Building a Hybrid Systems Modeler from Synchronous Language Principles

Marc Pouzet

DI, École normale supérieure
Marc.Pouzet@ens.fr

IRT SystemX, Palaiseau
January 26, 2016

¹Joint work with A. Benveniste, T. Bourke, B. Caillaud (INRIA); J-L. Colaco, B.
Pagano, C. Pasteur (Esterel-Tech./ANSYS Core Team)
SCADE: a DSL for critical control software

- Pioneering work of Caspi and Halbwachs on Lustre.
- SCADE 6 provides original language extensions and compile-time analysis, with traceable compilation down to C code.
But modern systems need more
The Current Practice of Hybrid Systems Modeling

Embedded software interacts with physical devices.
The whole system has to be modeled: the controller and the plant.²

²Image by Esterel-Technologies/ANSYS.
Current Practice and Objective

Current Practice

- Simulink, Modelica used to **model**, rarely to **implement** critical soft.
- Software must be reimplemented in SCADE or imperative code.
- Interconnect tools (Simulink + Modelica + SCADE + Simploter + ...)
- Interchange format for co-simulation: S-functions, FMU/FMI

Objective

- **Increase the confidence** in what is simulated
- Reduce compiler bugs
- Synchronous code for both the controller and the plant
## Hybrid System Modelers

<table>
<thead>
<tr>
<th>Simulink / FMI</th>
<th>Simploer / Modelica</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordinary differential equation</td>
<td>Differential algebraic equation</td>
</tr>
<tr>
<td>( \dot{y} = f(y, t) )</td>
<td>( f(y, \dot{y}, t) = 0 )</td>
</tr>
<tr>
<td>Explicit</td>
<td>Implicit</td>
</tr>
<tr>
<td>Causal</td>
<td>Acausal</td>
</tr>
</tbody>
</table>

Ordinary differential equation:

\[
\dot{y} = f(y, t)
\]

Differential algebraic equation:

\[
f(y, \dot{y}, t) = 0
\]
## Hybrid System Modelers

<table>
<thead>
<tr>
<th>Simulink / FMI / Zélus / <strong>Scade Hybrid</strong></th>
<th>Simulorer / Modelica</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ordinary differential equation</strong></td>
<td><strong>Differential algebraic equation</strong></td>
</tr>
<tr>
<td>( \dot{y} = f(y, t) )</td>
<td>( f(y, \dot{y}, t) = 0 )</td>
</tr>
<tr>
<td>Explicit</td>
<td>Implicit</td>
</tr>
<tr>
<td>Causal</td>
<td>Acausal</td>
</tr>
</tbody>
</table>
Strange beasts...
Typing issue 1: Mixing continuous & discrete components

The shape of \( \text{cpt} \) depends on the steps chosen by the solver. Putting another component in parallel can change the result.
Typing issue 1: Mixing continuous & discrete components

![Diagram](image)

- The shape of `cpt` depends on the steps chosen by the solver.
- Putting another component in parallel can change the result.
Typing issue 2: Boolean guards in continuous automata

How long is a discrete step?

- Adding a parallel component changes the result.
- No warning by the compiler.
- The manual says: “A single transition is taken per major step”.

Discrete time is not logical: it is that of the simulation engine.
Causality issue: the Simulink state port

The output of the state port is the same as the output of the block's standard output port except for the following case. If the block is reset in the current time step, the output of the state port is the value that would have appeared at the block's standard output if the block had not been reset.

–Simulink Reference (2-685)
Causality issue: the Simulink state port

The output of the state port is the same as the output of the block’s standard output port except for the following case. If the block is reset in the current time step, the output of the state port is the value that would have appeared at the block’s standard output if the block had not been reset.

–Simulink Reference (2-685)

\[ t < 2: \quad x(t) = t, \quad y(t) = \frac{t^2}{2} \]

\[ t = 2: \quad x = -3 \cdot \text{last } y = -6, \quad y = -4 \cdot \text{last } x = -8 \]
Causality issue: the Simulink state port

The output of the state port is the same as the output of the block’s standard output port except for the following case. If the block is reset in the current time step, the output of the state port is the value that would have appeared at the block’s standard output if the block had not been reset.

