Case Study of Liveness Verification in IronFleet

Lucas Peña and Manasvi Saxena

University of Illinois at Urbana-Champaign,
{lpena7, msaxena2}@illinios.edu

Abstract. Ironclad [1] and IronFleet [2] are...

1 Introduction

1.1 Safety Verification

1.2 Liveness Verification

2 IronFleet

2.1 Dafny

2.2 End-to-end Verification

2.3 Refinement

2.4 Liveness Verification in IronFleet

Limitations

3 Temporal Logic of Actions

3.1 TLA Rules

3.2 Examples

4 Related Work

See [3]

5 Conclusion

References

1. C. Hawblitzel, J. Howell, J. Lorch, A. Narayan, B. Parno, D. Zhang, and B. Zill, "Ironclad apps: End-to-end security via automated full-system verification," in *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, USENIX Advanced Computing Systems Association, October 2014.
2. C. Hawblitzel, J. Howell, M. Kapritsos, J. Lorch, B. Parno, M. L. Roberts, S. Setty, and B. Zill, "Ironfleet: Proving practical distributed systems correct," in *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, ACM Association for Computing Machinery, October 2015.
3. P. K. Nalla, R. K. Gajavelly, H. Mony, J. Baumgartner, and R. Kanzelman, "Effective liveness verification using a transformation-based framework," in *2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems, Mumbai, India, January 5-9, 2014*, pp. 74–79, 2014.