and produces random control input $u_t \in \mathcal{U}$ for each epoch. The safety controller is invoked once $h(x) < 0$. Once the yaw rate exceeds $0.025$ (from the first to seventh epoch in Fig. 2), the safety controller drives the yaw rate to $\mathcal{C}$. Note that the simplex architecture assumes that there exists no adversary, which is different with Scenario I and II.

Therefore, the control policy computed using our proposed algorithm ensures safety of the system with respect to specified budget for any of the CRAs or the simplex architecture.

## VII. CONCLUSION

In this paper, we studied the problem of developing a common framework that allows safety analysis and control synthesis of CPS adopting the simplex architecture or the set of cyber resilient architectures including BFT++. We presented the models for cyber and physical subsystems, and formulated the safety property using a budget constraint. Our formulation captures strict safety constraint as a special case. We constructed a hybrid system that models CPS implementing any of these architectures. We derived a set of sufficient conditions for the control policy to satisfy the budget constraint. We translated the conditions into a set of sum-of-squares constraints, and proposed an algorithm to compute the control policy. We analyzed the convergence and complexity of the algorithm. A case study on the lateral control of a Boeing 747 was presented to demonstrate viability of our proposed framework.

## REFERENCES


[1] A. Greenberg, "Hackers remotely kill a Jeep on the highway–with me in it," 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[2] M. R. Lee, J. M. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," 2016. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

[3] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems," *Annual Reviews in Control*, vol. 32, no. 2, pp. 229–252, 2008.

[4] F. Sharifi, M. Mirzaei, B. W. Gordon, and Y. Zhang, "Fault tolerant control of a quadrotor UAV using sliding mode control," in *Conference on Control and Fault-Tolerant Systems (SysTol)*. IEEE, 2010, pp. 239–244.

[5] D. Xu, F. Zhu, Z. Zhou, and Y. Yao, "Distributed fault detection and estimation in cyber–physical systems subject to actuator faults," *ISA Transactions*, vol. 104, pp. 162–174, 2020.

[6] L. Sha, "Using simplicity to control complexity," *IEEE Software*, vol. 18, no. 4, pp. 20–28, 2001.

[7] S. Bak, D. K. Chivukula, O. Adekunle, M. Sun, M. Caccamo, and L. Sha, "The system-level simplex architecture for improved real-time embedded system safety," in *15th IEEE Real-Time and Embedded Technology and Applications Symposium*. IEEE, 2009, pp. 99–107.

[8] S. Mohan, S. Bak, E. Betti, H. Yun, L. Sha, and M. Caccamo, "S3A: Secure system simplex architecture for enhanced security and robustness of cyber-physical systems," in *the 2nd ACM International Conference on High Confidence Networked Systems*, 2013, pp. 65–74.

[9] J. S. Mertoguno, R. M. Craven, M. S. Mickelson, and D. P. Koller, "A physics-based strategy for cyber resilience of CPS," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, vol. 11009. International Society for Optics and Photonics, 2019, p. 110090E.

[10] M. A. Arroyo, M. T. I. Ziad, H. Kobayashi, J. Yang, and S. Sethumadhavan, "YOLO: frequently resetting cyber-physical systems for security," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, vol. 11009. International Society for Optics and Photonics, 2019, p. 110090P.

[11] M. Arroyo, H. Kobayashi, S. Sethumadhavan, and J. Yang, "Fired: frequent inertial resets with diversification for emerging commodity cyber-physical systems," *arXiv preprint arXiv:1702.06595*, 2017.

[12] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[13] M. Pajic, Z. Jiang, I. Lee, O. Sokolsky, and R. Mangharam, "Safety-critical medical device development using the UPP2SF model translation tool," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 13, no. 4s, pp. 1–26, 2014.

[14] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *18th European Control Conference (ECC)*. IEEE, 2019, pp. 3420–3431.

[15] M. H. Cohen and C. Belta, "Approximate optimal control for safety-critical systems with control barrier functions," in *59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 2062–2067.

[16] Z. Qin, K. Zhang, Y. Chen, J. Chen, and C. Fan, "Learning safe multi-agent control with decentralized neural barrier certificates," *arXiv preprint arXiv:2101.05436*, 2021.

[17] S. L. Herbert, M. Chen, S. Han, S. Bansal, J. F. Fisac, and C. J. Tomlin, "Fastrack: A modular framework for fast and guaranteed safe motion planning," in *56th Annual Conference on Decision and Control (CDC)*. IEEE, 2017, pp. 1517–1522.

[18] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2014, pp. 163–174.

[19] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[20] A. A. Cardenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *Proceedings of the 3rd Conference on Hot Topics in Security*, vol. 5. USENIX Association, 2008, p. 15.

[21] L. Niu, D. Sahabandu, A. Clark, and P. Radha, "Verifying safety for resilient cyber-physical systems via reactive software restart," in *To Appear in ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, 2022.

[22] P. Larsen, A. Homescu, S. Brunthaler, and M. Franz, "SoK: Automated software diversity," in *2014 IEEE Symposium on Security and Privacy*. IEEE, 2014, pp. 276–291.

[23] G. S. Kc, A. D. Keromytis, and V. Prevelakis, "Countering code-injection attacks with instruction-set randomization," in *Proceedings of the 10th ACM conference on Computer and communications security*, 2003, pp. 272–280.

[24] F. Abdi, R. Tabish, M. Rungger, M. Zamani, and M. Caccamo, "Application and system-level software fault tolerance through full system restarts," in *ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2017, pp. 197–206.

[25] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Guaranteed physical security with restart-based design for cyber-physical systems," in *ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2018, pp. 10–21.

[26] R. Romagnoli, P. Griffioen, B. H. Krogh, and B. Sinopoli, "Software rejuvenation under persistent attacks in constrained environments," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 4088–4094, 2020.

[27] T. Arauz, J. Maestre, R. Romagnoli, B. Sinopoli, and E. Camacho, "A linear programming approach to computing safe sets for software rejuvenation," *IEEE Control Systems Letters*, vol. 6, pp. 1214–1219, 2021.

[28] G. F. Franklin, J. D. Powell, A. Emami-Naeini, and J. D. Powell, *Feedback Control of Dynamic Systems*. Prentice hall Upper Saddle River, 2002, vol. 4.