billaudel: Real-time adaptive fault detection and isolation on a high-speed multi-injection molding machine, 2019 4th Conference on Control and Fault Tolerant Systems (SysTol), 2019 Indexare IEEE		**0.5**	
	VP Shkodyrev, KI Yagafarov: The Approach to Emergency Situation Prediction in Dynamical Systems Using Neural Networks, Proceedings of the 2018 2nd International Conference on Mechatronics Systems and Control Engineering Indexare ACM		**0.5**	
	C. Siaterlis, B. Genge, and M. Hohenadel: EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 319-330, 2013.	636-643		
	R. Liu, A. Srivastava: Integrated simulation to analyze the impact of cyber-attacks on the power grid, Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2015 Workshop on, Seattle, WA, pp. 1-6, 2015 Indexare IEEE		**1**	
	Evan Plumley, Mason Rice, Stephen Dunlap, John Pecarina: Categorization of cyber training environments for industrial control systems, International Conference on Critical Infrastructure Protection, 2017 Indexare Springer		**1**	
	S Schwab, E Kline: Cybersecurity Experimentation at Program Scale: Guidelines and Principles for Future Testbeds, 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) Indexare IEEE		**1**	
	E Kotsakis, A Lucas, N Andreadou: Recent research conducted at the SGILab towards an efficient and interoperable smart grid, 2018 AEIT International Annual Conference Indexare IEEE		**1**	
	O Salunkhe, M Gopalakrishnan, A Skoogh: Cyber-Physical Production Testbed: Literature Review and Concept Development, 8th Swedish Production Symposium, SPS 2018 Indexare Elsevier		**1**	
	Y Xie, W Wang, F Wang: VTET: A Virtual Industrial Control System Testbed for Cyber Security Research, 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC) Indexare IEEE		**1**	
	SD Antón, M Gundall, D Fraunholz: Implementing scada scenarios and introducing attacks to obtain training data for intrusion detection methods, ICCWS 2019 14th International Conference on Cyber Warfare and Security Indexare Google Books		**1**	
	SD Anton, D Fraunholz, D Krummacker: The Dos and Don'ts of Industrial		**1**	

	Network Simulation: A Field Report, ISCSIC '18 Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control Article No. 6 Indexare ACM			
	B. Genge, C. Enachescu: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks, Wiley, Volume 9, Issue 15, pp. 2696-2714, 2016.	644-650		
	Sun-young Im, S. H. Shin, Ki Yeol Ryu and Byeong-hee Roh, "Performance evaluation of network scanning tools with operation of firewall," 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), Vienna, 2016, pp. 876-881. Indexare IEEE		**1**	
	Na S., Kim T., Kim H. (2017) A Study on the Classification of Common Vulnerabilities and Exposures using Naïve Bayes. In: Barolli L., Xhafa F., Yim K. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2016. Lecture Notes on Data Engineering and Communications Technologies, vol 2. Springer, Cham Indexare Springer		**1**	
	Na S., Kim T., Kim H. (2017) A Study on the Service Identification of Internet-Connected Devices Using Common Platform Enumeration. In: Park J., Chen SC., Raymond Choo KK. (eds) Advanced Multimedia and Ubiquitous Engineering. MUE 2017, FutureTech 2017. Lecture Notes in Electrical Engineering, vol 448. Springer, Singapore Indexare Springer		**1**	
	JS Rae, MDM Chowdhury: Internet of Things Device Hardening Using Shodan. io and ShoVAT: A Survey, 2019 IEEE International Conference on Electro Information Technology (EIT) Indexare IEEE		**1**	
	J Choi, A Anwar, H Alasmary, J Spaulding: IoT malware ecosystem in the wild: a glimpse into analysis and exposures, SEC '19 Proceedings of the 4th ACM/IEEE Symposium on Edge Computing, 2019 Indexare ACM		**1**	
	YC Lin, F Wang: Machine Learning Techniques for Recognizing IoT Devices, International Computer Symposium, 2018 – Springer Indexare Springer		**1**	
	J O'Hare, R Macfarlane, O Lo: Identifying Vulnerabilities Using Internet-Wide Scanning Data, 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019 Indexare IEEE		**1**	
	V Pham, T Dang: CVExplorer: Multidimensional Visualization for Common Vulnerabilities and Exposures, 2018 IEEE International Conference on Big Data (Big Data) Indexare IEEE		**1**	
	A Hansson, M Khodari, A Gurtov: Analyzing Internet-connected industrial equipment, 2018 International Conference on Signals and Systems (ICSigSys) Indexare IEEE		**1**	