–Simulink Reference (2-685)

\[ t < 2: \quad x(t) = t, \quad y(t) = \frac{t^2}{2} \]

\[ t = 2: \quad x = -3 \cdot \text{last} \ y = -6, \quad y = -4 \cdot \text{last} \ x = -8 \]
Causality issue: the Simulink state port

\[ t < 2: \quad x(t) = t, \quad y(t) = \frac{t^2}{2} \]

\[ t = 2: \quad x = -3 \cdot \text{last } y = -6, \]

\[ y = -4 \cdot \text{last } x = -8 \]

The output of the state port is the value that would have appeared at the block’s standard output if the block had not been reset.

\[ \text{Simulink Reference (2-685)} \]
Excerpt of C code produced by RTW (release R2009)

```c
static void mdlOutputs(SimStruct * S, int_T tid)
{
    _rtX = (ssGetContStates(S));
    ...
    _rtB = (_ssGetBlockIo(S));
    _rtB->B_0_0_0 = _rtX->Integrator1_CSTATE + _rtP->P_0;
    _rtB->B_0_1_0 = _rtP->P_1 * _rtX->Integrator1_CSTATE;
    if (ssIsMajorTimeStep (S))
    {
        if (zcEvent || ...)
        {
            (ssGetContStates (S))->Integrator0_CSTATE =
                _ssGetBlockIo (S))->B_0_1_0;
        }
        ...
    }
    ...
    (_ssGetBlockIo (S))->B_0_2_0 =
        (ssGetContStates (S))->Integrator0_CSTATE;
    _rtB->B_0_3_0 = _rtP->P_2 * _rtX->Integrator0_CSTATE;
    if (ssIsMajorTimeStep (S))
    {
        if (zcEvent || ...)
        {
            (ssGetContStates (S))->Integrator1_CSTATE =
                (ssGetBlockIo (S))->B_0_3_0;
        }
    }
    ...
}
```

Before assignment: integrator state contains ‘last’ value

After assignment: integrator state contains the new value

$x = -3 \cdot \text{last } y$

$y = -4 \cdot x$

So, $y$ is updated with the new value of $x$

There is a problem in the treatment of causality.
Causality: Modelica example

model scheduling
  Real x(start = 0);
  Real y(start = 0);
equation
  der(x) = 1;
  der(y) = x;

  when x >= 2 then
    reinit(x, -3 * y)
  end when;
  when x >= 2 then
    reinit(y, -4 * x);
  end when;
end scheduling;
Causality: Modelica example

model scheduling
    Real x(start = 0);
    Real y(start = 0);
equation
    der(x) = 1;
    der(y) = x;
    when x >= 2 then
        reinit(x, -3*y)
    end when;
    when x >= 2 then
        reinit(y, -4*x);
    end when;
end scheduling;
model scheduling
  Real x(start = 0);
  Real y(start = 0);
equation
  der(x) = 1;
  der(y) = x;
  when x >= 2 then
    reinit(x, -3 * y)
  end when;
  when x >= 2 then
    reinit(y, -4 * x);
  end when;
end scheduling;
Background: [Benveniste et al., 2010 - 2014]

“Build a hybrid modeler on synchronous language principles”

Milestones

- Do as if time was global and discrete [JCSS’12]
- Lustre with ODEs [LCTES’11]
- Hierarchical automata, both discrete and hybrid [EMSOFT’11]
- Causality analysis [HSCC’14]

This was experimented in the language Zélus [HCSS’13]

The validation on an industrial compiler remained to be done.

