Similarities between Timing Constraints

Towards Interchangeable Constraint Models for Real-World Software Systems

Yue Yu

yyu8@iit.edu

Illinois Institute of Technology

Background

Software for real-world systems

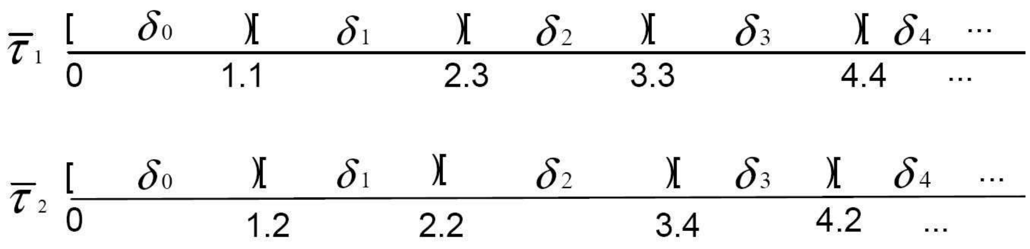
- **System Complexity:** guarantees of exact system behavior are impractically expensive [Lee, 2005].
- **Operating Environment:** The unpredictable nature of the environments in which software systems operate determines that their interactions with the outer world may not be totally expected [Jackson et al., 2007].
- **Computational Intractability:** From a theoretical point of view, achieving exactness in the verification of system properties is sometimes intractable [Alur and Dill, 1994].

$$\Box\,(p \longrightarrow \Diamond_{=5} q)$$

Related Works [Huang et al., 2003, Huang et al., 2004]

Similarities between timed state sequences

- A *timed state sequence* is a linear structure $(\delta_0, I_0), (\delta_1, I_1), (\delta_2, I_2), \ldots$ where $\delta_i \subseteq Prop$



- Absolute displacement between two interval sequences $\bar{I}$ and $\bar{I}'$

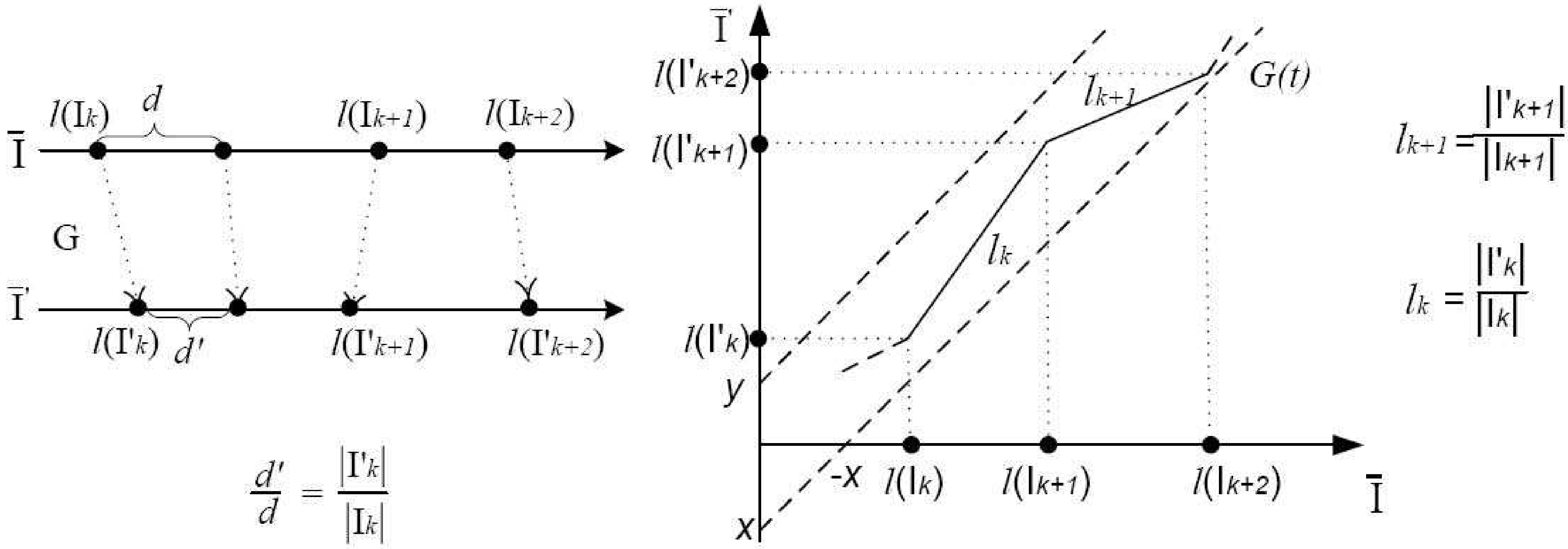
$$D_a^{\mathcal{I}}\left(\bar{I}, \bar{I}'\right) = \left[d_{a_{\inf}}^{\mathcal{I}}\left(\bar{I}, \bar{I}'\right), d_{a_{\sup}}^{\mathcal{I}}\left(\bar{I}, \bar{I}'\right)\right]$$

