Reducing Autonomy Risks through Rational Selection of Verification Strategies

Julian Richardson, RIACS/NASA Ames Research Center

Barry Boehm, Ray Madachy, LiGuo Huang, University of Southern California

Dan Port, Rick Kazman, University of Hawaii

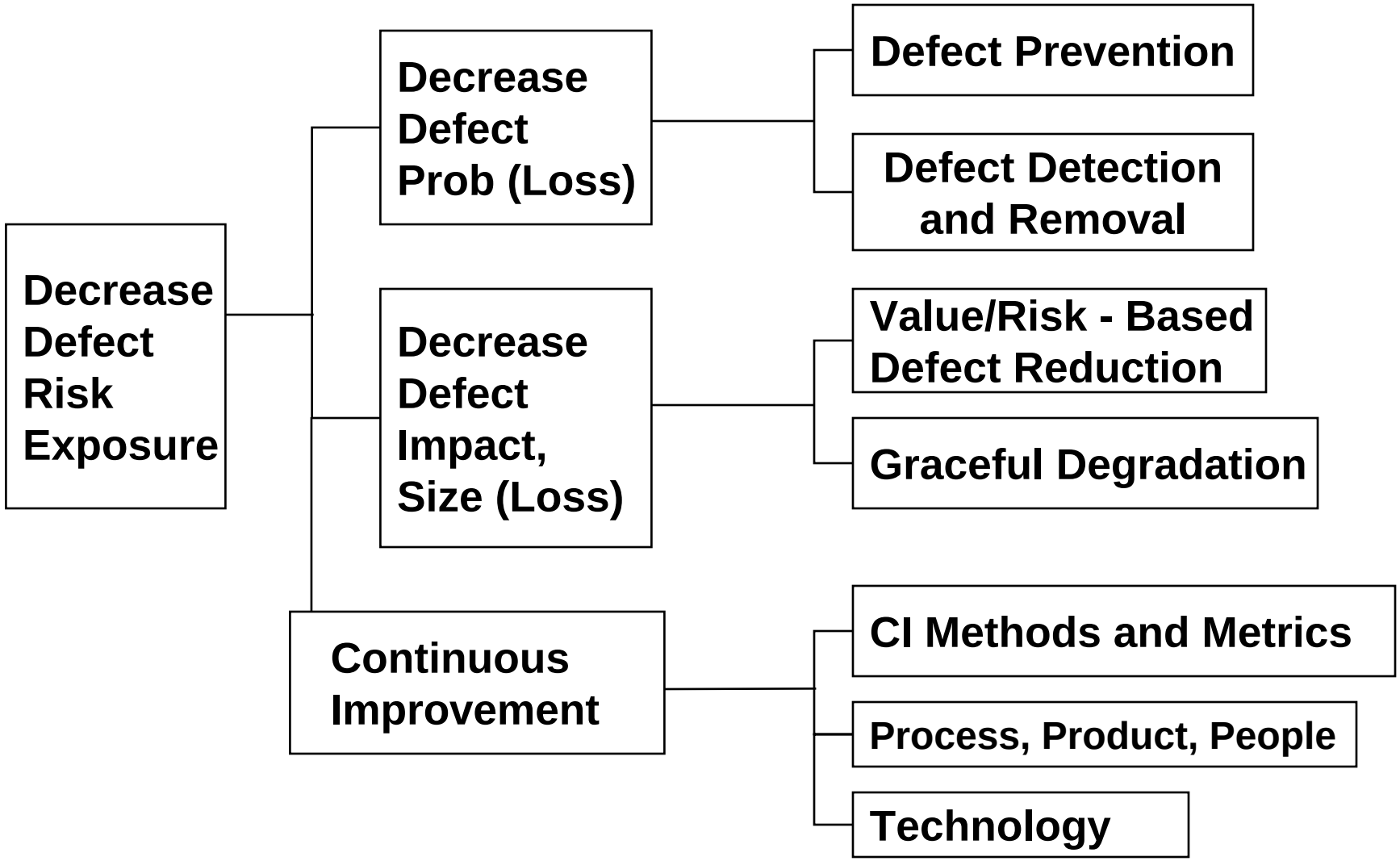
GSAW 2006

March 29, 2006

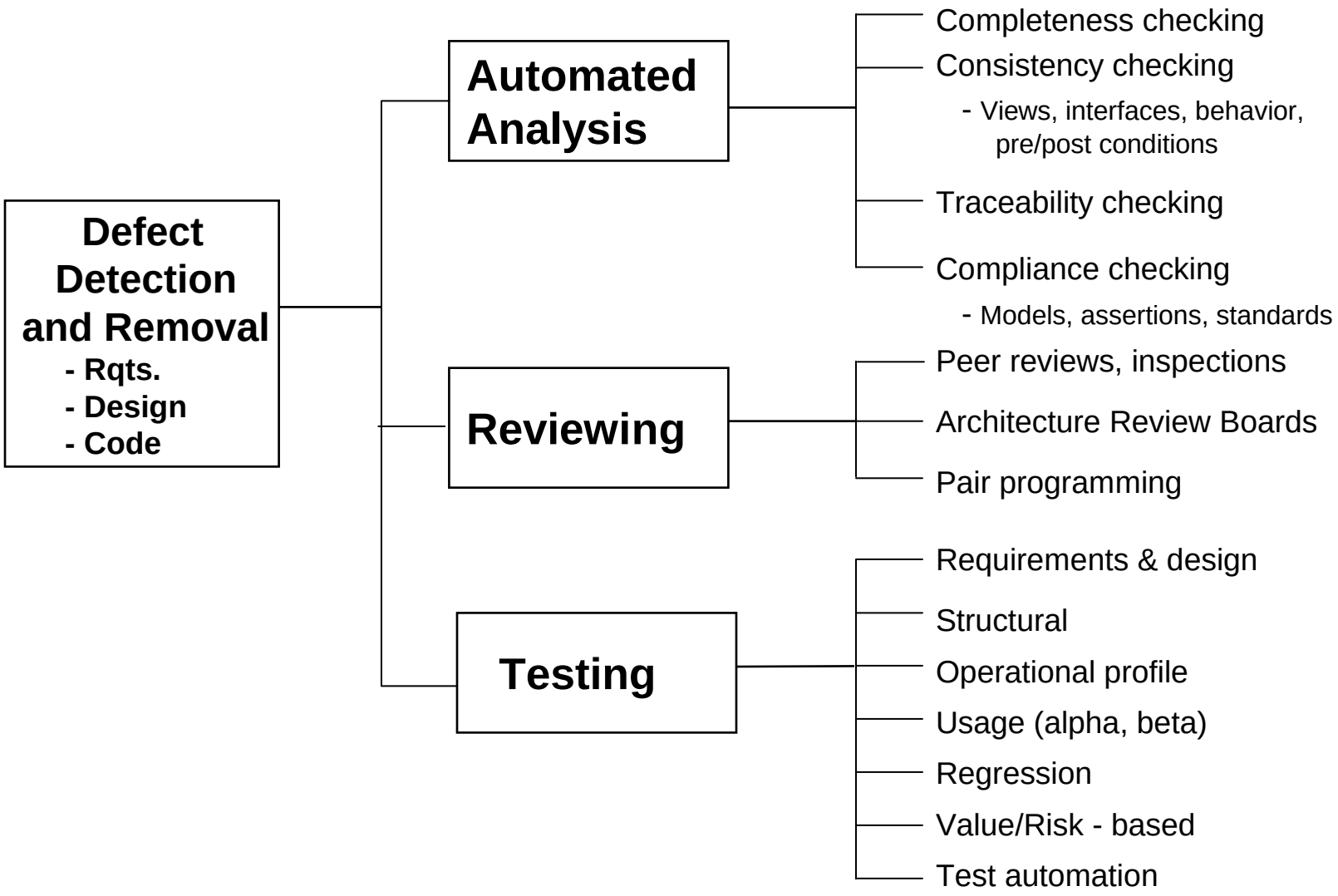
Understanding Autonomy Risks

- **Autonomy high payoff technology for NASA:**
  - **e.g.: automated rendezvous and docking, ISHM; deep space**
- **But there are barriers to use:**
  - **little heritage, hard to ensure correctness, new failure modes**
- ***Aim to assist identification and quantification of risks for (autonomy) software***
- **Key risk quantities:**
  - **Risk Exposure RE = Prob(Loss) * Size(Loss)**
  - **Risk Leverage RL = (RE(before) – RE(after)) / mitigation cost**