SCADE Hybrid (summer 2014)

- Prototype based on KCG 6.4 (now KCG 6.5 - 2015)
- SCADE Hybrid = full SCADE + ODEs
- Generates FMI 1.0 model-exchange FMUs with Simploter
In the sequel, we give examples in the concrete syntax of Zélus. Examples in SCADE Hybrid and generated C code at:

zelus.di.ens.fr/cc2015
Synchronous languages in a slide

- Compose stream functions; basic values are streams.
- Operation apply pointwise + unit delay (fby) + automata.

\[(\ast \text{computes } x(n) + y(n) + 1 \text{ at every instant } n \ast)\]
\[
\text{fun add } (x,y) = x + y + 1
\]

\[(\ast \text{returns } \text{true} \text{ when the number of } t \text{ has reached } \text{bound} \ast)\]
\[
\text{node after (bound, t) = (c = bound) where}
\]
\[
\text{rec c = 0 fby (min(tick, bound))}
\]
\[
\text{and tick = if } t \text{ then } c + 1 \text{ else } c
\]

The counter can be instantiated twice in a two state automaton,

\[
\text{node blink (n, m, t) = x where}
\]
\[
\text{automaton}
\]
\[
| \text{On} \rightarrow \text{do } x = \text{true} \text{ until } (\text{after(n, t)}) \text{ then Off}
\]
\[
| \text{Off} \rightarrow \text{do } x = \text{false} \text{ until } (\text{after(m, t)}) \text{ then On}
\]

From it, a synchronous compiler produces \textbf{sequential loop-free code} that compute a single \textbf{step} of the system.
A Simple Hybrid System

Yet, time was discrete. Now, a simple heat controller. ³

\[
(*) a \text{ model of the heater defined by an ODE with two modes } *
\]

hybrid \( \text{heater(active)} = \text{temp} \) where

rec \( \text{der temp} = \text{if active then } c - k \times \text{temp else } - k \times \text{temp} \) init temp0

\[
(*) \text{ an hysteresis controller for a heater } *
\]

hybrid \( \text{hysteresis\_controller(temp)} = \text{active} \) where

rec automaton

| Idle \( \rightarrow \) do active = false until (up(t\_min \( - \) temp)) then Active
| Active \( \rightarrow \) do active = true until (up(temp \( - \) t\_max)) then Idle

\[
(*) \text{ The controller and the plant are put parallel } *
\]

hybrid \( \text{main()} = \text{temp} \) where

rec active = hysteresis\_controller(temp)

and temp = heater(active)

Three syntactic novelties: keyword \textit{hybrid}, \textit{der} and \textit{up}.

---

³Hybrid version of N. Halbwachs’s example in Lustre at Collège de France, Jan.10.
From Discrete to Hybrid

The type language [LCTES'11]

\[
bt \ ::= \ \text{float} | \text{int} | \text{bool} | \text{zero} | \cdots \\
\sigma \ ::= \ bt \times \cdots \times bt \xrightarrow{k} bt \times \cdots \times bt \\
k \ ::= \ D | C | A
\]

Function Definition: \( \text{fun } f(x_1, \ldots) = (y_1, \ldots) \)

- **Combinatorial functions** (A); usable anywhere.

Node Definition: \( \text{node } f(x_1, \ldots) = (y_1, \ldots) \)

- **Discrete-time constructs** (D) of SCADE/Lustre: pre, \( \rightarrow \), fby.

Hybrid Definition: \( \text{hybrid } f(x_1, \ldots) = (y_1, \ldots) \)

- **Continuous-time constructs** (C): \( \text{der } x = \ldots \), up, down, etc.
Mixing continuous/discrete parts

Zero-crossing events

- They correspond to event indicators/state events in FMI
- Detected by the solver when a given signal crosses zero

Design choices

- A discrete computation can only be triggered by a zero-crossing
- Discrete state only changes at a zero-crossing event
- A continuous state can be reset at a zero-crossing event
Example

node counter() = cpt where
  rec cpt = 1 → pre cpt + 1

hybrid hybrid_counter() = cpt where
  rec cpt = present up(z) → counter() init 0
  and z = sinus()

Output with SCADE Hybrid + Simpler
Mix of synchronous code and a continuous model

E.g., implement the hysteresis controller by a synchronous function.