	R Egert, T Grube, D Born: AVAIN-a Framework for Automated Vulnerability Indication for the IoT in IP-based Networks, 2019 International Conference on Networked Systems (NetSys) Indexare IEEE		**1**	
	B. Genge, C. Siaterlis, and M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228-239, 2012.	657-662		
	Y. Soupionis, and T. Benoist: Demo abstract: Demonstrating cyber-attacks impact on cyber-physical simulated environment. Cyber-Physical Systems (ICCPS), 2014 ACM/IEEE International Conference on, 2014. Indexare IEEE		**1**	
	I. Heckl, P.I. Borbas, B. Szombathelyi, M. Frits: Simulator for Distribution Scheduling in Downstream, MACRo 2015. Volume 1, Issue 1, Pages 73–77, 2015. Indexare DeGruyter		**1**	
	M Tiloca, G Dini, F Racciatti, A Stagkopoulou: SEA++: A Framework for Evaluating the Impact of Security Attacks in OMNeT++/INET, In: Virdis A., Kirsche M. (eds) Recent Advances in Network Simulation. EAI/Springer Innovations in Communication and Computing. Springer, Cham, 2019. Capitol carte Indexare Springer		**1**	
	A Shahid, B Khalid, S Shaukat, H Ali: Internet of Things shaping smart cities: a survey, Internet of Things and Big Data Analytics Toward Next-Generation Intelligence, 2017 Indexare Springer		**1**	
	B. Genge, P. Haller, I. Kiss: Cyber Security-Aware Network Design of Industrial Control Systems, IEEE Systems Journal, 11(3), pp.1373-1384, 2017.	663-668		
	J Yang, C Zhou, Y Zhao: A Security Protection Approach Based on Software Defined Network for Inter-Area Communication in Industrial Control Systems, System Safety and Cyber-Security 2017 (SCSS), 12th International Conference on, 2017. Indexare IEEE		**1**	
	I Ciornei, M Albu, M Sănduleac: Adaptive distributed EMS for small clusters of resilient LVDC microgrids, 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe) Indexare IEEE		**1**	
	A Robles-Durazno, N Moradpoor: WaterLeakage: A Stealthy Malware for Data Exfiltration on Industrial Control Systems Using Visual Channels, 2019 IEEE 15th International Conference on Control and Automation (ICCA) Indexare IEEE		**1**	

	B Qi, H Zou, Y Wang, J Li: Items Selection Strategy of Cyber Security CD-CAT Based on Collaborative Filtering, 2018 IEEE 18th International Conference on Communication Technology (ICCT) Indexare IEEE		**1**	
	TA Tareke, S Datta: Automated and Cloud Enabling Cyber Security Improvement in Selected Institutions/Organizations, 2018 Second International Conference on Computing Methodologies and Communication (ICCMC) Indexare IEEE		**1**	
	Y Wang, B Qi, HX Zou, JX Li: Framework of Raising Cyber Security Awareness, 2018 IEEE 18th International Conference on Communication Technology (ICCT) Indexare IEEE		**1**	
	B. Genge, and C. Siaterlis: Analysis of the Effects of Distributed Denial-of-Service Attacks on MPLS Networks. International Journal of Critical Infrastructure Protection, Elsevier, vol. 6, no. 2, pp. 87-95, 2013.	669-674		
	Gilbert E. Pérez, Ivica Kostanic: Comparing a Real-Life WSN Platform Small Network and its OPNET Modeler Model using Hypothesis Testing, Journal on Systemics, Cybernetics and Informatics: JSCI, Volume 12 - Number 7, pp. 66-73, 2014. Indexare EBSCO		**1**	
	Anju Bhandari, V.P.Singh: Proposal and Implementation of MPLS Fuzzy Traffic Monitor, International Journal of Advanced Computer Science and Applications, vol. 7, no. 1, 2016. Indexare ISI ESCI		**1**	
	R Leszczyna: Cybersecurity Assessment, Cybersecurity in the Electricity Sector, 2019 Capitol carte Springer		**1**	
	R Leszczyna: The Current State of Cybersecurity in the Electricity Sector, Cybersecurity in the Electricity Sector, 2019 Capitol carte Springer		**1**	
	B. Genge, and C. Siaterlis: Physical process resilience-aware network design for SCADA systems. Computers and Electrical Engineering, Elsevier, vol. 40, no. 1, pp. 142-157, 2014.	651-656		
	D Kuschnerus, A Bilgic, F Bruns, T Musch: A hierarchical domain model for safety-critical cyber-physical systems in process automation, Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on, Cambridge, United Kingdom, pp. 430-436, 2015. Indexare IEEE		**1**	
	FM Enescu, N Bizon: SCADA Applications for Electric Power System, Reactive Power Control in AC Power Systems, Power Systems, pp. 561-609, 2017. Capitol carte Springer		**1**	
	FM Enescu, N Bizon, IC Hoarca: Energy Management of the Grid-Connected PV Array, Microgrid Architectures, Control and Protection Methods, 2019 Capitol carte Springer		**1**	

