Scade 6: A Formal Language for Embedded Critical Software Development
Jean-Louis Colaço, Bruno Pagano, Marc Pouzet

To cite this version:

HAL Id: hal-01666470
https://inria.hal.science/hal-01666470
Submitted on 18 Dec 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Scade 6: A Formal Language for Embedded Critical Software Development

(Invited Paper)

Jean-Louis Colaco
ANSYS/Esterel-Technologies, Jean-Louis.Colaco@ansys.com

Bruno Pagano
ANSYS/Esterel-Technologies, Bruno.Pagano@ansys.com

Marc Pouzet
UPMC/ENS/INRIA Paris, Marc.Pouzet@ens.fr

Abstract—SCADE is a high-level language and environment for developing safety critical embedded control software. It is used for more than twenty years in various application domains like avionics, nuclear plants, transportation, automotive. SCADE has been founded on the synchronous data-flow language Lustre invented by Caspi and Hallwachs. In the early years, it was mainly seen as a graphical notation for Lustre but with the unique and key addition of a code generator qualified with the highest standards for safety critical applications.

In 2008, a major revision based on the new language ‘Scade 6’ was released. This language originally combines the Lustre data-flow style with control structures borrowed from Esterel and SyncCharts, compilation and static analyses from Lucid Synchrone to ensure safety properties. This expressiveness increase for SCADE together with a qualified code generator have dramatically widened the scope of applications developed with.

While previous publications have described some of its language constructs and compiler algorithms, no reference publication on ‘Scade 6’ existed so far. In this paper, we come back to the decisions made for its design, illustrate the main language features, static analyses, and the compiler organization in the context of a qualification process.

I. INTRODUCTION

Synchronous languages [1] were introduced about thirty years ago by the concomitant work on three academic languages: SIGNAL [2], ESTEREL [3] and LUSTRE [4]. These domain specific languages were targeted for real-time control software, allowing to write a modular and mathematically precise system specification, to simulate, test and verify it, and to automatically translate it into embedded executable code.

They were founded on the synchronous approach [5] where a system is modeled ideally, with communications/computations supposed to be instantaneous, formally checking on the model important safety properties like determinism, deadlock freedom, the ability to generate an implementation that runs in bounded time and space, and verifying a posteriori that this implementation (software or hardware) is fast enough.

These foundations immediately raised the interest of industries having to deal with safety critical applications implemented in software or hardware, in particular those assessed by independent authorities and following certification standards [6]. This is the context in which SCADE 1 was initiated in the mid nineties, with the support of two companies, Airbus and Merlin Gerin, by a collaboration between the

1SCADE stands for: Safety Critical Development Environment

2http://www.ansys.com/products/embedded-software/ansys-scade-suite


to automatically translate it into embedded executable code. The objective in designing SCADE 6 was to provide novel language features to widen the scope of applications developed with SCADE, but carefully selected to preserve the qualities that made SCADE accepted for safety critical development. One was the mix of models, from purely data-flow ones already well covered, to control-flow ones better covered by languages like ESTEREL and the SyncChart [9], and complex interactions between the two. An other limitation of SCADE was the absence of arrays. LUSTRE V4 provided powerful recursive arrays definitions very well suited for hardware but the static expansion they imposed was inadequate for software. Finally, there were also quests for other language extensions (such as modules), more expressive types (in particular around numerics), compiler optimizations.

To meet these objectives, we were guided by several works:

• ESTEREL and SyncChart for control-dominated system expressed by hierarchical state machines;
• functional arrays and iterators [10];
Several other works were instrumental. For example, mode automata [14] gave a first answer for writing mixed models between a subset of LUSTRE and the hierarchical automata of ARGOS [15]. Yet, several questions remained, in particular the integration in a complete language. The language ESTEREL V7 did integrate data-flow and control-flow but it was tuned for generating very efficient hardware. How to adapt it for software and integrate it into a qualified compiler was unknown at that time.

The main design decision was to build the language and compiler on the following idea: (1) define a minimal kernel language together with a static and dynamic semantics and used as some kind of ‘typed assembly language’ from which sequential code is produced; (2) express richer programming constructs in terms of the basic language by a source-to-source translation, and give a static and dynamic semantics for all language constructs that preserves this translation semantics. For the kernel language, we defined a clocked data-flow language, close to LUSTRE but with some modifications that we motivate.

