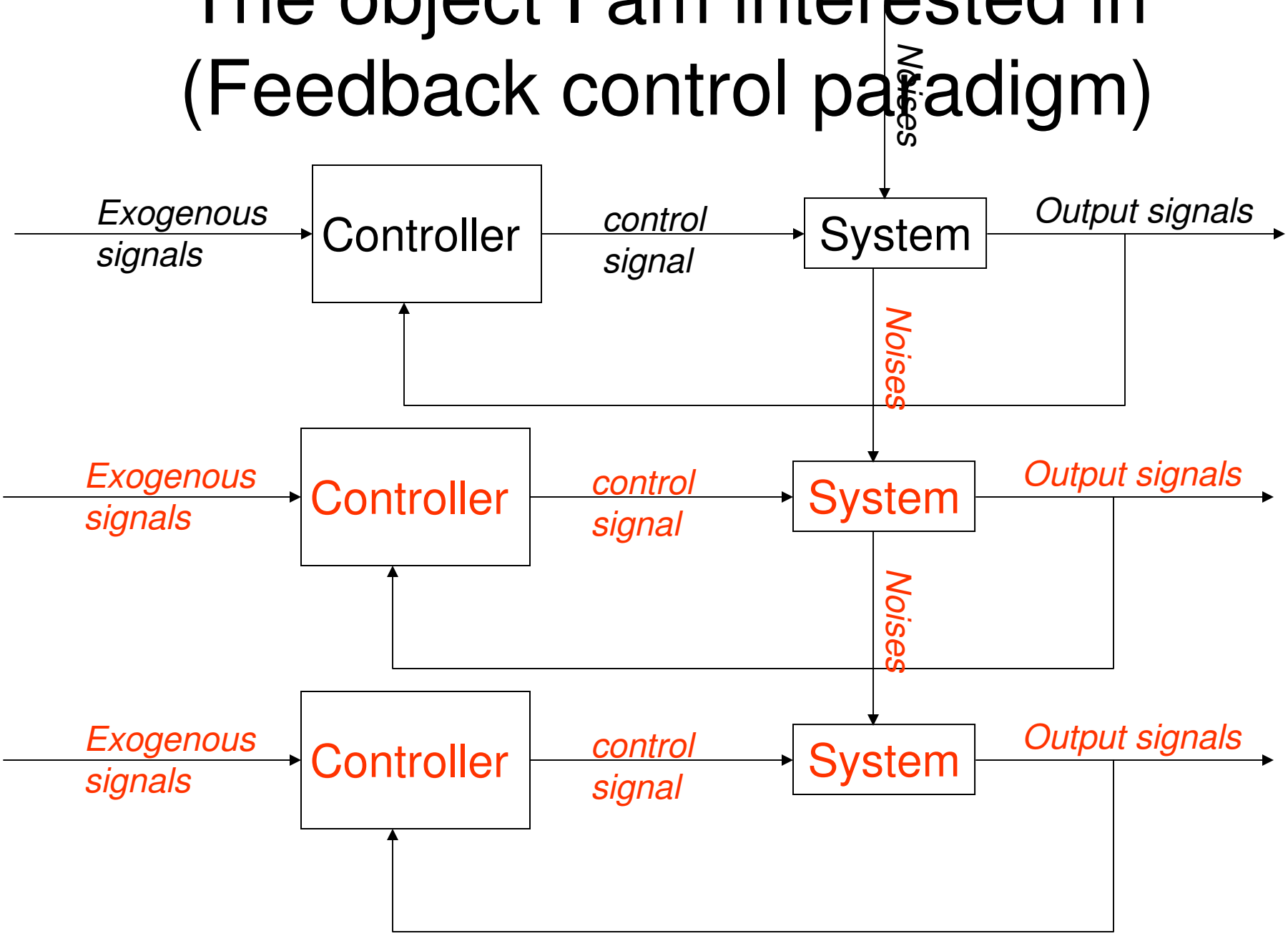
Control systems V&V

Eric Feron

The object I am interested in (Feedback control paradigm)



Chracteristics of control system design

- Big emphasis on model-based design: Model of the controller and model of the object to be controlled
- Big emphasis on formalism: Implementation won't proceed until thorough analysis of controller properties. First and foremost "stability"
- Previous bullet forced by catastrophic consequences of system failure

Analyses of control systems

- Many “static analyzers” of system specifications:
  - Bode, Nyquist, Root-locus plots: Survivors or “back of the envelope” analysis era. Not full coverage of possible behaviors.
  - Mu tools, IQC beta: primarily continuous, primarily linear systems with uncertainties. Full coverage of possible behaviors. Automatic extraction of invariants (Lyapunov theory).
  - Linear matrix inequalities, sum of squares, polynomial methods: Application to nonlinear systems, possibly discrete “mode switches”. Automatic extraction of invariants.
  - Other tools for analysis of systems with continuous and discrete components. Also analysis of “Systems that optimize”.
  - Some analyses available for specific concurrent processes (consensus seeking algorithms)

- Creative, case-to-case methods (1 proof→1 paper) are still very fashionable: Case-study driven.

Control systems and software

- Control systems coded by hand or auto-coded.
- Semantics of specifications usually not handed down to implementations.
- Some code-level static analyses (eg variable boundedness) already available and proven at specification level but not handed down.

Control systems and certification (Alwyn Goodloe, NASA)

- “System level stuff”

Stability, performance analyses as indicated above. Including static analyses.

- “Software level stuff” (DO-178B/C)

Correctness of software implementation of specifications. Requirements for determinism.

- Encourages specification / implementation segregation.