

## REFERENCES

- [1] Chensheng Liu et al. “Dynamic State Recovery for Cyber-Physical Systems Under Switching Location Attacks”. In: *IEEE Trans. Control. Netw. Syst.* 4.1 (2017). Number: 1, pp. 14–22. DOI: 10.1109/TCNS.2016.2580906.
- [2] Lin Zhang et al. “Real-Time Attack-Recovery for Cyber-Physical Systems Using Linear Approximations”. In: *41st IEEE Real-Time Systems Symposium, RTSS 2020, Houston, TX, USA, December 1-4, 2020*. IEEE, 2020, pp. 205–217. DOI: 10.1109/RTSS49844.2020.00028.
- [3] Lin Zhang et al. “Real-time Attack-recovery for Cyber-physical Systems Using Linear-quadratic Regulator”. In: *ACM Trans. Embed. Comput. Syst.* 20.5 (2021). Number: 5s, 79:1–79:24. DOI: 10.1145/3477010.
- [4] Rafael Rosales, Wael Guibene, and German Fabila Garcia. “Actor-Oriented Design Patterns for Performance Modeling of Wireless Communications in Cyber-physical Systems”. In: *Proceedings of the 14th ACM International Symposium on QoS and Security for Wireless and Mobile Networks*. Q2SWinet’18. New York, NY, USA: Association for Computing Machinery, Oct. 25, 2018, pp. 29–38. ISBN: 978-1-4503-5963-4. DOI: 10.1145/3267129.3267136. URL: <https://doi.org/10.1145/3267129.3267136> (visited on 03/23/2022).
- [5] Hugo Meyer et al. “An analytics-based method for performance anomaly classification in cyber-physical systems”. In: *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, Mar. 30, 2020, pp. 210–217. ISBN: 978-1-4503-6866-7. URL: <https://doi.org/10.1145/3341105.3373851> (visited on 03/23/2022).
- [6] Aitor Gartzia. “Microservice-based performance problem detection in cyber-physical system software updates”. In: *Proceedings of the 43rd International Conference on Software Engineering: Companion Proceedings*. IEEE Press, May 25, 2021, pp. 147–149. URL: <https://doi.org/10.1109/ICSE-Companion52605.2021.00062> (visited on 03/23/2022).
- [7] Khalil Oumimoun et al. “A Solo-Checkpointing Co-Recovery Mechanism for Reliability Improvement of Cyber-Physical Systems”. In: *64th IEEE International Midwest Symposium on Circuits and Systems, MWSCAS 2021, Lansing, MI, USA, August 9-11, 2021*. IEEE, 2021, pp. 88–91. DOI: 10.1109/MWSCAS47672.2021.9531695.
- [8] Fábio Januário, Alberto Cardoso, and Paulo Gil. “A Distributed Multi-Agent Framework for Resilience Enhancement in Cyber-Physical Systems”. In: *IEEE Access* 7 (2019), pp. 31342–31357. DOI: 10.1109/ACCESS.2019.2903629.
- [9] Zhiheng Xu, Daniel Jun Xian Ng, and Arvind Easwaran. “Automatic Generation of Hierarchical Contracts for Resilience in Cyber-Physical Systems”. In: *25th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, RTCSA 2019, Hangzhou, China, August 18-21, 2019*. IEEE, 2019, pp. 1–11. DOI: 10.1109/RTCSA.2019.8864556.
- [10] Charalambos Konstantinou et al. “Chaos Engineering for Enhanced Resilience of Cyber-Physical Systems”. In: *2021 Resilience Week (RWS)*. 2021 Resilience Week (RWS). Oct. 2021, pp. 1–10. DOI: 10.1109/RWS52686.2021.9611797.
- [11] Gongyu Wu, Meiyang Li, and Zhaojun Steven Li. “Resilience-Based Optimal Recovery Strategy for Cyber-Physical Power Systems Considering Component Multistate Failures”. In: *IEEE Trans. Reliab.* 70.4 (2021). Number: 4, pp. 1510–1524. DOI: 10.1109/TR.2020.3025179.