This design decision was put into practice in Reluc, a prototype language and compiler written in OCAML that was used to experiment new programming constructs and compilation techniques. This prototype evolved continuously between 2000 and 2006. In 2006, SCade 6 was launched from it, with a first release in 2008.

In this paper, we present the way this design decision has been followed. We illustrate the main language features, compile-time static analyses and the compiler architecture. The paper focuses on the language, information about graphical support and modeling tool were published in [17].

Section II reminds the LUSTRE kernel behind SCade till version 5. Section III presents the new core language on which SCade 6 is built. Section IV illustrates the static semantics of SCade 6. Section V presents the mix of data-flow and control-flow. Section VI explains the treatment of arrays. Section VII discusses the code generator design and qualification. Section VIII gives a few concluding remarks.

In the paper, we use LUSTRE for the underlying language of SCade until version 5 and SCade 6 for the new versions.

II. From LUSTRE core to SCade 6 core

LUSTRE is a synchronous interpretation of the block diagrams used for decades by control engineers. In this interpretation, time is discrete and can be identified by an integer. Hence, a discrete-time signal is a sequence or stream of values and a system is a stream function.

A. The core LUSTRE language

Since sequences are the basic elements of LUSTRE, operations are lifted to apply pointwise. This is what is done in

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>nil</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>x0</td>
<td>y0</td>
<td>nil</td>
<td>...</td>
</tr>
<tr>
<td>x1</td>
<td>y1</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>x_n</td>
<td>y_n</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

An important primitive is the unit delay \( \text{pre} \) (for ‘previous’):

\[
\begin{array}{c|c|c|c}
\text{x} & x_0 & x_1 & x_2 & \ldots & x_n \ldots \\
\text{y} & y_0 & y_1 & y_2 & \ldots & y_n \ldots \\
\end{array}
\]

If \( x = (x_n)_{n \in \mathbb{N}} \), \( \text{pre} \ x \) is the sequence \((p_n)_{n \in \mathbb{N}}\) defined by:

\[
p_0 = \text{nil} \quad \text{and} \quad \forall n \in \mathbb{N}, p_{n+1} = x_n
\]

where \( \text{nil} \) is an undefined value of the right type.

The first value of a stream can be specified with the initialization operator \( (->) \):

\[
\begin{array}{c|c|c|c|c|c|c}
\text{x} & x_0 & x_1 & \ldots & x_n \ldots \\
\text{y} & y_0 & y_1 & \ldots & y_n \ldots \\
\end{array}
\]

More formally:

\[
\begin{array}{c}
(x -> y)_0 = x_0 \\
\forall n \in \mathbb{N}, (x -> y)_{n+1} = y_{n+1}
\end{array}
\]

Its combination with \( \text{pre} \) defines the initialized delay:

\[
\begin{array}{c|c|c|c|c|c|c}
\text{pre} \ x & x_0 & x_1 & \ldots & x_n \ldots \\
\text{pre} \ y & y_0 & y_1 & \ldots & y_{n-1} \ldots \\
\end{array}
\]

The following LUSTRE equation illustrates them:

\[
nat = 0 -> 1 + \text{pre} \ nat;
\]

which means that, for all \( n \in \mathbb{N} \):

\[
nat_n = (0 -> 1 + \text{pre} \ nat)_n = 0 \quad \text{if} \quad n = 0
\]

\[
= (1 + \text{pre} \ nat)_n = 1 + \text{nat}_{n-1} \quad \text{otherwise}
\]

The last important notion is that of a clock. The clock of a stream tells when its current value is present (or ready). Clocks are modified by two operators, when and current. A stream can be filtered according to a boolean condition:

\[
\begin{array}{c|c|c|c|c|c|c}
\text{h} & \text{true} & \text{false} & \text{true} & \text{true} & \text{false} \ldots \\
\text{x} & x_0 & x_1 & x_2 & x_3 & x_4 \ldots \\
\text{when h} & \_ & \_ & \_ & \_ \ldots \\
\end{array}
\]

