Problem Structure

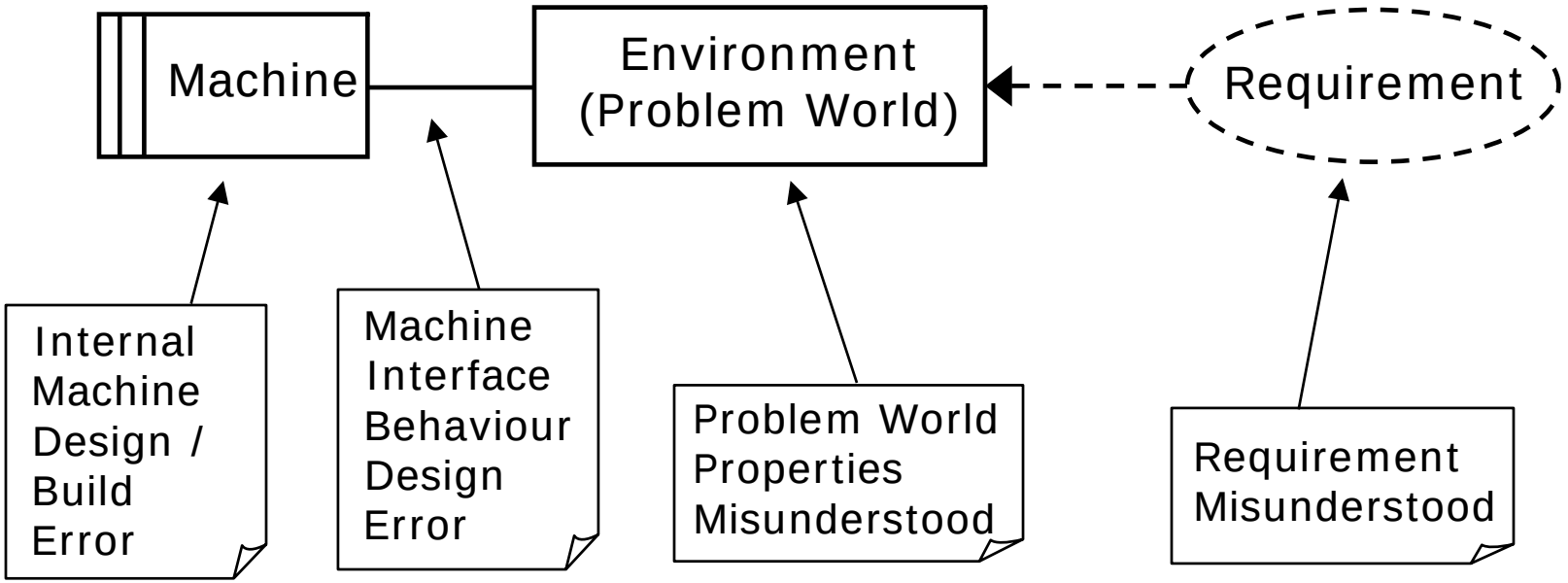
and

Dependable Architecture

Michael Jackson
jacksonma@acm.org

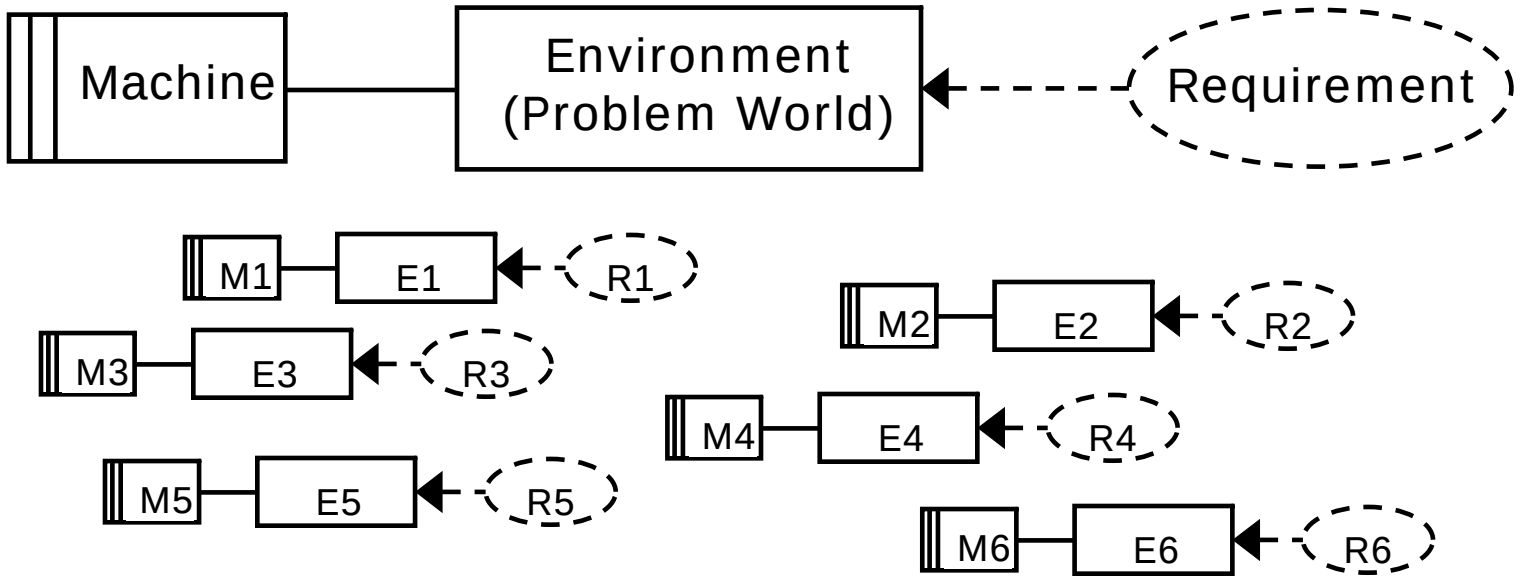
WADS2004
ICSE 2004 Edinburgh
25 May 2004

Dependability Exposure In a Problem



- Satisfying a requirement that is not what was desired
- Relying on properties the problem world doesn't have
- Error in specifying machine behaviour at interface
- Error in internal design or construction of machine

Decompose Requirement and Machine



- Decomposition is not in general hierarchical
  - Subproblems are projections
- Machine is a composition of M1, M2, ...
  - Architecture is composition of machines M1, M2, ...

Some Decomposition Concerns

- Subproblems must be of known classes
  - Decomposition must be from unknown to known
- Complexity must be addressed directly
  - Restriction to known subproblem classes
    - Familiar complexity is not complexity
  - Separating subproblem from composition concerns
    - Much complexity is subproblem interaction
- Composition concerns must be deferred
  - Architecture should be arrangement of known parts
    - Not top-down!

Some Composition & Architecture Concerns

- What is a dependable system?
  - The most important functions are most dependable
- Order machines' requirements by importance
  - Emergency shut-off > logging commands
- Graceful degradation of domain properties
  1. Lift mechanism working as desired
  2. Failure of a floor sensor
  3. Motor failure
  4. Hoist cable breakage
- Implementable architecture
  - eg Prefer pipe-and-filter to blackboard
- Heterogeneous architecture
  - Subproblems and their interactions are heterogeneous