- [12] Francis Akowuah et al. “Recovery-by-Learning: Restoring Autonomous Cyber-physical Systems from Sensor Attacks”. In: *27th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, RTCSA 2021, Houston, TX, USA, August 18-20, 2021*. IEEE, 2021, pp. 61–66. DOI: 10.1109/RTCSA52859.2021.00015.
- [13] Robert G. Pettit IV and Aedan D. Pettit. “On the feasibility of automatically detecting and recovering from SEUs in cyber-physical space systems”. In: *Proceedings of the 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems, ICSE 2018, Gothenburg, Sweden, May 27, 2018*. Ed. by Tomás Bures et al. ACM, 2018, pp. 26–29. DOI: 10.1145/3196478.3196487.
- [14] Lorenzo Pagliari, Raffaella Mirandola, and Catia Trubiani. “A Case Study to Elicit Challenges for Performance Engineering of Cyber Physical Systems”. In: *Proceedings of the 8th ACM/SPEC on International Conference on Performance Engineering Companion*. ICPE ’17 Companion. New York, NY, USA: Association for Computing Machinery, Apr. 18, 2017, pp. 217–222. ISBN: 978-1-4503-4899-7. DOI: 10.1145/3053600.3053650. URL: <https://doi.org/10.1145/3053600.3053650> (visited on 03/23/2022).
- [15] Jubril Gbolahan Adigun et al. “Collaborative Artificial Intelligence Needs Stronger Assurances Driven by Risks”. In: *Computer* 55.3 (2022), pp. 52–63. DOI: 10.1109/MC.2021.3131990.
- [16] Matteo Camilli et al. “Risk-driven compliance assurance for collaborative ai systems: A vision paper”. In: *International Working Conference on Requirements Engineering: Foundation for Software Quality*. Springer, 2021, pp. 123–130.
- [17] Shengwei Mei, Wei Wei, and Feng Liu. “On engineering game theory with its application in power systems”. In: *Control Theory and Technology* 15.1 (2017). Publisher: Springer, pp. 1–12.

- [18] Lampros Flokas et al. “No-regret learning and mixed Nash equilibria: They do not mix”. In: *arXiv preprint arXiv:2010.09514* (2020).
- [19] Lei Cui et al. “Improving data utility through game theory in personalized differential privacy”. In: *Journal of Computer Science and Technology* 34.2 (2019). Publisher: Springer, pp. 272–286.
- [20] Amel Bennaceur et al. “Modelling and analysing resilient cyber-physical systems”. In: *Proceedings of the 14th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*. SEAMS ’19. Montreal, Quebec, Canada: IEEE Press, May 25, 2019, pp. 70–76. doi: 10.1109/SEAMS.2019.00018. URL: <https://doi.org/10.1109/SEAMS.2019.00018> (visited on 03/23/2022).
- [21] Shanshan Bi et al. “Novel cyber fault prognosis and resilience control for cyber-physical systems”. In: *IET Cyber-Phys. Syst.: Theory & Appl.* 4.4 (2019). Number: 4, pp. 304–312. doi: 10.1049/iet-cps.2018.5061.
- [22] Giuseppina Murino, Alessandro Armando, and Armando Tacchella. “Resilience of Cyber-Physical Systems: an Experimental Appraisal of Quantitative Measures”. In: *11th International Conference on Cyber Conflict, CyCon 2019, Tallinn, Estonia, May 28-31, 2019*. Ed. by Tomás Minárik et al. IEEE, 2019, pp. 1–19. doi: 10.23919/CYCON.2019.8757010.
- [23] Michel Barbeau et al. “Metrics to Enhance the Resilience of Cyber-Physical Systems”. In: *19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020, Guangzhou, China, December 29, 2020 - January 1, 2021*. Ed. by Guojun Wang et al. IEEE, 2020, pp. 1167–1172. doi: 10.1109/TrustCom50675.2020.00156.
- [24] Eskandar Kouicem, Clément Raïevsky, and Michel Occello. “Artificial Emotions for Distributed Cyber-physical Systems Resilience”. In: *Proceedings of the Cyber-Physical Systems PhD Workshop 2019, an event held within the CPS Summer School "Designing Cyber-Physical Systems - From concepts to implementation", Alghero, Italy, September 23, 2019*. Ed. by Luca Pulina. Vol. 2457. CEUR Workshop Proceedings. CEUR-WS.org, 2019, pp. 84–95. URL: <http://ceur-ws.org/Vol-2457/9.pdf> (visited on 03/16/2022).