The _ is not a special value but indicates the absence of a value. Thus, the stream \( x \text{ when h} \) is the sub-sequence \( x_0, x_2, x_3, \ldots \). We say that its clock is \( h \), that is, it is present when \( h \) is present and true. By filtering a stream, it is possible to model a slow process. E.g., if \( \varepsilon \) is a stream function such that its input and output are on the same clock, then \( f(x \text{ when h}) \) has clock \( h \) and contains the application of \( f \) to the sub-sequence of \( x \) filtered by \( h \). Note that \( h \) can be any boolean expression and thus, it can encode a periodic clock.
A stream can be completed by keeping its value between two samples. This corresponds to a zero-order hold.

\[
\begin{array}{c|ccccc}
 h & \text{true} & \text{false} & \text{false} & \text{true} & \text{false} \\
 a & a_0 & a_0 & a_0 & a_1 & a_1 \\
\end{array}
\]

If \( a \) has some clock \( h \), the clock of \( \text{current} \ a \) is the clock of the clock of \( a \). Hence, \( a \) cannot be on the fastest clock (termed the ‘base’ clock) of the system. \( \text{current} \) is the way to go from a slow process to a fast one. E.g., \( \text{current}(f(x \text{ when } h)) \) returns a stream whose clock is that of \( x \) and \( h \).

A program can be \textit{synchronously executed} when the execution can proceed as a global sequence of steps where streams expected to be present are indeed present and those expected absent are indeed absent. In particular, a combinatorial function that expects its two arguments to be present or absent, e.g., the operation \( + \), have its two arguments present or absent. All computations of the corresponding Kahn Process Network are clocked according to a global time scale, removing all necessary buffer synchronisations [18].

A dedicated static analysis, named the \textit{clock calculus}, statically rejects a program that actually uses a stream at a clock different from what is expected. E.g., writing \( x + (x \text{ when } h) \) is rejected because the sum operator expects its two arguments to be on the same clock.

In LUSTRE, a user defined operator (or stream function) is introduced by the keyword \textbf{node}. Below is the example of a smoothing function that computes the average of its input \( x \) with its previous value \( \text{pre } x \). Figure 1 shows the corresponding block diagram.

\[
\text{node sliding_average (x : real) returns (average : real);} \\
\text{let} \\
\text{average = x -> (x + \text{pre } x) / 2.0;} \\
\text{tel}
\]

The body is an unordered set of equations which allows introduce/remove auxiliary equations. E.g., the following node computes the very same sequence with a local variable \( s \):

\[
\text{node sliding_average (x : real) returns (average : real);} \\
\text{let} \\
\text{average = x -> s / 2.0;} \\
\text{s = x + \text{pre } x;} \\
\text{tel}
\]

An equation of the form \( x = e \), where \( x \) is a variable and \( e \) an expression holds at every instant, that is, \( \forall n \in \mathbb{N}, x_n = e_n \).

\textbf{B. The question of determinism}

The semantics of LUSTRE formally defines what is the current value of a stream. The compiler checks that this value exists, is unique, can be computed sequentially from current inputs, possibly past computed values and in bounded time and space. Parallelism is not the only source of non-determinism. Operators may introduce non-determinism too. An example is the operator \( \text{pre} \) whose initial value \( \text{nil} \) is undetermined. It is thus important that an observed output does not depend on it. \( \text{current} \) also introduces \( \text{nil} \). E.g.:

\[
\begin{array}{c|ccccc}
 h & \text{false} & \text{false} & \text{false} & \text{true} & \text{false} \\
 a & \text{nil} & \text{nil} & \text{nil} & a_0 & a_0 \\
\end{array}
\]

\( h \) is the clock of \( a \). The prefix of \( \text{nil} \) values is arbitrarily long, unless \( h \) is initially \text{true}. \( \text{current} \) (\( \text{pre } x \)) is another example of a stream defined only after the second value of \( x \).

The decision problem — is a given output depend on the actual value of \( \text{nil} \) — is undecidable in the general case and at least combinatorial. It can be safely approximated by a SAT problem. Yet the time complexity and good diagnostics are difficult to give. Moreover, its conclusion — the system is safe — would have to be justified in the context of a qualified compiler. For SCADE 6, we took a more modest approach, designing a dedicated initialization analysis which deals with the particular case of the un-initialized delay and refuse to compile a program where \( \text{nil} \) may happen anywhere but in a first position of a sequence.