	FM Enescu, N Bizon, CM Moraru: Issues in Securing Critical Infrastructure Networks for Smart Grid Based on SCADA, Other Industrial Control and Communication Systems, Power Systems Resilience, 2018 Capitol carte Springer		**1**	
	KC Lu, IH Liu, JS Li: Venerability and Protection Tool Surveys of Industrial Control System, 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW) Indexare IEEE		**1**	
	KC Lu, IH Liu, JS Li: Venerability and Protection Tool Surveys of Industrial Control System, 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW) Indexare IEEE		**1**	
	KC Lu, IH Liu, MW Sun, JS Li: A Survey on SCADA Security and Honeypot in Industrial Control System, International Conference of Reliable Information and Communication Technology Indexare Springer		**1**	
	B. Genge, C. Siaterlis, and M. Hohenadel: Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems. International Journal of Computers, Communications & Control, vol. 7, no. 4, pp. 673-686, 2012.	675-680		
	M. Krotofil, and D. Gollmann: Industrial control systems security: What is happening?. Industrial Informatics (INDIN), 2013 11th IEEE International Conference on, pp. 670-675, 2013. Indexare IEEE		**1**	
	N. Mpofu, and R. Chikati: Strategy matrix for containing cyber-attacks: a generic approach. Proc. 10th International Conference on Cyber Warfare and Security ICCWS-2015, pp. 207-215, 2015. Indexare SCOPUS		**1**	
	H Orojloo, MA Azgomi: Modelling and evaluation of the security of cyber-physical systems using stochastic Petri nets, IET Cyber-Physical Systems: Theory & Applications, 2019 Indexare IEEE		**1**	
	Y Maleh, S Mohammad, D Ashraf, H Abdelkrim: Cybersecurity and Privacy in Cyber Physical Systems, Book Taylor and Francis Group Carte indexata Taylor and Francis		**1**	
	B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera: Analyzing Cyber-Physical Attacks on Networked Industrial Control Systems. Hannover, New Hampshire, USA, 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection V, vol. 367, Revised Selected Papers, Springer, pp. 167-183, 2011.	681-685		
	M. Krotofil, and D. Gollmann: Industrial control systems security: What is happening?. Industrial Informatics (INDIN), 2013 11th IEEE International Conference on , pp. 670-675, 2013. Indexare IEEE		**0.5**	
	A Di Pietro, C Foglietta, S Palmieri: Assessing the Impact of Cyber		**0.5**	

	Attacks on Interdependent Physical Systems. J. Butts and S. Shenoi (Eds.), Critical Infrastructure Protection VII IFIP Advances in Information and Communication Technology, vol. 417, Springer, 2013. Capitol carte Springer			
	Jun Wu and K. Kobara: Comparison of tools and simulators for control system security studies. Industrial Informatics (INDIN), 2012 10th IEEE International Conference on , pp. 45-50, 2012. Indexare IEEE		**0.5**	
	C Foglietta, S Panzieri, F Pascucci: Algorithms and Tools for Risk/Impact Evaluation in Critical Infrastructures. E. Kyriakides and M. Polycarpou (Eds.), Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems, Studies in Computational Intelligence, Springer, vol. 565, 2015. Capitol carte Springer		**0.5**	
	H Kavak, JJ Padilla, D Vernon-Bido: A characterization of cybersecurity simulation scenarios, CNS '16 Proceedings of the 19th Communications & Networking Symposium, 2016. Indexare ACM		**0.5**	
	M Wan, W Shang, P Zeng: Clustering-Based Self-learning Approach for Security Rules in Industrial Communication Protocol, International Conference on Mechatronics and Intelligent Robotics, 2017. Indexare Springer		**0.5**	
	B Bordel, R Alcarria, D Sánchez-de-Rivera: Protecting Industry 4.0 Systems Against the Malicious Effects of Cyber-Physical Attacks, International Conference on Ubiquitous Computing and Ambient Intelligence, 2017 Indexare Springer		**0.5**	
	H Yang, Z Zhou: A novel intrusion detection scheme using Cloud Grey Wolf Optimizer, 2018 37th Chinese Control Conference (CCC) Indexare IEEE		**0.5**	
	B. Genge, C. Siaterlis, and G. Karopoulos: Data Fusion-Based Anomaly Detection in Networked Critical Infrastructures. 43th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013), Workshop on Reliability and Security Data Analysis (RSDA 2013), Budapest, Hungary, pp. 1-8, 2013.	686-691		
	A. Di Pietro, S. Panzieri, A. Gasparri: Situational Awareness Using Distributed Data Fusion with Evidence Discounting. J. Butts and S. Shenoi (Eds.), Critical Infrastructure Protection IX IFIP Advances in Information and Communication Technology, vol. 466, pp. 281-296, Springer, 2015. Capitol carte Springer		**1**	
	RB Benisha, SR Ratna: Prevention of Cyber Attacks in Control Systems: A Review, 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018 Indexare IEEE		**1**	
	B. Genge, F. Graur, P. Haller: Experimental Assessment of Network Design Approaches for Protecting Industrial Control Systems, International	696-700		