- [25] Mohammad Shihabul Haque et al. “Contract-Based Hierarchical Resilience Management for Cyber-Physical Systems”. In: *Computer* 51.11 (2018). Number: 11, pp. 56–65. doi: 10.1109/MC.2018.2876071.
- [26] Baozhong Ti et al. “Resilience Assessment and Improvement for Cyber-Physical Power Systems Under Typhoon Disasters”. In: *IEEE Trans. Smart Grid* 13.1 (2022). Number: 1, pp. 783–794. doi: 10.1109/TSG.2021.3114512.
- [27] Sebti Mouelhi et al. “Predictive Formal Analysis of Resilience in Cyber-Physical Systems”. In: *IEEE Access* 7 (2019), pp. 33741–33758. doi: 10.1109/ACCESS.2019.2903153.
- [28] Zhaoxi Liu and Lingfeng Wang. “A Distributionally Robust Scheme for Critical Component Identification to Bolster Cyber-Physical Resilience of Power Systems”. In: *IEEE Transactions on Smart Grid* (2022). Conference Name: IEEE Transactions on Smart Grid, pp. 1–1. ISSN: 1949-3061. doi: 10.1109/TSG.2022.3147421.
- [29] Ada Bagozi, Devis Bianchini, and Valeria De Antonellis. “Context-Based Resilience in Cyber-Physical Production System”. In: *Data Sci. Eng.* 6.4 (2021). Number: 4, pp. 434–454. doi: 10.1007/s41019-021-00172-2.
- [30] Stephen Hopkins, Ezhil Kalaimannan, and Caroline Sangeetha John. “Foundations for Research in Cyber-Physical System Cyber Resilience using State Estimation”. In: *2020 SoutheastCon*. 2020 SoutheastCon. ISSN: 1558-058X. Mar. 2020, pp. 1–2. doi: 10.1109/SoutheastCon44009.2020.9249745.
- [31] Fan Fei et al. “Learn-to-Recover: Retrofitting UAVs with Reinforcement Learning-Assisted Flight Control Under Cyber-Physical Attacks”. In: *2020 IEEE International Conference on Robotics and Automation (ICRA)*. 2020 IEEE International Conference on Robotics and Automation (ICRA). ISSN: 2577-087X. May 2020, pp. 7358–7364. doi: 10.1109/ICRA40945.2020.9196611.
- [32] Korosh Vatanparvar and Mohammad Abdullah Al Faruque. “Self-Secured Control with Anomaly Detection and Recovery in Automotive Cyber-Physical Systems”. In: *Design, Automation & Test in Europe Conference & Exhibition, DATE 2019, Florence, Italy, March 25-29, 2019*. Ed. by Jürgen Teich and Franco Fummi. IEEE, 2019, pp. 788–793. doi: 10.23919/DATe.2019.8714833.
- [33] Tomas Bures et al. “Performance Modelling of Smart Cyber-Physical Systems”. In: *Companion of the 2018 ACM/SPEC International Conference on Performance Engineering*. ICPE ’18. New York, NY, USA: Association for Computing Machinery, Apr. 2, 2018, pp. 37–40. ISBN: 978-1-4503-5629-9. doi: 10.1145/3185768.3186306. URL: <https://doi.org/10.1145/3185768.3186306> (visited on 03/23/2022).
- [34] Silvia Colabianchi et al. “Discussing resilience in the context of cyber physical systems”. In: *Comput. Ind. Eng.* 160 (2021), p. 107534. doi: 10.1016/j.cie.2021.107534.
- [35] Vyacheslav Kharchenko and Oleg Illiashenko. “Concepts of green IT engineering: taxonomy, principles and implementation”. In: *Green IT Engineering: Concepts, Models, Complex Systems Architectures*. Springer, 2017, pp. 3–19.