\textbf{III. SCADE 6: A NEW DATA-FLOW CORE}

Instead of \( \text{current} \) we chose an alternative operator \( \text{merge} \) borrowed from LUCID SYNCHRONIZE and which merges two complementary streams.

\[
\begin{array}{c|ccccc}
 h & \text{true} & \text{false} & \text{true} & \text{true} & \text{false} \\
 a & a_0 & a_0 & a_1 & a_2 & a_2 \\
 b & b_0 & b_0 & b_1 & b_1 & b_2 \\
\end{array}
\]

\( \text{hold(i, h, a)} \) which holds the value of \( a \) itself on clock \( h \) is programmed:

\[
\text{node hold (i: 't; clock h: bool; a: 't when h) returns (o : 't);} \\
\text{o = merge(h; a; (i -> \text{pre } o) when not h);} \\
\]

Contrary to \( \text{current} \), \( \text{merge} \) does not introduce a \( \text{nil} \). Moreover, its implementation does not use any memory but only local variables and is easier to compile efficiently. Finally, there are common situations in LUSTRE of an equation of the form: \( o = \text{if } h \text{ then current } a \text{ else current } b; \) with \( a \) on clock \( h \) and \( b \) on clock \( h = \text{false} \) that is difficult to compile efficiently. It uses two memories (one for each \( \text{current} \)) that are difficult to remove and three conditionals on \( h \) (one for every \( \text{current} \) plus the one of the condition) which need to be fused. This equation is equivalent to: \( o = \text{merge}(h; a; b); \)

Finally, the \( \text{merge} \) is generalized to an \( n \)-ary form for merging several complementary sequences [19].

We now see the second change made on the data-flow core. LUSTRE does not provide a mean to modularly reset a system on a Boolean condition, that is, to re-initialize all its state

\footnote{The \textbf{let/tel} braces are optional when the body contains a single equation.}
This approach enjoys two properties: Robin Milner, “well-typed programs cannot go wrong” [23]. A program must satisfy before considering its execution. For account [22]. The static semantics gathers all the invariants that merge with extensions to take the

Figure 2 summarizes the differences between the two cores. This data-flow core is described in more detail in [21] and constitutes the basic language of SCADE 6.

IV. STATIC SEMANTICS

The dynamic semantics of SCADE 6 is that of Lustre with extensions to take the merge and modular reset into account [22]. The static semantics gathers all the invariants that a program must satisfy before considering its execution. For SCADE 6 we express them as typing problems so that, quoting Robin Milner, “well-typed programs cannot go wrong” [23]. This approach enjoys two properties:

- A type system is modular in the sense that a function type gathers all the information needed to check the correct use of this function.
- It allows for giving good error diagnostics, as far as the type language is simple enough.

Four dedicated type systems exist in the SCADE 6 compiler that are summarized below. They are applied in sequence: when one fail, the compilation stops. The type systems are presented following the order they are applied in KCG.

A. Types

The first (and pretty standard) static verification step is the type checking. Its main features are:

- All types must be declared; a type can be an enumerated set of values, a record, an array parameterized by a size, or an abstract type.
- Type equivalence is based on structural equality;
- The language provides a number of built-in type classes, like numeric and integer. E.g., int8, int16, int32, etc. are elements of the class integer.
- Types can be polymorphic and possibly constrained by the type class numeric, float, integer, signed, unsigned.
- Functions may be parameterized by a size. Such a parameter can be used in an array type.

Figure 3 illustrates several of these features. It defines a few operators working on matrices and vector whose sizes are given as parameters and whose coefficients are of a numeric type. The function root makes use of the generic matrix product for particular type and sizes.

The type system is formalized in the KCG project documentation. It is a simplified form of the type classes used in Haskell [24]. In particular, type classes are built-in and cannot be defined by the user. Moreover, the language is first-order (it is not possible to write a function which takes or returns a function). A type expression may also contain a size expression (e.g., float64 37 defines the type of matrices of size 7 x 3 of doubles). A size must be a compile-time static expression. To avoid having to incorporate a decision procedure — is size expression x + y equal to y + x? — type checking is performed in two steps: the first step does regular type checking but generates a set of equality constraints between size expressions. In a second step, one static expansion has been performed, it checks that equality constraints are trivial.