	Journal of Critical Infrastructure Protection, Elsevier, vol. 11, pp. 24-38, 2015.			
	M Wan, Y Song, Y Jing, Z Wang, J Zhao: Software-Defined Data Flow Detection and Control Approach for Industrial Modbus/TCP Communication, International Conference on Intelligent and Interactive Systems and Applications, 2019 Indexare Springer		**1**	
	EN Ylmaz, B Ciylan, S Gönen: Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect, 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG) Indexare IEEE		**1**	
	SO Subairu, J Alhassan, S Misra: An Experimental Approach to Unravel Effects of Malware on System Network Interface, Advances in Data Sciences, Security and Applications, 2019 Indexare Springer		**1**	
	B. Genge, A. Beres, and P. Haller: A Survey on Cloud-based Software Platforms to Implement Secure Smart Grids. 49th IEEE International Universities' Power Engineering Conference, Cluj-Napoca, Romania, September, pp. 1-6, 2014	701-704		
	Y. Guo, S. Feng, K. Li, W. Mo, Y. Liu and Y. Wang, "Big data processing and analysis platform for condition monitoring of electric power system," 2016 UKACC 11th International Conference on Control (CONTROL), Belfast, pp. 1-6, 2016 Indexare IEEE		**1**	
	M. H. Cintuglu and O. A. Mohammed, "Cloud communication for remote access smart grid testbeds," 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, pp. 1-5, 2016 Indexare IEEE		**1**	
	N Popovic, M Stanojevic, I Seskar: An Optimal Placement of ADMS in Cloud Data Center, IEEE EUROCON 2019 -18th International Conference on Smart Technologies Indexare IEEE		**1**	
	S Mo, H Chen, U Kothapa: Synchrophasor Applications as a Service for Power System Operation, 2018 North American Power Symposium (NAPS) Indexare IEEE		**1**	
	A Choeichum, Y Krutgard, W Inyoo: IoT for Fault Detection in Thailand, International Conference on Internet of Things, 2019 Indexare Springer		**1**	
	B. Genge, D.A. Rusu, and P. Haller: A Connection Pattern-based Approach to Detect Network Traffic Anomalies in Critical Infrastructures. 2014 ACM European Workshop on System Security (EuroSec2014), Amsterdam, The Netherlands, pp. 1-6, 2014.	691-695		
	BooJoong Kang, Kieran McLaughlin, and Sakir Sezer. 2016. Towards a stateful analysis framework for smart grid network intrusion detection. In Proceedings of the 4th International Symposium for ICS & SCADA		**1**	

