

CPS: Verification and Certification

John Rushby

Computer Science Laboratory
SRI International
Menlo Park CA USA

Not Certification as Usual

- CPS will be pervasive, high impact on society
- Requires assurance to stakeholders that systems do what they want, not what they fear
- Traditional certification standards are a brake on innovation
- We want certification as an **enabler**
- **Assurance case**: explicit claims, evidence, argument
 - Multiple forms of evidence and their combination
- Compositional certification
 - Difficult because assurance case may not decompose on architectural lines
 - So what is an architecture?

But That's All Still Standard Embedded Systems

- We need to consider poorly modeled systems (e.g., a specific human body), human interaction, societal interaction, unplanned events, massive failures, AI and adaptive control, and opportunistic systems
- **Radical idea**: move certification to **runtime**
- Or more plausibly, assurance has to be integrated with development and execution
 - Runtime Monitors
 - **Synthesis** rather than verification

Verification Research Topics

- Formal verification and synthesis
- Currently, hybrid systems seem most relevant
 - But need to do better than reachability analysis
 - Newer methods often depend on powerful deductive tools like SMT solvers
 - But these don't do nonlinear arithmetic, nor functions like sin, cos etc.
- But what about socio-technic systems?
- Very large scale systems
- Overall, broad foundation, more automation, more synthesis
- But in a CPS context
 - Center of the flower, not an isolated orchid