TOWARDS THE APPLICABILITY OF ALF TO MODEL CYBER-PHYSICAL SYSTEMS

Alessandro Gerlinger Romero
romgerale@yahoo.com.br
Klaus Schneider
Maurício Gonçalves Vieira Ferreira

Brazilian National Institute for Space Research – INPE – Brazil
Department of Computer Science – University of Kaiserslautern – Germany

International Workshop on Cyber-Physical Systems (IWCPS’13)
Kraków, Poland, September 8-11, 2013
Agenda

• Introduction
  ▪ Motivation
  ▪ Goal

• Context

• Initial approach
  ▪ Timing and Concurrency
  ▪ Inter-Object Communication

• Example

• Conclusions
Agenda

• Introduction
  ▪ Motivation
  ▪ Goal
• Context
• Initial approach
  ▪ Timing and Concurrency
  ▪ Inter-Object Communication
• Example
• Conclusions
Motivation

• Cartwright *et al.* (2006) define the following topics as the most important research challenges in CPSs:

  (1) Effective methods for **analysis**, simulation and validation of models;

  (2) Methods and techniques for guaranteeing real-time properties;

  (3) **Modeling languages** for (hybrid) cyber-physical systems.
Goal

• **Problem:** Behavioural definitions in SysML – activity diagrams, sequence diagrams, state machine diagrams, action language, etc...

• **Goal:** *specialization* to the *action language* for foundational UML (Alf)
  • according to the *synchronous-reactive* Model of Computation
  • for *discrete* behavioural definitions
  • embedded in *SysML* models describing *CPSs*.

*The properties themselves are more difficult to state, were *weaker than* could be achieved in the *synchronous case*, and required *considerable complexity* to be added to the model to ensure that even the weakened properties were true.*

(Miller et. Al., 2005, section 6.3, pg 23)
Agenda

• Introduction
  ▪ Motivation
  ▪ Goal

• Context

• Initial approach
  ▪ Timing and Concurrency
  ▪ Inter-Object Communication

• Example

• Conclusions
Towards the Applicability of Alf to Model Cyber-Physical Systems

CPSs

Hybrid System

Network

(Zhang et al., 2008)

(Ogata, 2009)
OMG Specifications – fUML and Alf

- **fUML** (Semantics of a Foundational Subset for Executable UML Models) is a subset of UML consisting of the key parts of UML **activities** and **classes** (OMG, 2012).

- **Alf** is the **concrete syntax** for the abstract action language defined by fUML (OMG, 2013).

- fUML, and also Alf, is **not directly feasible to safety-critical systems** (execution model) is **nondeterministic** (Benyahia et. al., 2010).
OMG Specifications – fUML and Alf (2/2)

Slide 9 of 20
**SysML**

- **SysML (Systems Modeling Language)** - general-purpose modeling language for systems engineering applications. It reuses a subset of UML, and provides additional extensions to satisfy the necessities of systems engineering, e.g., Requirements Diagram, Parametric Diagram, and allocation.
Towards the Applicability of Alf to Model Cyber-Physical Systems

Synchronous-reactive MoC

• Provides precise behavioural representation using the fundamental model of time as a **sequence of discrete** instants, **computation and communication executed in zero-time**, and **parallel composition as a conjunction** of behaviors (Benveniste *et al.*, 2003). Solutions can be desynchronized.

• Macro step consists of finitely many micro steps
• Macro steps correspond to reactions of reactive systems, while micro steps correspond with atomic actions

• Languages: Esterel, Quartz, Signal, Lustre, etc...
Agenda

• Introduction
  ▪ Motivation
  ▪ Goal

• Context

• Initial approach
  ▪ Timing and Concurrency
  ▪ Inter-Object Communication

• Example

• Conclusions
Timing and Concurrency

- **Time**
  - a discrete succession of instants; each instant corresponds to one macro step
  - demarcation of macro steps @pausable
    - After each execution of a loop body, it waits for the next macro step.
    - All concurrent behaviors run in lockstep: they execute the actions inside the loop in zero time, and synchronize before next iteration.

- **Concurrency**
  - concurrent statements (using @parallel)
  - multiple active objects

### Annotations in the Specialized Alf

<table>
<thead>
<tr>
<th>Annotation</th>
<th>Informal semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td>@delayed</td>
<td>Delayed assignment or SendSignalAction</td>
</tr>
<tr>
<td>@pausable</td>
<td>Macro step demarcation</td>
</tr>
<tr>
<td>@parallel</td>
<td>Computations on each block are carried out concurrently</td>
</tr>
<tr>
<td>@nonblocking</td>
<td>AcceptEventAction read nonblocking, makes optional signals available</td>
</tr>
</tbody>
</table>
Inter-object communication

• Performed sending signals (*SendSignalAction*) to other active object (not blocking)
• Multicasting was introduced by an active class called *MessageDispatcher*
  • Work as bus transferring instances of signals between previously registered active objects, which generate events in the target active object.
Agenda

• Introduction
  ▪ Motivation
  ▪ Goal
• Context
• Initial approach
  ▪ Timing and Concurrency
  ▪ Inter-Object Communication
• Example
• Conclusions
Example – Synchronous Ping Pong

```java
//Player1
while(true){
    //@delayed
    this.messageDispatcher.send(this, new Pong()); //P11
    accept(Pong); //P12
}

//Player2
while(true){
    //@delayed
    this.messageDispatcher.send(this, new Pong()); //P21
    accept(Pong); //P22
}
```

```java
//PingPongSystem
MessageDispatcher bus = new MessageDispatcher(); //S1
this.player2 = new Player2(bus); //S2
this.player1 = new Player1(bus); //S3
bus.register(this.player1); bus.register(this.player2); //S4
//@pausable
while(true){ //S5
    
`; }
Agenda

- Introduction
  - Motivation
  - Goal
- Context
- Initial approach
  - Timing and Concurrency
  - Inter-Object Communication
- Example
- Conclusions
Conclusions

• **Specializing** well-known vendor-independent specifications (Alf and SysML) can provide an understandable set of languages for modeling, analyzing, and verifying CPS.

• Such a set of languages can enable **formal** verification for **discrete** parts of CPS.
Acknowledgment
TOWARDS THE APPLICABILITY OF ALF TO MODEL CYBER-PHYSICAL SYSTEMS

Alessandro Gerlinger Romero
romgerale@yahoo.com.br
Klaus Schneider
Maurício Gonçalves Vieira Ferreira

Brazilian National Institute for Space Research – INPE – Brazil
Department of Computer Science – University of Kaiserslautern – Germany

International Workshop on Cyber-Physical Systems (IWCPS’13)
Kraków, Poland, September 8-11, 2013