Finally, Types must incorporate an information that is specific to SCADE 6. Combinatorial functions (whose current outputs only depend on current inputs) are given the kind function whereas a statefull function (whose outputs may also depend on the past) are given the kind node. Kinds are checked during typing simply: if a function is declared with kind k, all the function it calls must also be of kind k.

The compiler imposes a strong typing discipline, that is, programs which do not type check are rejected. This allows stating the following property.

Property 1 (Well typed program execution): A well typed program is such that:

- arguments of functions have the expected type;
- array accesses are within array bounds.

B. Clock checking

The purpose of this analysis is to ensure that programs can be executed synchronously. Once done, every expression is clocked with respect to the global time scale, named the base clock. Precisely, the clock of a stream is an expression of the following language: $ck ::= ck \oplus e | \alpha$ where $e$ is a Boolean expression of the core language and $\alpha$ a clock variable. For example, an expression with clock $(\alpha \oplus e_1) \oplus e_2$ is present if an only if $e_2$ is present with clock $e_1$ and true. An expression with clock variable $\alpha$ is present iff $\alpha$ evaluates to true. The clock checking existed since the early days of Lustre [25]. In [18], it was shown to be a typing problem, precisely a typing problem with dependent types [26]. SCADE 6 adopts this point-of-view but takes a simpler formulation where equivalence between Boolean expressions is replaced by name equivalence [27]. It adds an extra simplification to this proposal by imposing that the clock of variables is declared and a function to use a single clock variable $(\alpha)$ whereas the original proposal, implemented in Lucid Synchrone V3, did not impose those two restrictions.

Given a function definition, the compiler checks clocks and computes a clock signature. The signature for the function hold (Section III) is: $\forall \alpha. \alpha \times (h : \alpha) \times \alpha \circ h \rightarrow \alpha$. It states
that, for any clock \( \alpha \), the first input of \text{hold} must have clock \( \alpha \), the second, named \( h \), clock \( \alpha \), the third, clock \( \alpha \) on \( h \). Then, the output has clock \( \alpha \).

Property 2 (Synchronous execution): A well clocked SCADE 6 model can execute synchronously.

A corollary is that a SCADE 6 model can be implemented in bounded memory, provided that imported functions do.

C. Causality analysis

The purpose of this analysis is to ensure that a set of processes running synchronously produces one and at most one output at every reaction. LUSTRE follows a simple approach, reducing it to the analysis of instantaneous loops in the data-dependences relation between variables. A more expressive constructive causality was proposed for ESTEREL [28].

Following a preliminary work [29], the causality analysis for SCADE 6 has been specified as a type system. The intuition is to associate a time stamp to every variable and to check that the relation between those time stamps is a partial order (thus, with no cycle). We illustrate it on the following two integration functions:

```plaintext
node fwd_Euler <<K, T>> (IC : 't ; u : 't) returns (y : 't) where 't numeric
  y = IC -> pre (y + K * T * u);
node bwd_Euler <<K, T>> (IC : 't ; u : 't) returns (y : 't) where 't numeric
  y = IC -> pre y + K * T * u;
```

The causality type of \text{fwd} _\text{Euler} is \( \forall \gamma_1, \gamma_2. \gamma_1 \times \gamma_2 \rightarrow \gamma_1 \) which indicates that the output only depends instantaneously of its first input. From this signature, one can see that this operator is able to break a dependency cycle on its second input. \text{bwd} _\text{Euler} has type \( \forall \gamma. \gamma \times \gamma \rightarrow \gamma \) that expresses the dependency of the output on both inputs. This is enough information to deduce that this integration function cannot be used to break a cycle.

Property 3 (Schedulability): A causal SCADE 6 model can compiled into a statically scheduled sequential code.