	Cyber Security Research (ICS-CSR '16), 2016 Indexare ACM			
	Antoine Lemay, Jonathan Rochon, and José M. Fernandez. 2016. A practical flow white list approach for SCADA systems. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR'16), 2016 Indexare ACM		**1**	
	RH Tsaih, SY Huang, MC Lian: ANN Mechanism for Network Traffic Anomaly Detection in the Concept Drifting Environment, 2018 IEEE Conference on Dependable and Secure Computing (DSC) Indexare IEEE		**1**	
	B. Genge, P. Haller: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016.	705-708		
	M Wan, Y Song, Y Jing, Z Wang, J Zhao: Software-Defined Data Flow Detection and Control Approach for Industrial Modbus/TCP Communication, International Conference on Intelligent and Interactive Systems and Applications, 2019 Indexare Springer 1		**1**	
	P. Haller, B. Genge: Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems, IEEE Access, vol. 5, pp. 9336-9347, 2017.	709-711		
	A Kondiloglu, H Bayer, E Celik: Information security breaches and precautions on Industry 4.0, Technology audit and production reserves, 2017 Indexare EBSCO		**1**	
	P Schneider, A Giehl: Realistic Data Generation for Anomaly Detection in Industrial Settings Using Simulations, International Workshop on Security and Privacy Requirements Engineering, 2018 Indexare Springer		**1**	
	KK Wankhade, KC Jondhale: An ensemble clustering method for intrusion detection, International Journal of Intelligent Engineering Informatics, 2019 Indexare DBLP		**1**	
	B. Genge, P. Haller, I. Kiss: A Framework for Designing Resilient Intrusion Detection Systems for Critical Infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, Volume 15, December, pp. 3-11, 2016.	712-714		
	N. Mangathayaru, G. R. Kumar and G. Narsimha, "Text mining based approach for intrusion detection," International Conference on Engineering & MIS (ICEMIS), Agadir, pp. 1-5, 2016 Indexare IEEE		**1**	
	G. R. Kumar, N. Mangathayaru and G. Narsimha, "An approach for intrusion detection using fuzzy feature clustering," 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, pp. 1-8, 2016 Indexare IEEE		**1**	
	Kumar, Gunupudi Rajesh; Mangathayaru, Nimmala; Narsimha,		**1**	

	Gugulothu: A feature clustering-based dimensionality reduction for intrusion detection (FCBDR), IADIS International Journal on Computer Science & Information Systems, Vol. 12 Issue 1, p26-44, 2017 Indexare ISI ESCI			
	Feofilovs, M., & Romagnoli, F. Resilience of critical infrastructures: probabilistic case study of Feofilovs, M., & Romagnoli, F. (2017). Resilience of critical infrastructures: probabilistic case study of a district heating pipeline network in municipality of Latvia. Energy Procedia, 128, 17-23. a district heating pipeline network in municipality of Latvia. Energy Procedia, 128, pp. 17-23, 2017. Indexare Elsevier		**1**	
	S Boudko, H Abie: Adaptive Cybersecurity Framework for Healthcare Internet of Things, 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT) Indexare IEEE		**1**	
	H. Sandor, B. Genge, G. Sebestyen: Resilience in the Internet of Things: The Software Defined Networking Approach, IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 545-552, 2015.	715-717		
	W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, 2016, pp. 1-8. Indexare IEEE		**1**	
	KE Benson, G Wang: Ride: A resilient iot data exchange middleware leveraging sdn and edge cloud resources, 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI) Indexare IEEE		**1**	
	R Kanagavelu, KMM Aung: A Survey on SDN Based Security in Internet of Things, Future of Information and Communication Conference, 2018 Indexare Springer		**1**	
	A Taurshia, JW Kathrine, D Shibin: Prognostic Views on Software Defined Networks Based Security for Internet of Things, International Conference on Applications and Techniques in Information Security, 2019 Indexare Springer		**1**	
	B. Genge, and C. Siaterlis: Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future Smart Grid. IEEE PES Innovative Smart Grid Technologies, Manchester, UK, pp. 1-7, 2011.	721-722		
	R. Santini, C. Foglietta, S. Panzieri: Evidence theory for Smart Grid diagnostics. Innovative Smart Grid Technologies Europe (ISGT EUROPE), 2013 4th IEEE/PES , pp. 1-5, 2013. Indexare IEEE		**1**	
	HA Mantooth, Y Liu, C Farnell, F Zhang: Securing DC and hybrid microgrids, DC Microgrids (ICDCM), 2015 IEEE First International Conference on, Atlanta, GA, pp. 285-286c, 2015 Indexare IEEE		**1**	

