TAMING DR. FRANKENSTEIN: CONTRACT-BASED DESIGN FOR CYBER-PHYSICAL SYSTEMS PT. 2

ANTONIO IANNOPOLLO EE249
HOKEUN KIM
Platform-based design and contract-based design to formulate the design process with a meet-in-the-middle approach.

- Can be considered both horizontal and vertical contracts.
- Used “to govern the horizontal composition of the cyber and the physical components and to establish the conditions for correctness of their composition.
- It is possible to design a correct-by-construction system.
PLATFORM-BASED DESIGN: KEY CONCEPTS

Design through different abstraction layers, each one defined by a design platform.

Each design platform consists of

• A set of library components

• Models of the components in terms of functional and non-functional characteristics

• Rules for the determination of component composition
CONTRACT-BASED DESIGN
HORIZONTAL CBD

At level N, a set of contracts (1 ... j) $C^H(S_j) = (A^H_j, G^H_j)$

refine a the global contract of the level N

$C^H_N(S) = (A^H_N(S), G^H_N(S))$

Circular reasoning only valid for some classes of contracts (G and A as safety properties)
VERTICAL CBD

Layer N + 1

AS_{N+1\_TD}, GS_{N+1\_TD}
S
AS_{N+1\_BU}, GS_{N+1\_BU}

Layer N

AS_{N\_TD}, GS_{N\_TD}

A_{1\_TD}, G_{1\_TD}
S_1
A_{1\_BU}, G_{1\_BU}

A_{2\_TD}, G_{2\_TD}
S_2
A_{2\_BU}, G_{2\_BU}

A_{3\_TD}, G_{3\_TD}
S_3
A_{3\_BU}, G_{3\_BU}

p_{31}
p_{12}
p_{23}
p_{2S}
p_{S1}
p_{S2}

Layer N - 1

AS_{N-1\_TD}, GS_{N-1\_TD}
S
AS_{N-1\_BU}, GS_{N-1\_BU}

Refinement (strong assumptions)

Aggregation (weak assumptions)
CBD EXAMPLE: A WATER FLOW CONTROL SYSTEM

Problem Information:
- Input: Inlet pressure P
- Output: Water Level \( w_l \), outlet flow rate \( F_{out} \), energy consumption \( E \)
- Parameters: container size \( D \) and \( H \), inlet cross sections \( S_{in} \) and \( S_{out} \), evaporation rate \( \varepsilon \).

Translated in the global contract:
- Assumption: \( P \geq 5000 \)
- Promises:
  \[
  \forall t. (t \geq 10 \implies (1.0 \leq F_{out} \leq 2.0)) \\
  \forall t. (w_l(t) \leq H) \\
  E \leq E_l
  \]
CBD APPROACH

- Define a contract for each component
- Compose the different contracts
- Verify that the obtained composite contract is a refinement of the global contract
CBD APPROACH

The composite contract is characterized by

- **I/O:**
  \[
  I = \{ \lambda_{cmd}, F, \varepsilon \} \\
  O = \{ \lambda, F_{in}, wl, F_{out} \}
  \]

- **Assumption:**
  \[ \forall t. \varepsilon(t) \leq 0.25 \]

- **Promises:**
  \[
  \frac{d\lambda}{dt} = \text{sgn}(\lambda_{cmd}(t) - \lambda(t)) \cdot 0.5 \\
  F_{in} = F \cdot (0.2\lambda^2 + 0.8\lambda) \\
  \lambda(0) = 0 \\
  \forall t, t'. t' > t \implies w(t') = w(t) + \\
  + \frac{1}{\pi(D/2)^2} \int_{t}^{t'} (F_{in}(t'') - F_{out}(t'') - \varepsilon(t'')) dt'' \\
  F_{out} = V \cdot S_{out} = \sqrt{2g\cdot w} \cdot S_{out}
  \]
CBD APPROACH

The composite contract is characterized by

- **I/O:**
  \[
  I = \{ \lambda_{cmd}, F, \varepsilon \} \\
  O = \{ \lambda, F_{in}, \text{wl}, F_{out} \}
  \]

- **Assumption:** \( \forall t. \varepsilon(t) \leq 0.25 \)

- **Promises:**
  \[
  \frac{d\lambda}{dt} = \text{sgn}(\lambda_{cmd}(t) - \lambda(t)) \cdot 0.5 \\
  F_{in} = F \cdot (0.2\lambda^2 + 0.8\lambda) \\
  \lambda(0) = 0 \\
  \forall t, t'. t' > t \implies \text{wl}(t') = \text{wl}(t) + \\
  + \frac{1}{\pi(D/2)^2} \int_t^{t'} (F_{in}(t'') - F_{out}(t'') - \varepsilon(t'')) dt''
  \]

\[
F_{out} = V \cdot S_{out} = \sqrt{2g\text{wl} \cdot S_{out}}
\]
**CBD APPROACH**

The composite contract is characterized by

- **I/O:**
  \[ I = \{ F, \varepsilon \} \]
  \[ O = \{ \lambda, \lambda_{cmd}, F_{in},wl, wlm,F_{out}, E \} \]

- **Assumption:** \( \forall t. \varepsilon(t) \leq 0.25 \)

- **Promises:**
  \[ \frac{d\lambda}{dt} = \text{sgn}(\lambda_{cmd}(t) - \lambda(t)) \cdot 0.5 \]
  \[ F_{in} = F \cdot (0.2\lambda^2 + 0.8\lambda) \]
  \[ \lambda(0) = 0 \]
  \[ \forall t,t'. t' > t \implies \text{wl}(t') = \text{wl}(t) + \text{wl} \]
  \[ + \frac{1}{\pi(D/2)^2} \int_{t}^{t'} (F_{in}(t'') - F_{out}(t'') - \varepsilon(t'')) dt'' \]
  \[ F_{out} = V \cdot S_{out} = \sqrt{2g \text{wl} \cdot S_{out}} \]

  \[ \forall t. 0.95 \cdot \text{wl}(t) \leq \text{wl}_m(t) \leq 1.05 \cdot \text{wl}(t) \]
  \[ \text{wl}_m \leq \text{wl}_{min} \implies \lambda_{cmd} = 1 \]
  \[ \text{wl}_m \geq \text{wl}_{max} \implies \lambda_{cmd} = 0 \]
VERTICAL CONTRACTS IN CONTROL

Controllers are “bounds by contracts to the plant”
CONCLUSION

• Even in their most elementary form (informal textual requirements) contracts have a considerable methodological value

• Can be customized to match particular viewpoints in different design phases (safety, real-time, costs)

• Formal definition of contracts allows to think about new tools and frameworks