\[ (*) \text{ a discrete-time model of the controller; periodically sampled } (*) \]
\[
\text{node hysteresis_controller(temp) = active where}
\]
\[
\text{rec automaton}
\]
\[
| \text{Idle } \rightarrow \text{ do active = false until } (\text{temp } \leq \text{t}_{\text{min}}) \text{ then Active}
\]
\[
| \text{Active } \rightarrow \text{ do active = true until } (\text{temp } \geq \text{t}_{\text{max}}) \text{ then Idle}
\]

\[ (*) \text{ The controller and the plant are put parallel } (*) \]
\[
\text{hybrid main() = temp where}
\]
\[
\text{rec active = present (period (0.1)) } \rightarrow \text{ hysteresis_controller(temp) init false}
\]
\[
\text{and temp = heater(active)}
\]
Continuous and discrete PI controller [demo]

hybrid integr(x, y0) = y where
  rec der y = x init y0

hybrid pi(kp, ki, i) = cmd where
  rec cmd = kp \cdot i + ki \cdot integr(i, 0.0)
tel

let ts = 0.05

node disc_integr(x, y0) = y where
  rec init y = y0 and y = last y + Ts \cdot x

node disc_pi(kp, ki, i) = cmd where
  rec init cmd = Kp \cdot i
  and cmd = kp \cdot i + ki \cdot disc_integr(i, 0.0)
How to communicate between continuous and discrete time?

E.g., the bouncing ball

```plaintext
hybrid ball(y0) = y where
  rec der y = y_v init y0
  and der y_v = - g init 0.0 reset z \rightarrow 0.8 \ast last y_v
  and z = up(- y)
```

- Replacing `last y_v` by `y_v` would lead to a deadlock.
- In SCADE and Zélus, `last y_v` is the previous value of `y_v`.
- It coincides with the **left limit** of `y_v` when `y_v` is left continuous.
Internals
The Simulation Engine of Hybrid Systems

Alternate discrete steps and integration steps

\[ \sigma', y' = \text{next}_\sigma(t, y) \quad \text{upz} = g_\sigma(t, y) \quad \dot{y} = f_\sigma(t, y) \]

Properties of the three functions

- \( \text{next}_\sigma \) gathers all discrete changes.
- \( g_\sigma \) defines signals for zero-crossing detection.
- \( f_\sigma \) is the function to integrate.
Compilation

The Compiler has to produce:

1. Initialization function \textit{init} to define $y(0)$ and $\sigma(0)$.
2. Functions $f$ and $g$.
3. Function \textit{next}.

The Runtime System

1. Program the simulation loop, using a black-box solver (e.g., SUNDIALS CVODE);
2. Or rely on an existing infrastructure.

\textit{Zélus} follows (1); \textit{SCADE Hybrid} follows (2), targetting Simploter FMIs.
Compiler Architecture

Two implementations: Zélus and KCG 6.4 (Release 2014) of SCADE.

KCG 6.4 of SCADE

- Generates FMI 1.0 model-exchange FMUs for Simploer.
- Only 5% of the compiler modified. Small changes in:
  - static analysis (typing, causality).
  - automata translation; code generation.
  - FMU generation (XML description, wrapper).
- FMU integration loop: about 1000 LoC.
A SCADE-like Input Language

Essentially SCADE with three syntax extensions (in red).

d ::= const \ x = e | k f(pi) = pi where E | d; d
k ::= fun | node | hybrid
e ::= x | ν | op(e,...,e) | ν fby e | last \ x | f(e,...,e) | up(e)
p ::= x | (x,...,x)
pi ::= xi | xi,...,xi
xi ::= x | \ x last e | \ x default e
E ::= p = e | der \ x = e
| if e then E else E
| reset E every e
| local pi in E | do E and ... E done
A Clocked Data-flow Internal Language

The internal language is extended with three extra operations. Translation based on Colaco et al. [EMSOFT’05].

\[
d ::= \text{const } x = c \mid k f(p) = a \text{ where } C \mid d; d
\]

\[
k ::= \text{fun } \mid \text{node } \mid \text{hybrid}
\]

\[
C ::= (x_i = a_i)_{x_i \in I} \text{ with } \forall i \neq j . x_i \neq x_j
\]

\[
a ::= e^{ck}
\]

\[
e ::= x \mid v \mid op(a, \ldots, a) \mid v \text{ fby } a \mid \text{pre}(a) \mid f(a, \ldots, a) \mid \text{merge}(a, a, a) \mid a \text{ when } a \mid \text{integr}(a, a) \mid \text{up}(a)
\]

\[
p ::= x \mid (x, \ldots, x)
\]

\[
ck ::= \text{base } \mid ck \text{ on } a
\]
Clocked Equations Put in Normal Form

Name the result of every stateful operation. Separate into syntactic categories.