where

$$d_{a_{\sup}}^{\mathcal{I}}\left(\bar{I}, \bar{I}'\right) = \sup\left\{l(I_i') - l(I_i) | i < n\left(\bar{I}\right)\right\}$$
$$d_{a_{\inf}}^{\mathcal{I}}\left(\bar{I}, \bar{I}'\right) = \inf\left\{l(I_i') - l(I_i) | i < n\left(\bar{I}\right)\right\}$$

Related Works [Huang et al., 2003, Huang et al., 2004]

- Absolute $[x, y]$-tube function



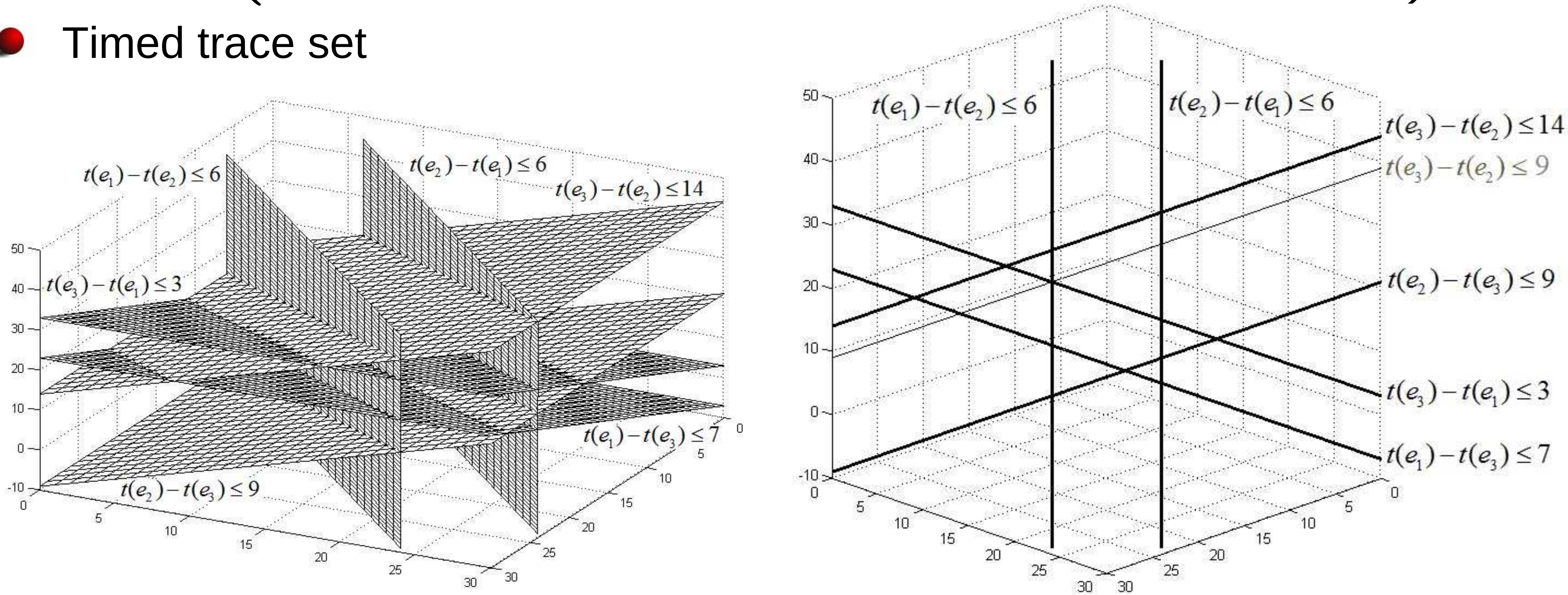
Let $\bar{I}$ and $\bar{I}'$ be two interval sequences. There exists an absolute $[x, y]$-tube function from $\bar{I}$ to $\bar{I}'$ iff $D_a^{\mathcal{I}}\left(\bar{I}, \bar{I}'\right) \subseteq [x, y]$

