Defining Redundancy in Fault-Tolerant Systems

(Brief Announcement)

Felix Gärtner

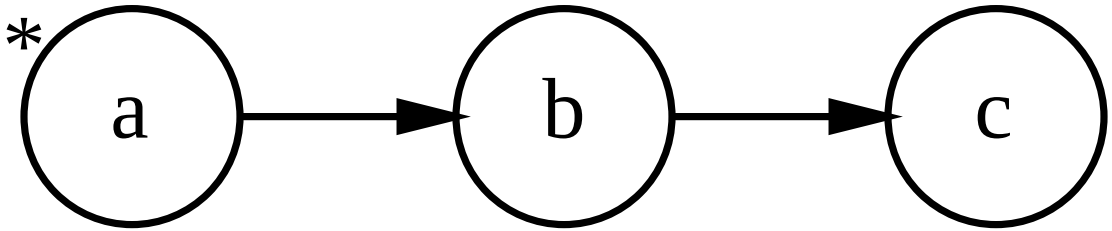
TU Darmstadt, Germany
felix@informatik.tu-darmstadt.de

joint work with Hagen Völzer
HU Berlin, Germany

(now with SVRC, The University of Queensland, Australia)

Systems

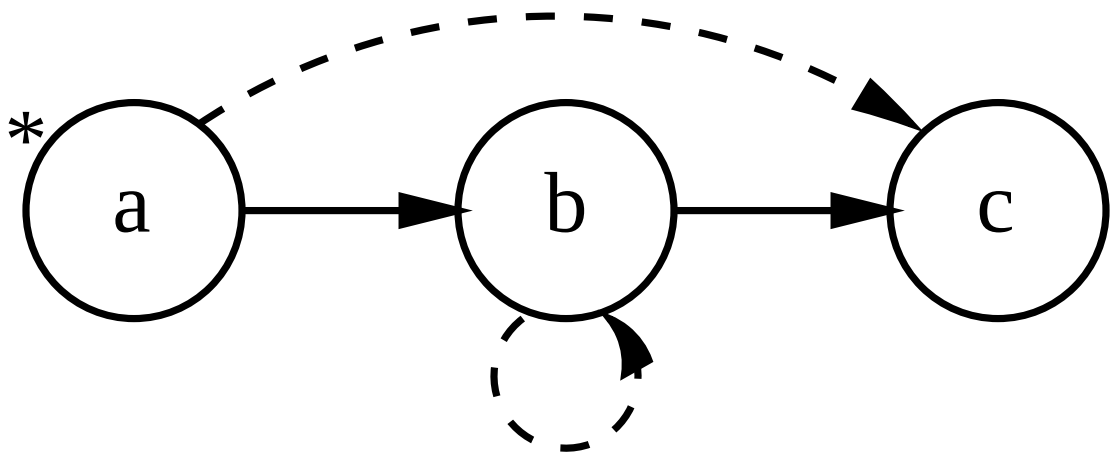
- System $\Sigma = (C, I, T, L)$



- L is a liveness assumption.

Faulty Systems

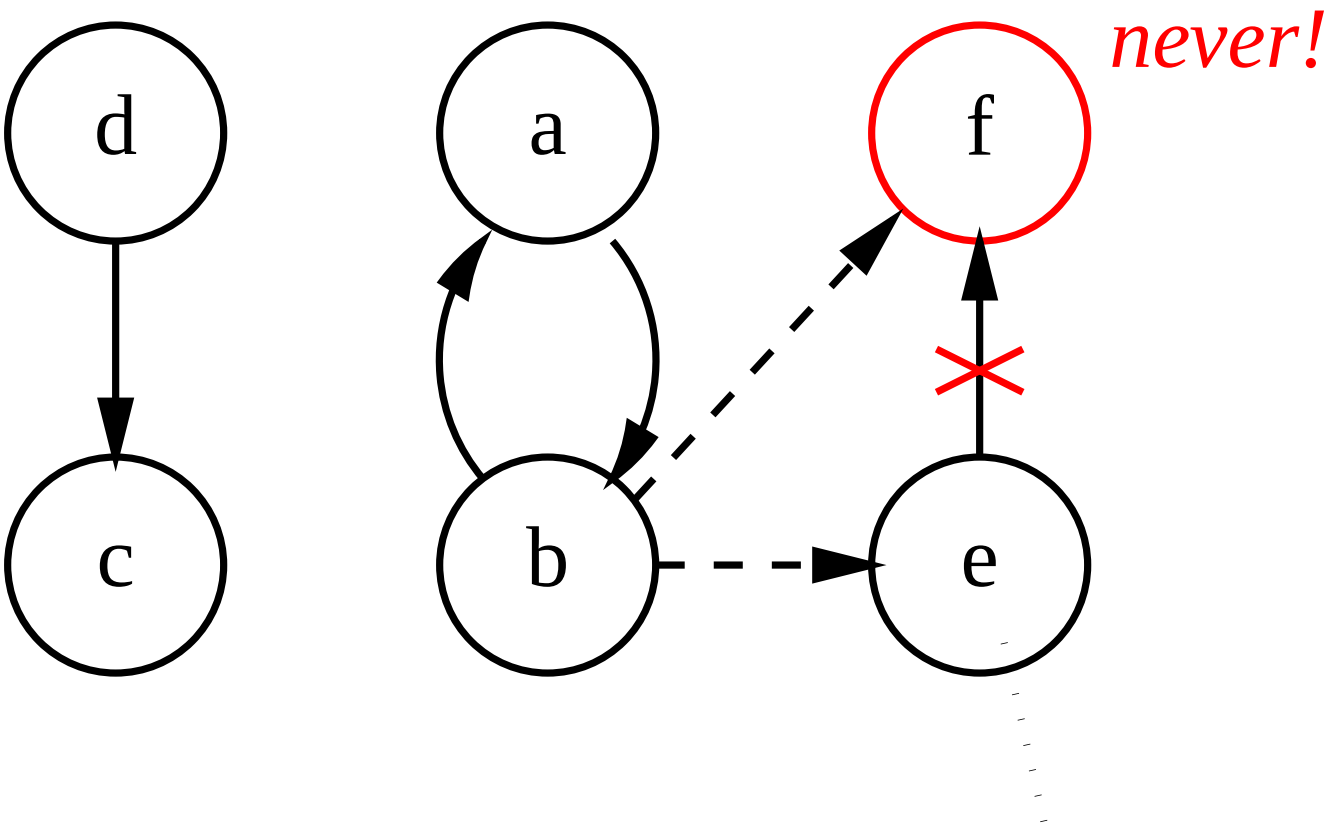
- Faults add transitions or weaken liveness assumption.



