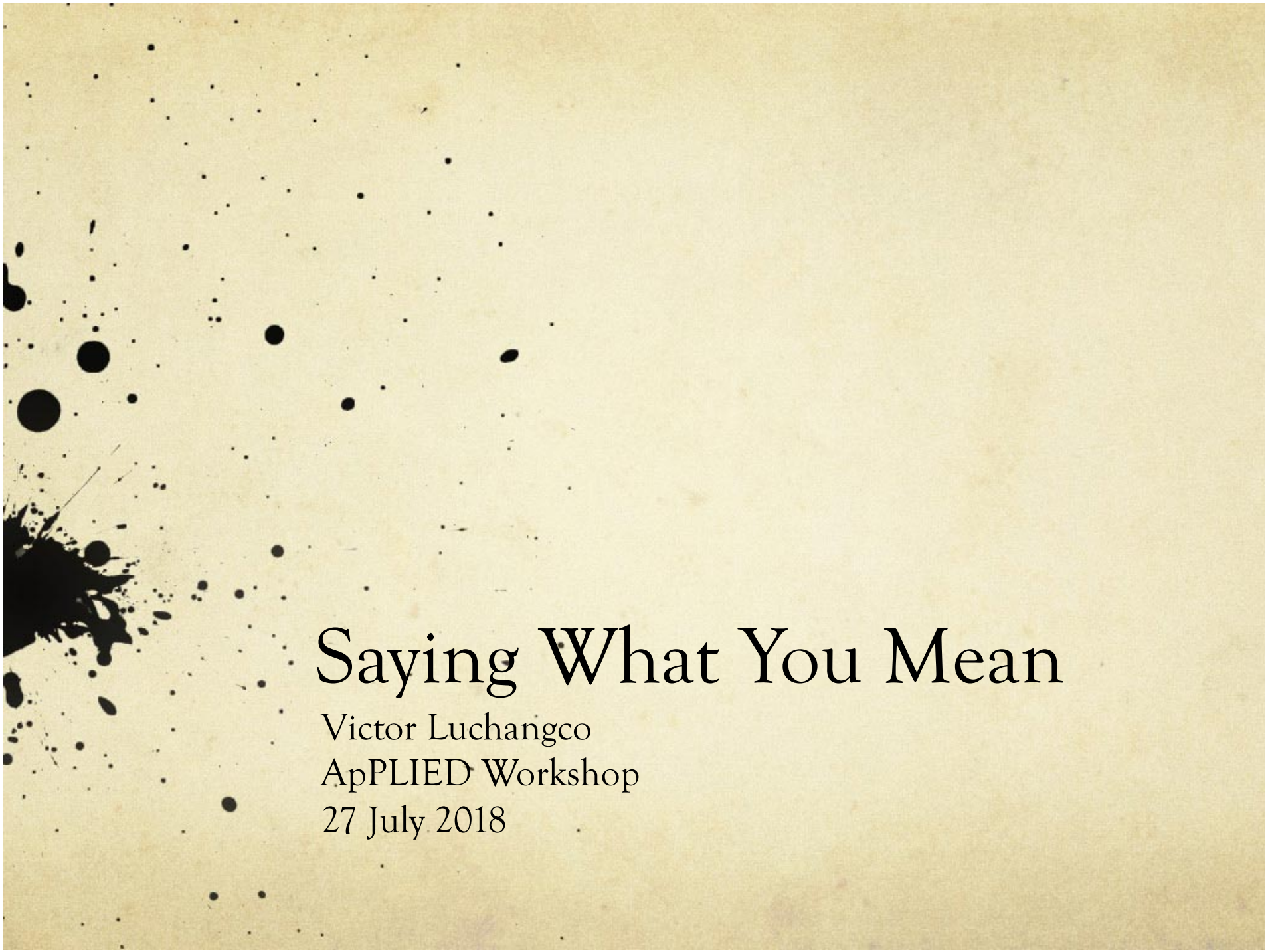

Saying What You Mean

Victor Luchangco

ApPLIED Workshop

27 July 2018

- Overspecification
- Underspecification
- Imprecision
- Missing details
- Too much detail
- Obscure/difficult to understand

Read-write lock

counter

waiting writer?

Read-write lock

waiting writer?

~~counter~~

nonzero indicator

Read-write lock

- Overspecification: only need nonzero indicator
- Specification includes performance characteristics
- What is scalability?

Specification ≠ Documentation

Desiderata

- Unambiguous
- Precise
- Comprehensible
- Illuminating
- Usable/Tractable
- Decomposed and Hierarchical
- Complete

Aids in specification

- Examples: tests, anomalies
- Dialogue (listening and explaining and asking)
- Writing
- Iteration
- Assertions
- Proofs
- Automated tools

Formal specifications

- Formal vs. informal
- State machine formalisms and refinement
- Specification languages
- Programming language inference rules
- Machine-readable languages
- Automated tools

Transactional memory specs

- Lock-based semantics
- Serializability
- Opacity
- TMS1
- TMS2
- Virtual World Consistency
- C++

Specifying languages

Summary

- Specification: stating essential properties of a problem
- Hierarchical state-machine models
- Performance specifications
- No unique “right” specification