- [36] Mila et al. *CodeCarbon.io*. URL: <https://codecarbon.io/> (visited on 07/25/2022).
- [37] Mayra Rodriguez, Guangtao Fu, and David Butler. “Green infrastructures and their impact on resilience: spatial interactions in centralized sewer systems”. In: *ARIC@SIGSPATIAL 2020: Proceedings of the 3rd ACM*

- SIGSPATIAL International Workshop on Advances in Resilient and Intelligent Cities, Seattle, WA, 3 November, 2020.* Ed. by Bandana Kar et al. ACM, 2020, pp. 49–57. DOI: 10.1145/3423455.3430302.
- [38] Hui Yang and Xiaohong Xiao. “How can green strategy contribute to organizational resilience?” In: *The 2021 12th International Conference on E-business, Management and Economics*. ICEME 2021. New York, NY, USA: Association for Computing Machinery, July 17, 2021, pp. 633–637. ISBN: 978-1-4503-9006-4. DOI: 10.1145/3481127.3481218. URL: <https://doi.org/10.1145/3481127.3481218> (visited on 03/23/2022).
- [39] Dana Eleftheriadou, Eddy Hartog, and Natalia Gkiaouri. “The Cities Challenge: Driving a Green and Digital Recovery and Social Resilience”. In: *Computer* 54.5 (2021). Number: 5, pp. 70–75. DOI: 10.1109/MC.2021.3064439.
- [40] Turja Nandy, Ronald A. Couto Jr, and Cristinel Ababei. “Carbon Monoxide Sensing Technologies for Next-Generation Cyber-Physical Systems”. In: *Sensors* 18.10 (2018). Number: 10, p. 3443. DOI: 10.3390/s18103443.
- [41] Yang Liu et al. “Leveraging carbon nanotube technologies in developing Physically Unclonable Function for cyber-physical system authentication”. In: *IEEE Conference on Computer Communications Workshops, INFOCOM Workshops 2016, San Francisco, CA, USA, April 10-14, 2016*. IEEE, 2016, pp. 176–180. DOI: 10.1109/INFCOMW.2016.7562067.
- [42] Ahmed Mohammed, Irina Harris, and Reda Nujoom. “Eco-Gresilient: Coalescing Ingredient of Economic, Green and Resilience in Supply Chain Network Design”. In: *Proceedings of the 7th International Conference on Operations Research and Enterprise Systems, ICORES 2018, Funchal, Madeira - Portugal, January 24-26, 2018*. Ed. by Greg H. Parlier, Federico Liberatore, and Marc Demange. SciTePress, 2018, pp. 201–208. DOI: 10.5220/0006614702010208.
- [43] Pramesh Pandey et al. “GreenTPU: Improving Timing Error Resilience of a Near-Threshold Tensor Processing Unit”. In: *Proceedings of the 56th Annual Design Automation Conference 2019, DAC 2019, Las Vegas, NV, USA, June 02-06, 2019*. ACM, 2019, p. 173. DOI: 10.1145/3316781.3317835.
- [44] Pramesh Pandey et al. “GreenTPU: Predictive Design Paradigm for Improving Timing Error Resilience of a Near-Threshold Tensor Processing Unit”. In: *IEEE Trans. Very Large Scale Integr. Syst.* 28.7 (2020). Number: 7, pp. 1557–1566. DOI: 10.1109/TVLSI.2020.2985057.
- [45] Matteo Poggi, Fabio Tosi, and Stefano Mattoccia. “Quantitative evaluation of confidence measures in a machine learning world”. In: *Proceedings of the IEEE International Conference on Computer Vision*. 2017, pp. 5228–5237.
- [46] John Von Neumann and Oskar Morgenstern. “Theory of games and economic behavior”. In: *Theory of games and economic behavior*. Princeton university press, 2007.
- [47] R. Duncan Luce and Howard Raiffa. *Games and decisions: Introduction and critical survey*. Courier Corporation, 1989.
- [48] C. Jill Stowe and Scott M. Gilpatrick. “Cheating and enforcement in asymmetric rank-order tournaments”. In: *Southern Economic Journal* 77.1 (2010). Publisher: Wiley Online Library, pp. 1–14.