Moving forward
with DIS and the Building Code

Kathleen Fisher, DARPA

Ray Richards, Rockwell Collins

John Hatcliff, Kansas State University

John Launchbury, Galois, Inc.

Bill Scherlis, CMU (moderator)

[Byron Cook, Microsoft Research]

4-I + 4-A + 3-G

Moving forward with DIS and the Building Code

- Questions
  - What are early indicators and incremental steps that might signal the best courses of action to pursue the vision?
  - What are technical opportunities and barriers to advancing the vision, and what research should be advanced?
  - What are possible business and policy enablers or impediments?
    - Affordability, ROI, measurement, economic modeling
    - Compliance and safe harbors → direct product assay
    - IP protection and exposure
    - Government drivers

Building codes, idealized

Five salient features

(1) Engineering constraints
(2) Predicted quality outcomes
(3) Visible evidence of quality
(4) Explicit support for response
(5) Continuous evolution

They exist.

They work.

Consensus and compromise

(1) Enable innovation
(2) Protect IP
(3) Limit impacts on cost, performance, schedule, quality
(4) Fairly allocate risk and responsibility
(5) Afford measurement and visibility of risk and cost

Accommodations and Possibilities

(1) Fast pace of technology and ecosystem advancement

- More goals (what); less mechanism (how)
- Require a positive case with concrete evidence

(2) Scale, interconnection, customization unlike physical systems

- Composition is key

(3) Diversity and inter-relatedness of quality attributes

- Build models, analyses, metrics, composition for each
- Combine quality and security attributes – breakage and threats

(4) Hardware special needs and opportunities

- Rethink trusted hardware

(5) Economics and measurement as fundamental drivers

- Address incentives in building code – from EVM to IDE
- Fairly allocate risk mitigation benefit