Fault-Tolerant Systems

- System Σ satisfies a specification $SPEC$ in fault-free environments.
- Σ violates $SPEC$ in faulty environments.
- What are necessary concepts to build a system Σ' from Σ that satisfies $SPEC$ in faulty environments?

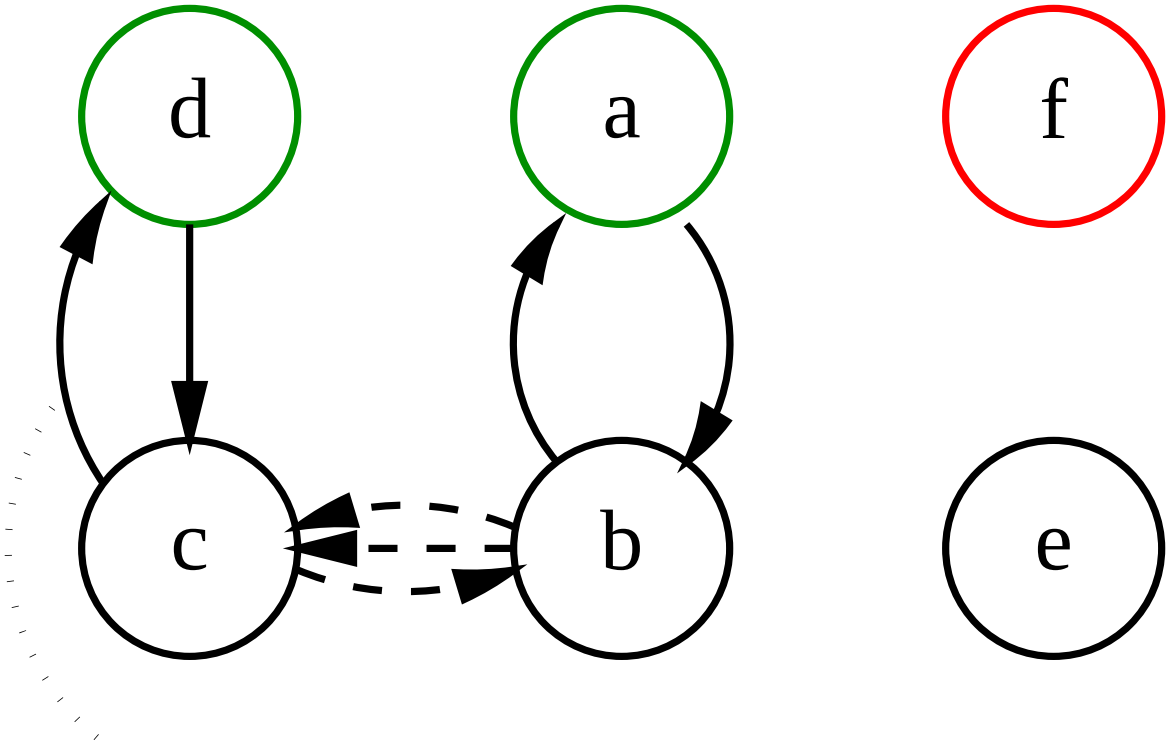
Satisfying Safety



redundancy in space

Satisfying Liveness

infinitely often!



redundancy in time

Summary of Results

fault-tolerant w.r.t.	necessary
safety	redundancy in space
liveness	redundancy in time + redundancy in space

- One possible definition of redundancy.
- Helps explain fault-tolerance theory of Arora and Kulkarni [AK98] and "fault-tolerance compiler" of Kulkarni and Arora [KA00].

Acknowledgements

• Slides produced using pdfLaTeX and Klaus Guntermann's PPower4.

References

[AK98] Anish Arora and Sandeep S. Kulkarni. Component based design of multitolerant systems. *IEEE Transactions on Software Engineering*, 24(1):63–78, January 1998.

[KA00] Sandeep S. Kulkarni and Anish Arora. Automating the addition of fault-tolerance. In Mathai Joseph, editor, *Formal Techniques in Real-Time and Fault-Tolerant Systems, 6th International Symposium (FTRTFT 2000) Proceedings*, number 1926 in Lecture Notes in Computer Science, pages 82–93, Pune, India, September 2000. Springer-Verlag.