Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems

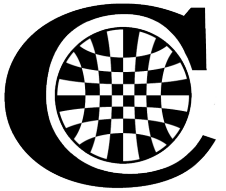
Surveyed and presented by

Hokeun Kim, Antonio Iannopollo

EECS, University of California, Berkeley

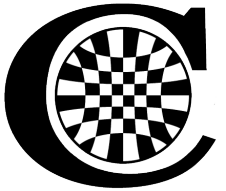
Chess

Introduction



- Cyber-physical systems
  - Integrations of computation with physical processes
  - Distributed in nature, involves large industries
- Complexities in designing cyber-physical systems
  - Complexity in systems
    - Distributed systems with heterogeneous components
  - Complexity in supply chains
    - Different vendors using a variety of design methods

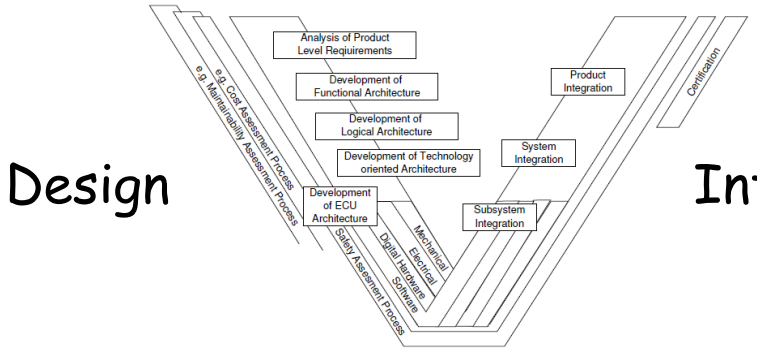
Introduction (cont'd)



- Contract-based design
  - Solution to cope with design complexity in cyber-physical systems
  - Formulates a broad and aggressive scope
  - Models description of functions, performances (time, energy, etc.), and safety
- Contracts
  - Formalizations of the conditions for correctness of element integration
  - Assume/Guarantee reasoning
    - $C=(A,G)=\{\text{Assumptions, Promises}\}$

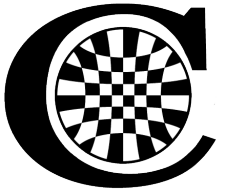
Methodologies

- For complexity of systems
  - Layered design
    - Supporting design activities at the corresponding level of abstraction
  - Component-based design
    - Assembling components with concise and rigorous interface specifications horizontally
  - The V-model of the design process
    - Splitting product development process into design and integration



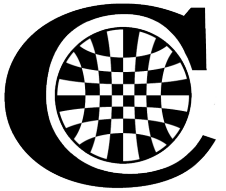
Design Integration

Methodologies (cont'd)



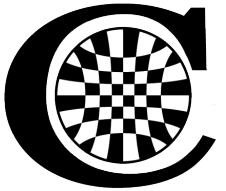
- For complexity of systems (cont'd)
  - Model-based development (MBD)
    - Support early requirement validation and virtual system integration
  - Virtual integration
    - Virtually integrate system, based on models of subsystems
- For complexity of supply chain
  - Standardization of design entities
  - Standardization/harmonization of processes

Contract model overview



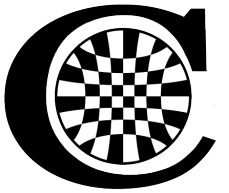
- Implementation
  - An instantiation "M" of a component, consists of
    - A set "P" of ports and variables
    - A set "M" of behaviors (or runs) which assign a history of "values" to ports
- Contract
  - Assertion "E"
    - A set of behaviors over ports
  - Contract "C", a pair of assertions "(A,G)" where
    - "A" represents assumptions given by an environment (physical part of a cyber-physical system)
    - "G" represents promises guaranteed by an implementation (cyber part of a cyber-physical system)

Contract model overview



- Relationship between an implementation "M" and an assertion "E" and a contract "C=(A,G)"
  - $M \subseteq E$, "M" satisfies "E"
  - $M \cap A \subseteq G$, For given assumption "A", "M" satisfies "G", or $M \models C$
- Controlled, uncontrolled ports and receptiveness
  - Ports of an implementation can be partitioned into controlled and uncontrolled ports, $\pi = (u,c)$
  - Assertion "E" is P'-receptive: E accepts any history offered to the subset P' of its ports P

Contract model overview (cont'd)



- Conjunction $\sqcap$
  - If $M \models C_f \sqcap C_t$, then $M \models C_f \wedge M \models C_t$
- Dominance
  - $C \preccurlyeq C'$: $C=(A,G)$ dominates $C'=(A',G')$ iff $A \supseteq A'$ and $G \subseteq G'$
  - If $M \models C$ and $C \preccurlyeq C'$, then $M \models C'$
- Consistency and Compatibility
  - For profile π = (u,c), where "u" represents uncontrolled ports and "c" represents controlled ports and contract $C=(A,G)$
  - C is consistent if G is u-receptive
  - C is compatible if A is c-receptive