Software Dependability Opportunity Tree

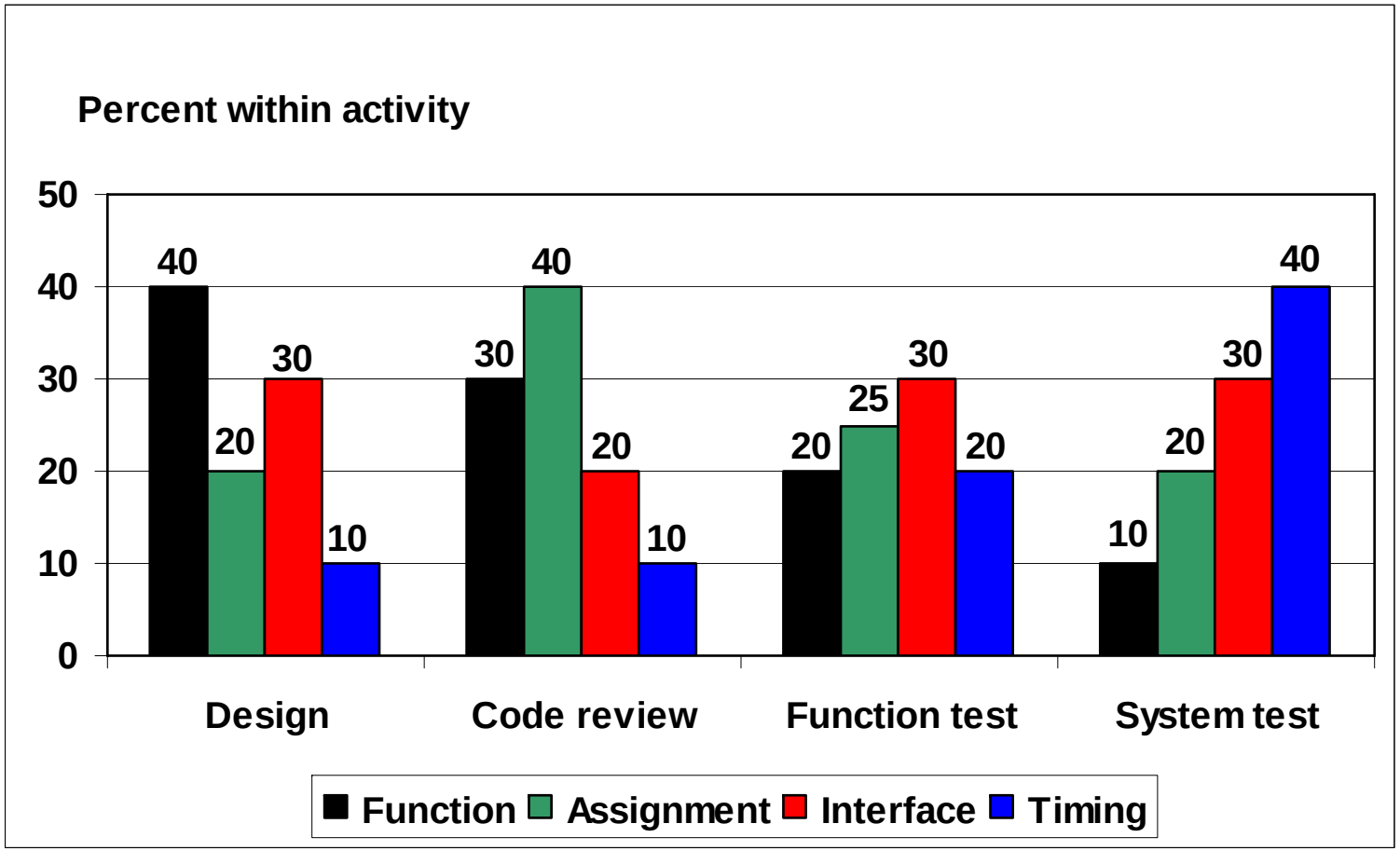


Software Defect Detection Opportunity Tree

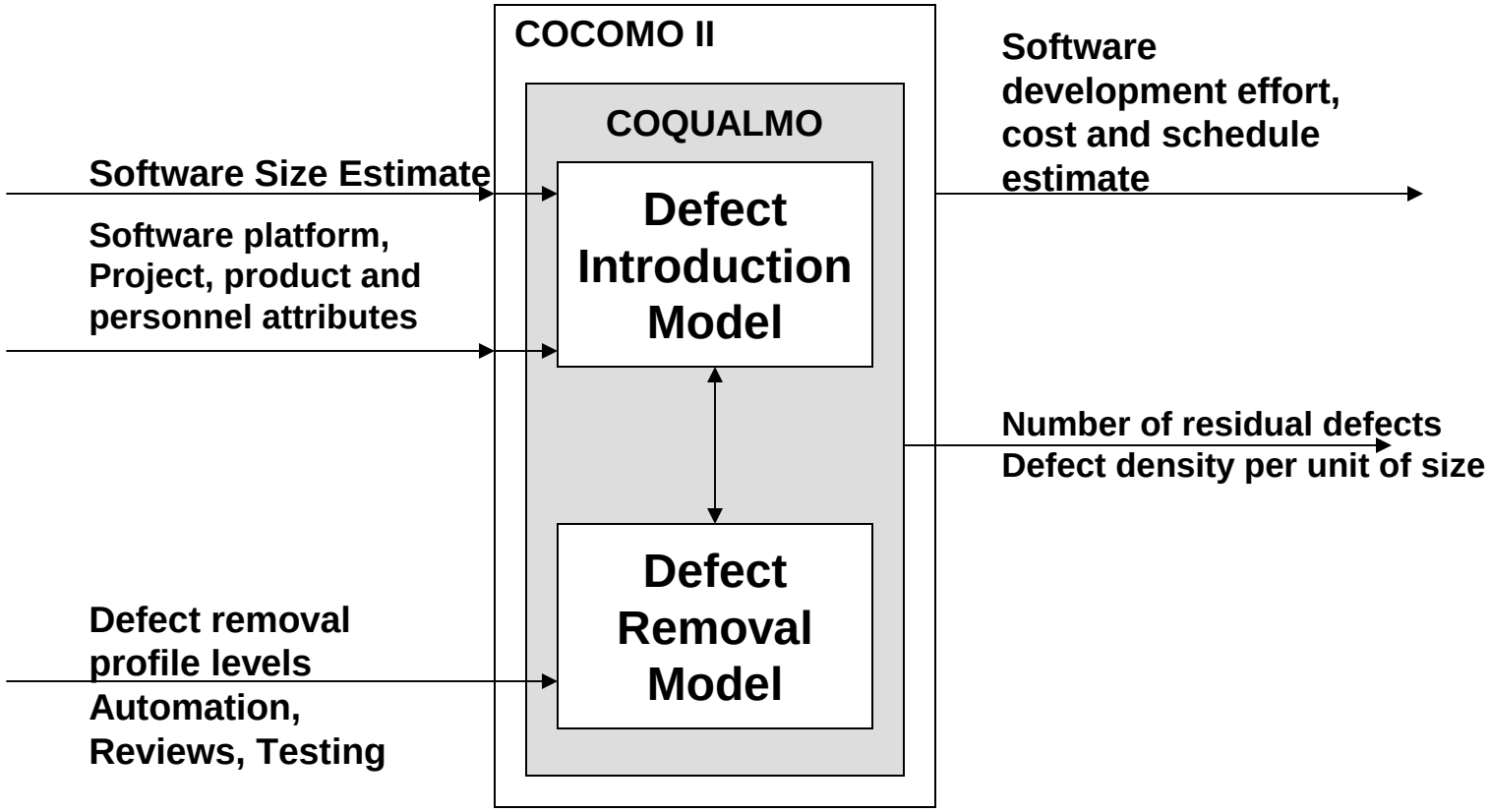