Timing Constraints

- Linear timing constraints

$$\left\{ \begin{array}{lll} t(e_1) - t(e_2) \leq 6, & t(e_2) - t(e_1) \leq 6, & t(e_1) - t(e_3) \leq 7, \\ t(e_3) - t(e_1) \leq 3, & t(e_2) - t(e_3) \leq 9, & t(e_3) - t(e_2) \leq 14 \end{array} \right\}$$

- Timed trace set

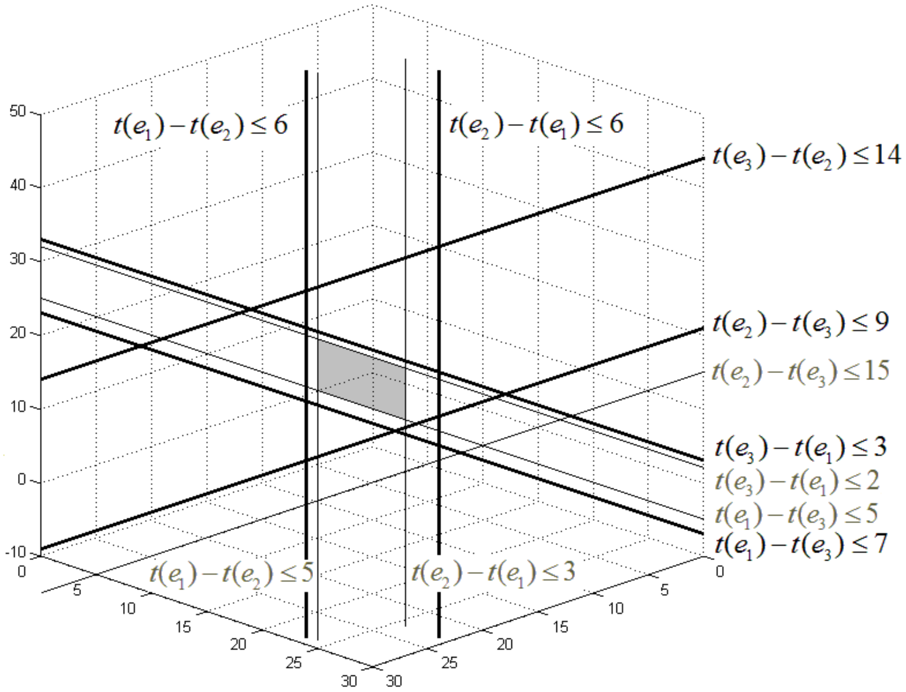


(a) (b)

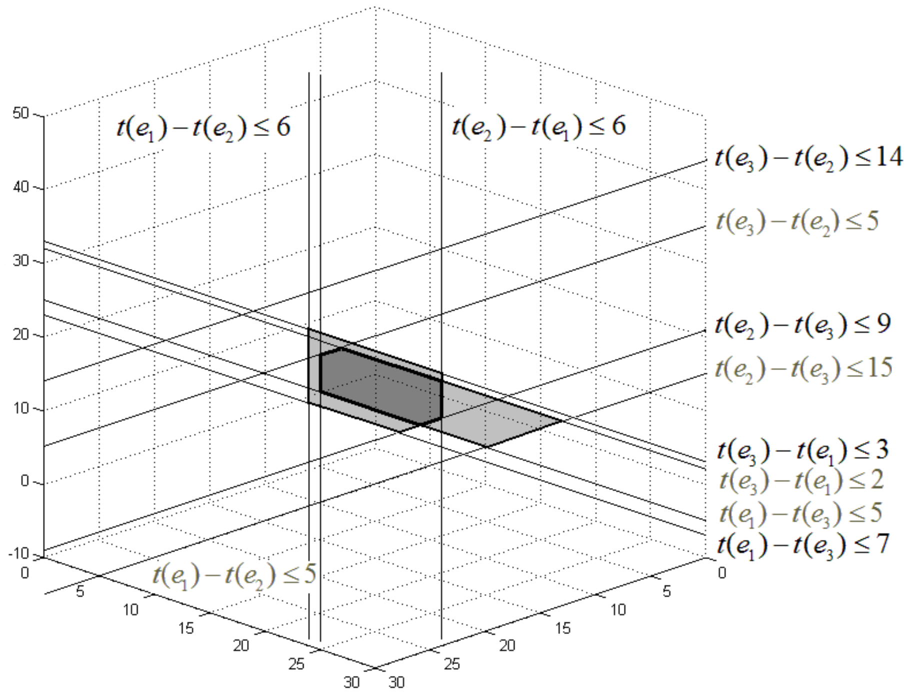
Difference relations between every *pairs* of events determine the shape of the trace polyhedron.

