Joint use of SysML and Reo to specify and verify CPS components

Perla Tannoury, Samir Chouali, and Ahmed Hammad

FEMTO-ST Institute, Univ. Bourgogne Franche-Comté, CNRS, France
Contexte : CPS

- Cyber-Physical Systems (CPS):
  - Collection of software and physical components.
  - Complex interaction between components.
CPS examples

Copyright © Dr. Sandip Ray 2021.

Copyright © Yong-Woon Hwang and Im-Yeong Lee 2020.
Objectif

How can we correctly model CPS?
CPS: Challenges

- Heterogeneity
- Interoperability
- Modeling difficulties
- Criticality
Outline

1. CPS context, examples
2. Objectif
3. CPS challenges
4. How to effectively model CPS?
5. How to enhance CPS interoperability and critical verification?
6. Contributions
   ○ Creating SysReo
   ○ CPS specification with SysReo
   ○ CPS verification with SysReo
7. Conclusion and future work
How can we effectively model CPS heterogeneous components for stakeholder comprehension, aligning with system requirements, architecture, and behavior?
Phase 1: Modeling CPS with SysML

- **System Modeling Language (SysML):**
  - OMG Standard.
  - Widely used in industries.
  - Model both the logical and physical components of a CPS.
  - Structured CPS modeling, covering requirements, architecture, and behavior (RD, BDD, IBD, SD, etc.).
Phase 1: SysML drawbacks

- **SysML drawbacks:**
  - Semi-formal language without the capability for formal verification of critical CPS.
  - Limited in accurately modeling complex behaviors (protocols) and component coordination in a CPS.
  - Limited in achieving full interoperability among CPS components.
How can we ensure **seamless interoperability** and verify **critical** requirements in CPS through effective modeling of **behaviors** and **coordination protocols**?
Phase 2: Modeling CPS with Reo

- **Reo coordination language:**
  - Exogenous Protocols: Captures explicitly system protocols.
  - Graphical notation: Enhances SysML models through Reo connectors or circuits.
  - Ordered Data Exchange: Enforces constraints on data exchange among components.
  - Formal semantics: Enables formal verification of CPS properties.
Phase 2: Reo drawbacks

- **Reo drawbacks:**
  - Challenging for Stakeholders: Formal semantics, hard to grasp, leading to potential compatibility issues and increased effort.
  - Limited Adoption and Support: Fewer resources, tools, and community support compared to widely adopted SysML.
Solution to CPS challenges

- Heterogeneity
- Modeling difficulties
- Interoperability
- Criticality

SysML

Reo

CPS challenges

SysReo

"Joint use of SysML and Reo to specify and verify the compatibility of CPS components"
Why SysReo?

- Explicit Protocol Modeling
- Holistic Design Approach
- Critical CPS Verification
- Stakeholder-Friendly

"Joint use of SysML and Reo to specify and verify the compatibility of CPS components"
How to model a CPS with **SysReo**?
1) Specification process: SysReo
1) Specification process: SysReo
Extending SysML with Reo:

Perla Tannoury
“Joint use of SysML and Reo to specify and verify the compatibility of CPS components”
1) Specification process: SysReo

**SysML IBD vs Reo IBD:**

(a) IBD of CBTC

(a) Reo IBD of CBTC

Perla Tannoury

“Joint use of SysML and Reo to specify and verify the compatibility of CPS components”
SysReo in a nutshell

- **SysReo**
  - Capture various aspects of CPS at all design levels (ExtBDD).
  - Explicitly characterize message flow and their properties (Reo IBD).

- Previous work focuses on SysML alone or Reo alone, but never on both.

- **SysReo** offers detailed and precise communication between components by explicitly modeling their architectures and interaction protocols.
2) Verification Process

1) Specification Process

- Specification: SysReo model
  - 1) Requirement Diagram
  - 2.1) ExtBDD, 2.2) Reo IBD
  - 3) SysReo SD

2) Verification Process

- Correct CPS
  - True verification results

- 4.1) Translation through algorithm
  - Formal Model: CA

- 4.2) Translation through property formulas
  - Formal Model: LTL

- 5) Verification: Veeofy Tool
Why SysReo SD?

- **SysReo SD:**
  - Extends SysML SD with Reo notation enhancing message exchange, coordination, and synchronization.
  - Enables explicit protocol specification.
  - Offers a comprehensive method for specifying protocols in system behavior and coordination.
  - Particularly advantageous for capturing communication flow and coordination in a single diagram.
2) Verification process: SysReo SD

Step 1: Extending SysML SD with Reo Sequencer

A) SysML SD

B) SysReo SD

Protocol: Reo sequencer

Step 2: Translating SysReo SD to CA

How to transform SysReo SD to Constraint automata?
2) Verification Process: Constraint Automata (CA)

- **Definition CA:**
  - A constraint automaton \( B = (S, S_0, N, \delta) \) is composed of:
    - \( S \): set of states (or locations).
    - \( S_0 \): initial state where \( S_0 \in S \).
    - \( N \): set of port names.
    - \( \delta \): transition relation \( \delta \subseteq S \times 2^N \times DC \times S \), where \( DC \) is the set of Data Constraints (DC) over a finite data domain Data.

- Formal representation and specification of Reo.
- Captures interactions and data flow in coordination models.
- Input for verification tools, e.g., Vereofy.
2) Verification Process Example using Vereofy

Rq1: The “SB” must constantly send temperature data to the “RTU” component using “sendTempData” message.

Rq2: The “RTU” shall respond to the “SB” component with an “ack” message.

Rq1: LTL: \[ G("\{A\} \& \#A == 1\} \rightarrow X(" state == S1 " \& " sendTempData == 1\} ) \] 

Rq2: LTL: \[ G("\{W\} \& \#W==1\})-\rightarrow X("state==S0" \& "ack==1")\]
Conclusion and Future Work

- **SysReo Introduction:**
  - A novel language for CPS modeling.
  - Ensuring CPS architecture, inner structure and interaction protocols.

- **Main contribution:**
  - Introducing SysReo SD that captures CPS behavior using exogenous protocol coordination.
  - Translating SysReo SD into Constraint Automata (CA).
  - Using Vereofy tool that verifies LTL properties for design compliance.

- **Future Work:**
  - Considering real-time notations in coordination and behavior of CPS components.
  - Exploring SysReo in Digital Twins (DT) for virtual interactions and behaviors.
Thank you!

Perla Tannoury

Université de Bourgogne Franche-comté (UBFC)

perla.tannoury@femto-st.fr