	A. Beres, B. Genge, and I. Kiss: A Brief Survey on Smart Grid Data Analysis in the Cloud. 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Tirgu Mures, Romania, vol. 19, Procedia Technology, pp. 858–865, 2015.	729-730		
	YVP Kumar, R Bhimasingu: Key Aspects of Smart Grid Design for Distribution System Automation: Architecture and Responsibilities. SMART GRID TECHNOLOGIES, Procedia Technology, Volume 21, 2015, pp. 352–359, 2015. Indexare Elsevier		**1**	
	I Kotsiuba, A Velykzhanin: Blockchain Evolution: from Bitcoin to Forensic in Smart Grids, 2018 IEEE International Conference on Big Data (Big Data) Indexare IEEE		**1**	
	C. Siaterlis, and B. Genge: Theory of Evidence-based Automated Decision Making in Cyber-Physical Systems. IEEE International Conference on Smart Measurements for Future Grids, Bologna, Italy, pp.107-112, 2011.	733-734		
	R Santini, C Foglietta, S Panzieri: Evidence theory for smart grid diagnostics, Innovative Smart Grid Technologies Europe (ISGT EUROPE), 2013 4th IEEE/PES, Lyngby, pp. 1-5, 2013. Indexare IEEE		**1**	
	R Santini, C Foglietta, S Panzieri: Evidence Theory for Cyber-Physical Systems, J. Butts and S. Shenoi (Eds.), Critical Infrastructure Protection VIII, IFIP Advances in Information and Communication Technology Volume 441, 2014, pp 95-109 Indexare Springer		**1**	
	Z. Gal, H. Sandor, B. Genge: Information flow and complex event processing of the sensor network communication, 2015 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Gyor, Hungary, pp. 1-6, 2015.	736		
	Namiot D., Sneps-Sneppe M. (2017) On Data Persistence Models for Mobile Crowdsensing Applications. In: Kalinichenko L., Kuznetsov S., Manolopoulos Y. (eds) Data Analytics and Management in Data Intensive Domains. DAMDID/RCDL 2016. Communications in Computer and Information Science, vol 706. Springer, Cham Indexare Springer		**1**	
	Y Tverdokhlib, V Dubrovin: Complex Parameters Evaluation of Wavelet Transformation, 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) Indexare IEEE		**1**	
	B Genge, F Graur, C Enăchescu: Non-intrusive Techniques for Vulnerability Assessment of Services in Distributed Systems, Procedia Technology 19, 12-19, 2015	744		
	J O'Hare, R Macfarlane, O Lo: Identifying Vulnerabilities Using Internet-Wide Scanning Data, 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019 Indexare IEEE		**1**	
	JH Kim, YS Choi, JC Na: Cybersecurity Vulnerability Scanner for Digital		**1**	

	Nuclear Power Plant Instrumentation and Control Systems, CSAI '18 Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, Pages 463-467 Indexare ACM			
	AV Duka, B Genge: Implementation of SIMON and SPECK lightweight block ciphers on programmable logic controllers, 2017 5th International Symposium on Digital Forensic and Security (ISDFS), 1-6	739		
	A Shah, M Engineer: A survey of lightweight cryptographic algorithms for iot-based applications, Smart Innovations in Communication and Computational Sciences, 2018 Capitol carte Springer		**1**	
	MA Philip: A survey on lightweight ciphers for IoT devices, 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy) Indexare IEEE		**1**	
	H Sandor, B Genge, P Haller, F Graur: Software defined response and network reconfiguration for industrial control systems, International Conference on Critical Infrastructure Protection, 157-173, 2017	740		
	J Vestin, A Kassler, J Åkerberg: FastReact: In-Network Control and Caching for Industrial Control Networks using Programmable Data Planes, 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA) Indexare IEEE		**0.5**	
	DA Rusu, B Genge, C Siaterlis: SPEAR: A systematic approach for connection pattern-based anomaly detection in SCADA systems, Procedia Technology 12, 168-173, 2014	741		
	A Lemay, J Rochon, JM Fernandez: A Practical flow white list approach for SCADA systems, 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR) Indexare ACM		**1**	
	JK Roy, SC Mukhopadhyay: Monitoring water in treatment and distribution system, Next Generation Sensors and Systems, 2016 – Springer Indexare Springer		**1**	
	H Sándor, B Genge, Z Szántó: Sensor data validation and abnormal behavior detection in the Internet of Things, 2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)	743		
	B Purnama, D Wahyudi, S Suryani: Measurement of Component Performance (Sensor) on Internet of Thing (IoT), 2018 International Conference on Electrical Engineering and Computer Science (ICECOS) Indexare IEEE		**1**	
	G. Spathoulas ; S. Evangelatos ; M. Anagnostopoulos ; G. Mema ; S. Katsikas: Detection of abnormal behavior in smart-home environments, 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) Indexare IEEE		**1**	