D. Initialization analysis

The purpose of this analysis is to ensure that the behaviour of a system does not depend on the unspecified value \text{nil}. A simple type-based analysis with sub-typing is described in [30]. For every expression, it computes its type with the following intuition:

- The type \( 1 \) is that of a stream which may have an uninitialized value \text{nil} at the very first instant;
- the type \( 0 \) is that of a stream which is always initialized.

It induces the natural sub-typing relation \( 0 \leq 1 \), meaning that an expression which is always initialized can be given to an expression that is expected to have type \( 1 \). E.g., the uninitialized rising edge operator:

```plaintext
node rising_edge (a : bool) returns (o : bool)
  o = a and not pre a;
```

gets the initialization type signature: \( 0 \rightarrow 1 \) and the following function:

```plaintext
node min_max(x, y : int32) returns (mi, ma : int32)
  mi, ma = if x < y then (x, y) else (y, x);
```

gets the signature: \( \forall \delta. \delta \times \delta \rightarrow \delta \times \delta \).

The initialization analysis does not force all functions to return well initialized streams. Hence, the following function (with signature \( 0 \times 0 \rightarrow 1 \)) which is accepted as a node declaration is not accepted if this node is the main node.

```plaintext
node root_bad (a, b : bool) returns (o : bool)
  o = rising_edge (a) or rising_edge (b);
```

whereas the following (with signature \( 0 \times 0 \rightarrow 0 \)) is accepted.

```plaintext
node root_good (a, b : bool) returns (o : bool)
  o = false -> (rising_edge (a) or rising_edge (b));
```

The main node defined what is finally executed on the target platform. Its outputs, in particular, must always be of type \( 0 \).

Property 4 (Determinism): A well initialized SCADE 6 model is deterministic in the sense that it never produces an output that depends on an undefined value (\text{nil}).

This analysis is defined for a synchronous data-flow language in [30]. It is applied to the full SCADE 6 language.

V. CONTROL-STRUCTURES

In LUSTRE, clocks are the only way for controlling the execution of a computation: an expression is computed only when its clock is true. Unfortunately, their use in LUSTRE is not easy, partly because of a lack of expressiveness of the clock language and automation (particularly clock polymorphism and inference).

Clocks exist in SCADE 6 but the language proposes an alternative by mean of dedicated control-structures. These are essentially syntactic sugar in the sense that they are translated into well-clocked equations of the data-flow core. This approach appeared extremely useful to ensure that all language extensions were consistent with each other. We were also convinced that the data-flow core was expressive enough to support this translation. The PhD work of Hamon [13] was pioneering in this direction.

In [14], Maraninchi and Rémont introduce the language of \text{node-automata} that mixes a subset of LUSTRE with ARGOS-like hierarchical automata. A compilation into guarded equations was proposed but with a source language which was less expressive than SCADE 6 and not done via a source-to-source transformation.

The following sections present and illustrate the new constructs. Their formalization and compilation are given in [19].

A. Activation blocks

The activation block is the simplest way of expressing that some equations are only active according to a boolean condition. The example below is a function that computes the complex solution of a second degree polynomial. This is a typical example where case analysis is needed. Depending on the sign of the discriminant, one of three solutions is selected.

```plaintext
function imported sqrt (x:float64) returns (y:float64);
function second_degree(a, b, c: float64)
  returns (x1, x2, y1, y2: float64)
var delta : float64;
```
The square root function is declared as imported (it is not a built-in primitive of SCADE 6). A local variable \( d \) is introduced to name the result. \( d \) only exists when \( \text{delta} > 0 \), as if \( d \) was ‘clocked’ by writing an equation \( d = \sqrt{\text{delta}} \) when \( (\text{delta} > 0) \). Indeed, the translation of the function \textit{second\_degree} precisely does that: it introduces such a clocked equation for every defined variable.