Orthogonal Defect Classification

- Chillarege, 1996



Current COQUALMO System



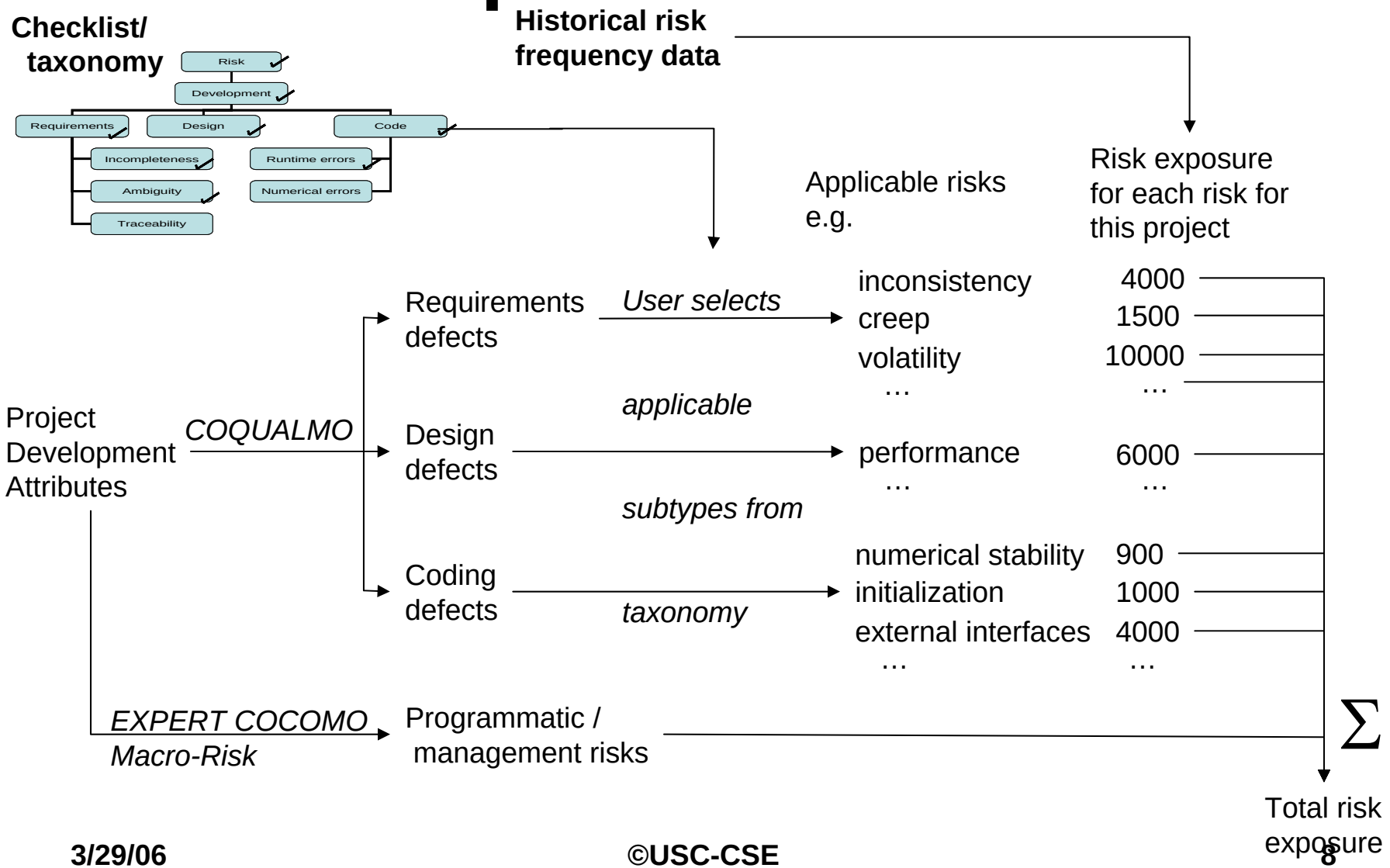
Tool/Technique mitigation for each defect

Two columns:
Left: Our expectation
Right: Experimental results
1 (good), 2 (OK),
3 (can detect), X (cannot detect),
? (don't know)