	K Wallis, F Schillinger, C Reich: Safeguarding Data Integrity by Cluster-Based Data Validation Network, 2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4) Indexare IEEE		**1**	
	B Genge, C Enăchescu: Non-intrusive historical assessment of internet-facing services in the internet of things, MACRo 2015 1 (1), 25-36, 2015	744		
	J O'Hare, R Macfarlane, O Lo: Identifying Vulnerabilities Using Internet-Wide Scanning Data, 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019 Indexare IEEE		**1**	
	B Genge, C Siaterlis: Investigating the effect of network parameters on coordinated cyber attacks against a simulated power plant, International Workshop on Critical Information Infrastructures Security, 140-151, 2011	745		
	T McEvoy, S Wolthusen: Agent interaction and state determination in SCADA systems, ICCIP 2012: Critical Infrastructure Protection VI pp 99-109 Indexare Springer		**1**	
	B Genge, P Haller, C Enachescu: Beyond Internet scanning: non-intrusive vulnerability assessment of Internet-facing services, International Journal of Information Security Science 4 (3), 81-91, 2015	747		
	X Li, P Avellino, J Janies: Software asset analyzer: A system for detecting configuration anomalies, MILCOM 2016 - 2016 IEEE Military Communications Conference Indexare IEEE		**1**	
	J O'Hare, R Macfarlane, O Lo: Identifying Vulnerabilities Using Internet-Wide Scanning Data, 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019 Indexare IEEE		**1**	
	TOTAL		**130.5**	
6.	**A3.6 Citări provenind din alte publicații (teze de doctorat, rapoarte de cercetare, alte forumuri)** **1/max(1,n-2)**			
	C. Siaterlis, A. Perez-Garcia, and B. Genge: On the use of Emulab testbeds for scientifically rigorous experiments. IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 929-942, 2013.	574-587		
	A Quereilhac: A generic approach to network experiment automation. PhD Thesis. Universitate Nice Sophia Antipolis, 2015. Teză doctorat		**1**	
	B. Genge, I. Kiss, and P. Haller: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015	604-617		
	Jose Manuel RUBIO HERNAN: Detection of attacks against cyber-physical industrial systems, Telecom Sudparis, 2017 Teză de doctorat		**1**	
	I. Kiss, B. Genge, P. Haller: A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems, INDIN 2015 IEEE International Conference on Industrial Informatics, 22-24 July 2015, pp. 142-148, 2015	618-627		

	DI Urbina Fuentes: Deep Packet Inspection for Physics-based Anomaly Detection in Industrial Control Systems, PhD Thesis, The University of Texas at Dallas, 2016. Teză de doctorat		**1**	
	DI Urbina, J Giraldo, AA Cardenas, J Valente, M Faisal: Survey and New Directions for Physics-Based Attack Detection in Control Systems, NIST GCR 16-010, Nov. 2016. Raport de cercetare		**1**	
	A Ghafouri: Resilient Anomaly Detection in Cyber-Physical Systems, PhD Thesis, Nashville, Tennessee, 2018 Teză de doctorat		**1**	
	X Ning: Analysis, Design and Demonstration of Control Systems Against Insider Attacks in Cyber-Physical Systems, PhD Thesis, The University of Western Ontario, 2019 Teză de doctorat		**1**	
	A. Coletta: Specification-based Predictive Continuous Monitoring for Cyber Physical Systems with Unobservables, PhD Thesis, University of Trento, 2018 Teză de doctorat		**1**	
	I. Kiss, B. Genge, P. Haller, and G. Sebestyen: Data clustering-based anomaly detection in industrial control systems. 2014 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September, pp. 275-281, 2014	628-635		
	A. Coletta: Specification-based Predictive Continuous Monitoring for Cyber Physical Systems with Unobservables, PhD Thesis, University of Trento, 2018 Teză de doctorat		**0.5**	
	N Ben Rabah: Approche Intelligente À Base De Raisonnement À Partir De Cas Pour Le Diagnostic En Ligne Des Systèmes Automatisés De Production, PhD Thesis, École Nationale des Sciences de l'Informatique (La Manouba, Tunisie) , 2018 Teză de doctorat		**0.5**	
	C. Siaterlis, B. Genge, and M. Hohenadel: EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 319-330, 2013.	636-643		
	G. Stergiopoulos: Securing Critical Infrastructures at software and interdependency levels. PhD Thesis, Department of Informatics, Athens University of Economics & Business, Athens, Greece, 2015. Teză de doctorat		**1**	
	Éric Freyssinet: Lutte contre les botnets: analyse et stratégie. PhD Thesis, Université Pierre et Marie Curie, 2015. France. Teză de doctorat		**1**	
	H Neema: Large-Scale Integration of Heterogeneous Simulations, Graduate School of Vanderbilt University, Nashville, Tennessee, 2018 Teză de doctorat		**1**	
	Guillaume BROGI: Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models, École		**1**	