Timed Trace Inclusions and Intersections

- Timed Trace Inclusions and Intersections



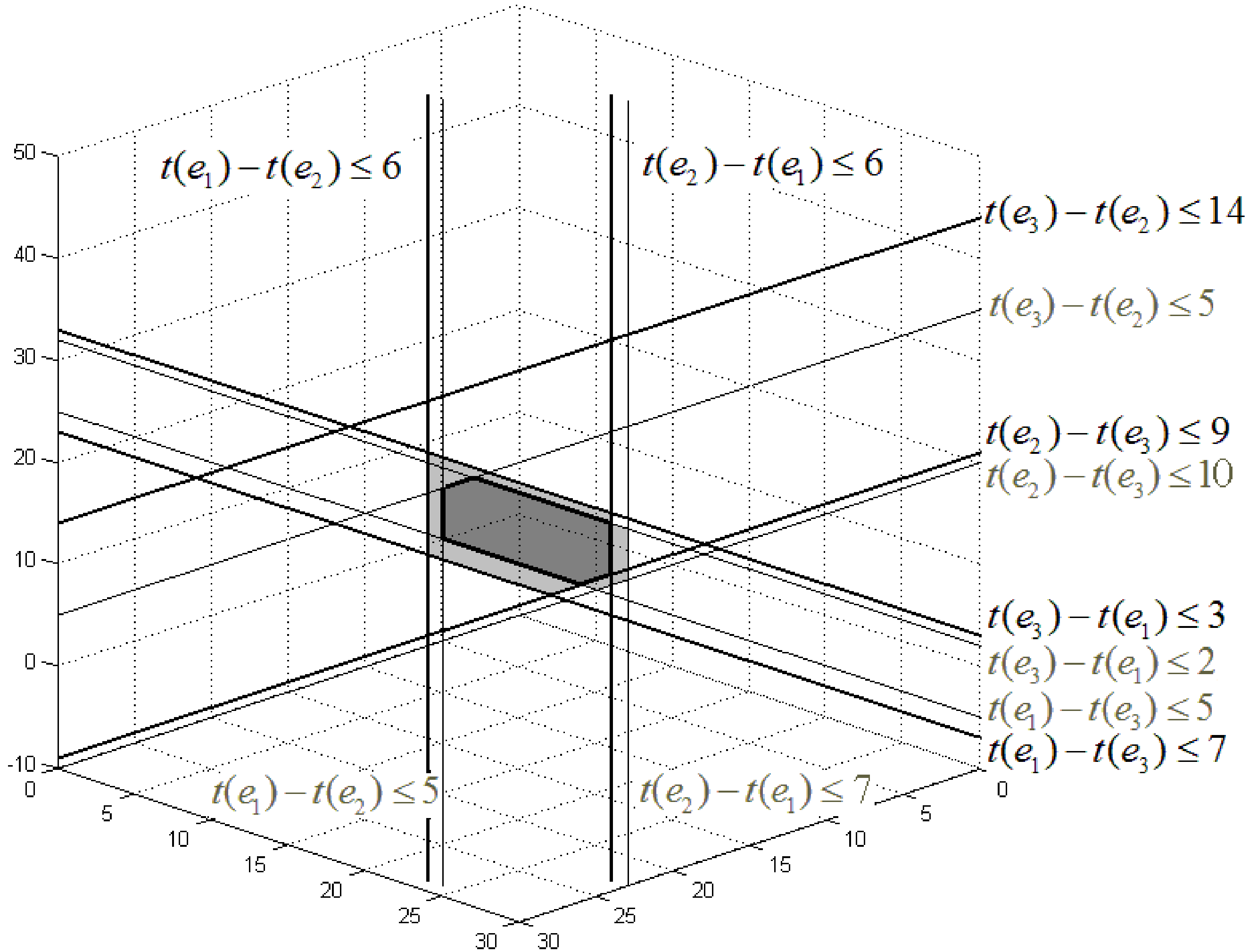
(c) Inclusion



(d) Intersection

Timed Trace Similarities

- Similarities between timed trace sets



Proposed Metrics: Absolute Differences

- Absolute differences

$$D_a(C, C') = \left[d_{a_{\inf}}(C, C'), d_{a_{\sup}}(C, C')\right]$$

where

$$d_{a_{\sup}}(C, C') = \sup\left\{ d^*_{i,j} - d'^*_{i,j} \middle| i = 1, \ldots, n, j = 1, \ldots, n, i \neq j \right\}$$

$$d_{a_{\inf}}(C, C') = \inf\left\{ d^*_{i,j} - d'^*_{i,j} \middle| i = 1, \ldots, n, j = 1, \ldots, n, i \neq j \right\}$$