- **se**: strict expressions
- **de**: delayed expressions
- **ce**: controlled expressions.

Equation $lx = \text{integr}(x', x)$ defines $lx$ to be the continuous state variable; possibly reset with $x$.

$$
eq ::= \quad x = ce^ck \mid x = f(sa, \ldots, sa)^ck \mid x = de^ck$$

$$
sa ::= se^ck$$

$$
ca ::= ce^ck$$

$$
se ::= x \mid v \mid \text{op}(sa, \ldots, sa) \mid sa \text{ when } sa$$

$$
ce ::= se \mid \text{merge}(sa, ca, ca) \mid ca \text{ when } sa$$

$$
de ::= \text{pre}(ca) \mid v \text{ fby } ca \mid \text{integr}(ca, ca) \mid \text{up}(ca)$$
Well Scheduled Form

Equations are statically scheduled.

Read\((a)\): set of variables read by \(a\).

Given \(C = (x_i = a_i)_{x_i \in I}\), a valid schedule is a one-to-one function

\[
\text{Schedule}(.) : I \rightarrow \{1 \ldots |I|\}
\]

such that, for all \(x_i \in I, x_j \in \text{Read}(a_i) \cap I\):

1. if \(a_i\) is strict, \(\text{Schedule}(x_j) < \text{Schedule}(x_i)\) and
2. if \(a_i\) is delayed, \(\text{Schedule}(x_i) \leq \text{Schedule}(x_j)\).

From the data-dependence point-of-view, integr\((ca_1, ca_2)\) and up\((ca)\) break instantaneous loops.
A Sequential Object Language (SOL)

- Translation into an intermediate imperative language [Colaco et al., LCTES’08]
- Instead of producing two methods `step` and `reset`, produce more.
- Mark memory variables with a kind `m`

\[
\begin{align*}
md & ::= \text{const } x = c \\
& \quad \text{| const } f = \text{class} \langle M, I, \text{where } S_i \rangle_{i \in [1..n]} \\
M & ::= [x : m[= v]; \ldots; x : m[= v]] \\
I & ::= [o : f; \ldots; o : f] \\
m & ::= \text{Discrete} | \text{Zero} | \text{Cont} \\
e & ::= v | lv | \text{op}(e, \ldots, e) | o\text{.method}(e, \ldots, e) \\
S & ::= () | lv \left\leftarrow e | S ; S | \text{var } x, \ldots, x \text{ in } S | \text{if } c \text{ then } S \text{ else } S \\
R, L & ::= S ; \ldots; S \\
lv & ::= x | lv\text{.field} | \text{state}(x)
\end{align*}
\]
State Variables

Discrete State Variables (sort *Discrete*)

- Read with \texttt{state}(x);
- modified with \texttt{state}(x) ← c

Zero-crossing State Variables (sort *Zero*)

- A pair with two fields.
- The field \texttt{state}(x).zin is a boolean, true when a zero-crossing on \( x \) has been detected, false otherwise.
- The field \texttt{state}(x).zout is the value for which a zero-crossing must be detected.

Continuous State Variables (sort *Cont*)

- \texttt{state}(x).der is its instantaneous derivative;
- \texttt{state}(x).pos its value
Example: translation of the bouncing ball

```plaintext
let bouncing = machine(continuous) {
  memories disc init_25 : bool = true;
  zero result_17 : bool = false;
  cont y_v_15 : float = 0.; cont y_14 : float = 0.

  method reset =
    init_25 <- true; y_v_15.pos <- 0.

  method step time_23 y0_9 =
    (if init_25 then (y_14.pos <- y0_9; ()) else ());
    init_25 <- false;
    result_17.zout <- (~-.) y_14.pos;
    if result_17.zin
      then (y_v_15.pos <- ( *. ) 0.8 y_v_15.pos);
    y_14.der <- y_v_15.pos;
    y_v_15.der <- (~-.) g; y_14.pos }
```
Finally

1. Translate as usual to produce a function step.
2. For hybrid nodes, **copy-and-paste** the step method.
3. Either into a **cont** method activated during the continuous mode, or two extra methods **derivatives** and **crossings**.
4. Apply the following:
   - During the continuous mode (method **cont**), all zero-crossings (variables of type **zero**, e.g., \( \text{state}(x).\text{zin} \)) are surely false. All zero-crossing outputs (\( \text{state}(x).\text{zout} \leftarrow ... \)) are useless.
   - During the discrete step (method **step**), all derivative changes (\( \text{state}(x).\text{der} \leftarrow ... \)) are useless.
   - Remove dead-code by calling an existing pass.