	Doctorale Informatique, Télécommunications et Électronique (Paris), 2018 Teză de doctorat			
	Jose Manuel RUBIO HERNAN: Detection of attacks against cyber-physical industrial systems, Telecom Sudparis, 2017 Teză de doctorat		**1**	
	J Grover, RM Garimella: Concurrency and Synchronization in Structured Cyber Physical Systems, Cyber-Physical Systems: Architecture, Security and Application, 2019 Capitol carte Springer		**1**	
	X Ning: Analysis, Design and Demonstration of Control Systems Against Insider Attacks in Cyber-Physical Systems, PhD Thesis, The University of Western Ontario, 2019 Teză de doctorat		**1**	
	B. Genge, C. Enachescu: ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks, Wiley, Volume 9, Issue 15, pp. 2696-2714, 2016.	644-650		
	LA Dawson, C Lamb, AJ Carbajal: Industrial Control Systems Cyber Security Risk Candidate Methods Analysis, Technical report, US DoE, 2018 Raport de cercetare		**1**	
	I Sluganovic: Security of mixed reality systems: authenticating users, devices, and data, PhD thesis, Univ. of Oxford, 2018 Teză de doctorat		**1**	
	B. Genge, C. Siaterlis, and M. Hohenadel: Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems. International Journal of Computers, Communications & Control, vol. 7, no. 4, pp. 673-686, 2012.	675-680		
	X Ning: Analysis, Design and Demonstration of Control Systems Against Insider Attacks in Cyber-Physical Systems, PhD Thesis, The University of Western Ontario, 2019 Teză de doctorat		**1**	
	Hingant Gómez, JE. (2019). Arquitectura de Cyber Situational Awareness (CySA) para la protección de infraestructuras críticas [Tesis doctoral no publicada]. Universitat Politècnica de València. Teză de doctorat		**1**	
	B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera: Analyzing Cyber-Physical Attacks on Networked Industrial Control Systems. Hannover, New Hampshire, USA, 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection V, vol. 367, Revised Selected Papers, Springer, pp. 167-183, 2011.	681-685		
	Queiroz Batista da Silva: A holistic approach for measuring the survivability of SCADA systems. PhD Thesis, RMIT University, 2012. Teză de doctorat		**0.5**	
	B. Genge, F. Graur, P. Haller: Experimental Assessment of Network Design Approaches for Protecting Industrial Control Systems, International	696-700		

	Journal of Critical Infrastructure Protection, Elsevier, vol. 11, pp. 24-38, 2015.			
	RJ Pfitscher: Monitoring and identifying bottlenecks in virtual network functions service chains, Porto Alegre, 2019 Teză de doctorat		**1**	
	F Holík: Using SDN to Enhance IoT Security, University of Pardubice, 2018 Teză de doctorat		**1**	
	H. Sandor, B. Genge, G. Sebestyen: Resilience in the Internet of Things: The Software Defined Networking Approach, IEEE 11th International Conference on Intelligent Computer Communication and Processing, September 3-5, Cluj-Napoca, Romania, pp. 545-552, 2015.	715-717		
	KE Benson: Resilient Communications Middleware for IoT Data Exchange, PhD thesis, UNIVERSITY OF CALIFORNIA,IRVINE, 2018 Teză de doctorat		**1**	
	B Genge, C Siaterlis: Investigating the effect of network parameters on coordinated cyber attacks against a simulated power plant, International Workshop on Critical Information Infrastructures Security, 140-151, 2011	745		
	TR McEvoy: Context-based Anomaly Detection in Critical Infrastructures, Royal Holloway London, PhD Thesis, 2013		**1**	
	TOTAL		**23.5**	
Punctaj obținut (perspectiva A3, CNATDCU Comisia Informatică: impactul rezultatelor – perspectiva c)			**1332**	

*Dovezile de realizare a activităţii se numerotează şi se indică documentul, pagina etc. pentru o identificare uşoară. **Documentul la care se face referire prin numarul paginilor: Publicatii și contracte (doc. 5_Publicatii_Contracte_GengeBela.pdf).**

Confirm prin prezenta că datele menţionate mai sus sunt reale şi se referă la propria mea activitate profesională şi ştiinţifică. Ataşez la dosar în format tipărit / electronic toate documentele justificative care atestă rezultatele ştiinţifice declarate mai sus.

Confirm prin prezenta că datele menţionate mai sus sunt reale şi se referă la propria mea activitate profesională şi ştiinţifică. Ataşez la dosar în format tipărit / electronic toate documentele justificative care atestă rezultatele ştiinţifice declarate mai sus.

Data 8 Ianuarie 2020 Semnătură candidat _____

Avizul Comisiei de verificare a îndeplinirii standardelor

_____

Obs:

În cazul neîndeplinirii standardelor minimale necesare se menţionează în detaliu motivul:

_____

_____

_____

Membrii Comisiei de verificare a îndeplinirii standardelor:

_____ _____ _____

(nume, semnătură)