For example, in the previous slide, the absolute difference between the two timed trace sets is derived as

$d_{a_{\sup}}(C, C') = \sup\{6-5, 6-7, 7-5, 3-2, 9-10, 9$[a]$-5\} = 4,$

$d_{a_{\inf}}(C, C') = \inf\{6-5, 6-7, 7-5, 3-2, 9-10, 9-5\} = -1,$ and

$D_a(C, C') = [-1, 4].$

[a] note that $d^*_{3,2} = 9$ instead of 14

Proposed Metrics: Absolute Differences

Proposition:(This directly follows from the inclusion theorem)

- Systems satisfying timing constraint set C will satisfy timing constraint set C' when every constraint in C' is incremented by $d_{a_{\sup}}(C,C')$, i.e., for all $i \neq j$: $d'^{*}_{i,j} + d_{a_{\sup}}(C,C')$; and symmetrically,
- systems satisfying timing constraint set C' will satisfy timing constraint set C when every constraint in C is incremented by $d_{a_{\sup}}(C',C)$, i.e., for all $i \neq j$: $d^{*}_{i,j} + d_{a_{\sup}}(C',C) = d^{*}_{i,j} + d_{a_{\inf}}(C,C')$.

Transitive relations can be bounded by:

$$D_a(C,C'') \subseteq \left[d_{a_{\inf}}(C,C') + d_{a_{\inf}}(C',C''), d_{a_{\sup}}(C,C') + d_{a_{\sup}}(C',C'')\right]$$

Proposed Metrics: Relative Differences

- Relative differences

$$D_r(C, C') = \left[d_{r_{\inf}}(C, C'), d_{r_{\sup}}(C, C')\right]$$

where

$$d_{r_{\sup}}(C, C') = \sup\left\{ \frac{d^*_{i,j}}{d'^*_{i,j}} \middle| i = 1, \ldots, n, j = 1, \ldots, n, i \neq j \right\}$$

$$d_{r_{\inf}}(C, C') = \inf\left\{ \frac{d^*_{i,j}}{d'^*_{i,j}} \middle| i = 1, \ldots, n, j = 1, \ldots, n, i \neq j \right\}$$

For example, the relative difference between the two timed trace sets is

$$d_{r_{\sup}}(C, C') = \sup\{6/5, 6/7, 7/5, 3/2, 9/10, 9/5\} = 9/5,$$

$$d_{r_{\inf}}(C, C') = \inf\{6/5, 6/7, 7/5, 3/2, 9/10, 9/5\} = 6/7, \text{ and}$$

$$D_r(C, C') = [6/7, 9/5].$$

Conjecture: The proportion of the "volume" of the intersection in that of C is lower bounded by $\frac{1}{d_{r_{\sup}}(C,C')}$; and symmetrically, the proportion of the "volume" of the intersection in that of C' is lower bounded by $\frac{1}{d_{r_{\sup}}(C',C)} = d_{r_{\inf}}(C, C')$.

References

[Alur and Dill, 1994] Alur, R. and Dill, D. L. (1994). A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235.

[Huang et al., 2003] Huang, J., Voeten, J., and Geilen, M. (2003). Real-time property preservation in approximations of timed systems. In *MEMOCODE '03: Proceedings of the First ACM and IEEE International Conference on Formal Methods and Models for Co-Design (MEMOCODE'03)*, page 163, Washington, DC, USA. IEEE Computer Society.

[Huang et al., 2004] Huang, J., Voeten, J., and Geilen, M. (2004). Real-time property preservation in concurrent real-time systems. In *Proceedings of the 10th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*.

[Jackson et al., 2007] Jackson, D., Thomas, M., and Millett, L. I. (2007). *Software for Dependable Systems: Sufficient Evidence?* The National Academies Press, Washington, D.C.

[Lee, 2005] Lee, E. A. (2005). Building unreliable systems out of reliable components: The real time story. Technical Report UCB/EECS-2005-5, EECS Department, University of California, Berkeley.