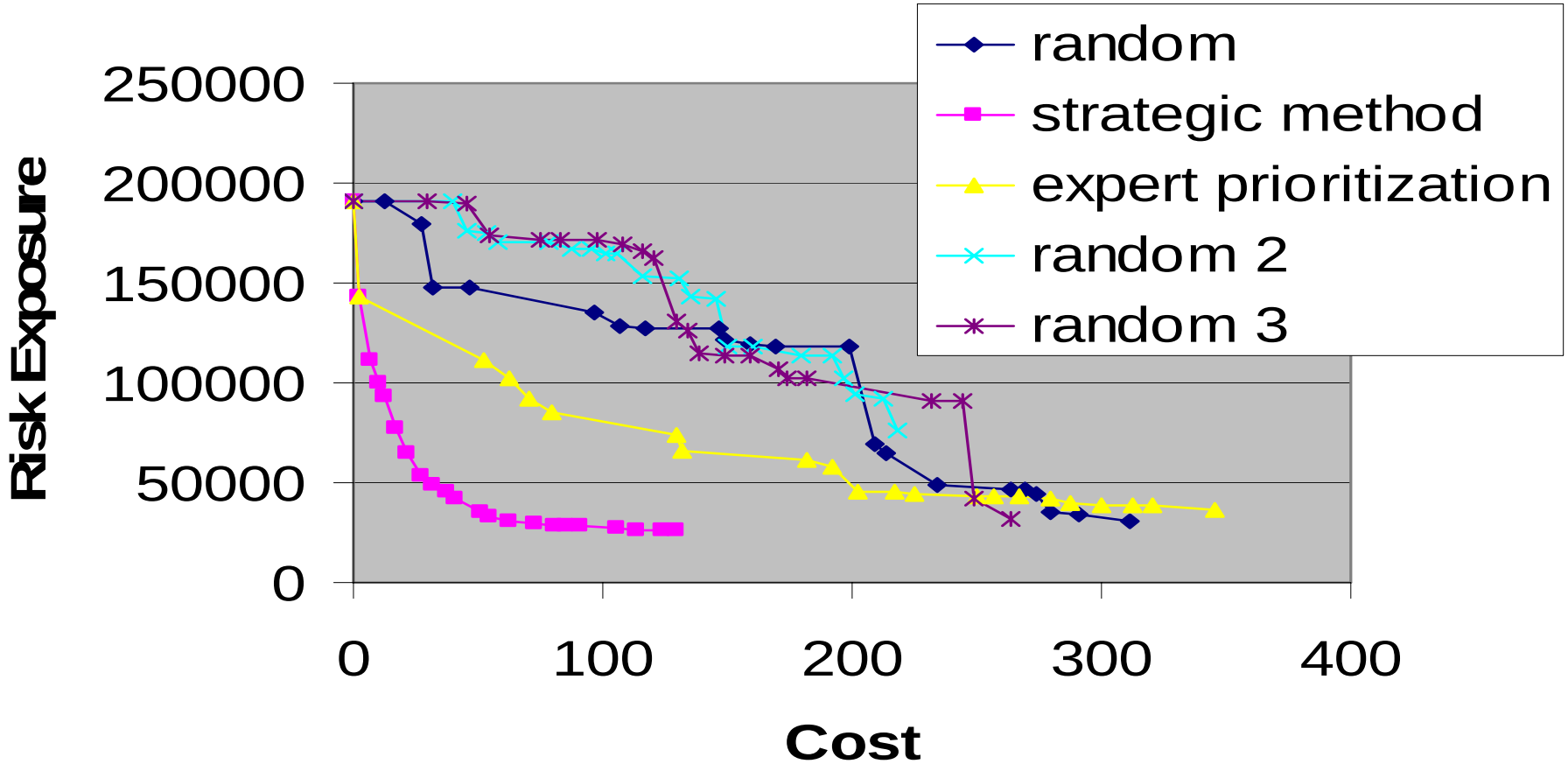
Defects versus V&V Tools

	Coverity		Polyspace		Model Checking		Runtime Analysis	
Divide by 0	1	X	1	3	1	?	3	2
Uninitialized Variable	1	1	1	2	1	?	3	3
Deadlock Race	X	X	3	?	1	1	3	2
Array bounds	1	2	1	2	2	?	3	2
Math functions	X	X	X	X	3	?	2	2
Resource contention	1	2	1	2	2	?	2	1
Error Handling	X	X	X	X	2	?	3	3
Return codes	1	?	1	?	2	?	2	2

Risk Exposure Calculation



RL-Prioritized Risk Mitigation



Macro-Risk Sources

- **Plans, Schedules, Budgets**
  - **Late, inadequate V&V, testbeds; lack of slack**
- **Contracts, Reviews**
  - **Overfocus on functions, hardware, nominal case**
  - **Lowest-cost labor, no retention incentives**
- **Systems of Systems, COTS**
  - **Inconsistent assumptions, interfaces, protocols; dynamism**
- **Change/Risk Management**
  - **Requirements creep, bureaucracy, SoS scalability**
- **KPP Trades**
  - **Safety/security/availability/performance/evolvability/scalability**