5. That’s all!

Examples (both Zélus and SCADE) at: zelus.di.ens.fr/cc2015
Example: translation of the bouncing ball

let bouncing = machine(continuous) {
    memories disc init_25 : bool = true;
    zero result_17 : bool = false;
    cont y_v_15 : float = 0.; cont y_14 : float = 0.

    method reset =
        init_25 <- true; y_v_15.pos <- 0.
    method step time_23 y0_9 =
        (if init_25 then (y_14.pos <- y0_9; ()) else ());
        init_25 <- false;
        if result_17.zin
            then (y_v_15.pos <- ( *. ) 0.8 y_v_15.pos);
        y_14.pos
    method cont time_23 y0_9 =
        result_17.zout <- (~-. ) y_14.pos;
        y_14.der <- y_v_15.pos;
        y_v_15.der <- (~-. ) g }
Conclusion

Two full scale prototypes

- The Zélus academic langage and compiler.
- The industrial KCG 6.5 (Release 2015) code generator of SCADE.
- For KCG, less than 5% of extra LOC, in all.
- The extension is fully conservative w.r.t existing SCADE.
- The very same code is used both for simulation and embedded code.

Lessons

- The existing compiler architecture of SCADE KCG, based on successive rewritting, helped a lot.
- The discipline to make the extension compatible with existing compile-time checks and semantics helped a lot.
- Is-it helful for identifying a safe subset of Simulink?
- Replace SUNDIALS by a guaranted solver working with intervals?
Zélus
A synchronous language with ODEs

Compiler
Zélus is a synchronous language extended with Ordinary Differential Equations (ODEs) to model systems with complex interaction between discrete-time and continuous-time dynamics. It shares the basic principles of Lustre with features from Lucid Synchrone (type inference, hierarchical automata, and signals). The compiler is written

Research
Zélus is used to experiment with new techniques for building hybrid modelers like Simulink/Stateflow and Modelica on top of a synchronous language. The language exploits novel techniques for defining the semantics of hybrid modelers, it provides dedicated type systems to ensure the absence of discontinuities during integration and the
Bibliography

Albert Benveniste, Timothy Bourke, Benoit Caillaud, Bruno Pagano, and Marc Pouzet.
A Type-based Analysis of Causality Loops in Hybrid Systems Modelers.
In *International Conference on Hybrid Systems: Computation and Control (HSCC)*, Berlin, Germany, April 15–17 2014. ACM.

Albert Benveniste, Timothy Bourke, Benoit Caillaud, and Marc Pouzet.
A Hybrid Synchronous Language with Hierarchical Automata: Static Typing and Translation to Synchronous Code.

Albert Benveniste, Timothy Bourke, Benoit Caillaud, and Marc Pouzet.
Divide and recycle: types and compilation for a hybrid synchronous language.

Albert Benveniste, Timothy Bourke, Benoit Caillaud, and Marc Pouzet.
Non-Standard Semantics of Hybrid Systems Modelers.
Special issue in honor of Amir Pnueli.

Albert Benveniste, Benoit Caillaud, and Marc Pouzet.
The Fundamentals of Hybrid Systems Modelers.
In *49th IEEE International Conference on Decision and Control (CDC)*, Atlanta, Georgia, USA, December 15-17 2010.

Timothy Bourke, Jean-Louis Colaço, Bruno Pagano, Cédric Pasteur, and Marc Pouzet.
A Synchronous-based Code Generator For Explicit Hybrid Systems Languages.

Timothy Bourke and Marc Pouzet.
ZéluS, a Synchronous Language with ODEs.