**B. Scope and shared variables**

The previous example illustrates the situation where a shared variable is defined by different equations and a single one is active at a time. Only the active equations are executed. In particular, an expression \texttt{pre} \((e)\) activated when a condition \( c \) is true denotes the previous ‘observed’ value of \( e \), that is, the value that \( e \) had, the last time \( c \) was true. This is illustrated on the function \textit{move1} with an execution trace given below:

```plaintext
let
    \textit{delta} = b*b - 4 * a*c;
    \textit{activate}
    \textit{if} \( \text{delta} > 0 \)
    \textit{then}
        \textit{var} \( d : \text{float64} \);
        \textit{let}
            \( d = \sqrt{\text{delta}} \);
            \( \text{xr}, \text{xi} = ((-\text{b} + \text{d}) / (2 * \text{a}), 0) ; \)
            \( \text{yr}, \text{yi} = ((-\text{b} - \text{d}) / (2 * \text{a}), 0) ; \)
        \textit{tel}
    \textit{else if} \( \text{delta} = 0 \)
    \textit{then}
        \textit{let}
            \( \text{xr}, \text{xi} = (-\text{b} / (2 * \text{a}), 0) ; \)
            \( \text{yr}, \text{yi} = (\text{xr}, \text{xi}) ; \)
    \textit{tel}
    \textit{else} \text{--} \( \text{delta} < 0 \)
    \textit{let}
        \( \text{xr}, \text{xi} = (-\text{b} / (2 * \text{a}), \sqrt{(-\text{delta})} / (2 * \text{a})) ; \)
        \( \text{yr}, \text{yi} = (\text{xr}, -\text{xi}) ; \)
    \textit{tel}

\textit{returns} \( \text{xr}, \text{yr}, \text{xi}, \text{yi} ; \)
\textit{tel}
```

In the proposal for \textit{mode automata} [14], the operator \texttt{pre} applied on a shared variable \( x \) behaves like \texttt{last} \( 'x \), which does not correspond to the \texttt{pre} of LUSTRE.

**C. Hierarchical Automata**

State machines are a convenient way to specify sequential behaviour with the two classical forms:

- Moore machines, when the current output is a function of the current state only;
- Mealy machines, when the current output is a function of both the current state and current input.

In [31], Harel introduced Statecharts, an extension of state machines to express complex systems in a modular and hierarchical way. ARGOS [15], SyncChart [9] and ESTEREL integrate this expressiveness within a synchronous framework with static conditions to ensure the existence and uniqueness of a reaction in every state. SyncChart [9] was the graphical notation used in the industrial tool-set based on ESTEREL.

SCADE 6 incorporates hierarchy a la SyncChart but where states may themselves contain other state machines and/or data-flow equations. A difference with the approach of ESTEREL/SyncChart is the existence of a textual support for automata. In general, a graphical representation of state machines is preferred, but proposing a textual support maintains the language and the graphical notation in a simple one to one correspondence and all the transformation work is concentrated at the compiler level. The main features of SCADE 6 hierarchical state machines are borrowed from the SyncChart:

- An automaton must have one \textit{initial} state;
- some states can be marked to be \textit{final};
- a transition can be \textit{weak} or \textit{strong};
- a transition may either reset or resume its target state;
- a \textit{synchronization} mechanism allows for firing a transition when all the automata inside the state are in a final state.

1) \textit{Intuitive Semantics:} The semantics has been formalized in [32] and through a translation into the data-flow core [19]. SCADE 6 imposes an extra constraint: \textit{at most one transition is fired per cycle}.

A cycle consists of deciding, from the current \textit{selected} state what is the \textit{active} state; execute the corresponding set of equations; then determine what is the \textit{selected} state for the next cycle. Precisely:

- At first cycle, the \textit{selected} state is the state marked initial.
- Evaluate all the guards of the \textit{selected} state strong transitions. The \textit{active} state is the target of the first (taken sequentially) firable strong transition if any, otherwise it is the \textit{selected} state.
- Execute the equations of the \textit{active} state.
- Evaluate all the guards of the \textit{active} state weak transitions. The next \textit{selected} state is the target of the first (taken sequentially) firable weak transition if any, otherwise it is the current \textit{active} state.

2) \textit{Two simple examples:} The example below shows a node that returns an integer output \( o \) with last value initialized to 0. It is defined by a two states automaton. \( \text{up} \) is the initial state.

```plaintext
\text{node move1 (c : bool) returns (o : int32)}
\text{activate if} \( c \) \text{then} \( o = (0 \rightarrow \text{pre} o) + 1; \)
\text{else} \( o = (0 \rightarrow \text{pre} o) - 1; \) \text{returns} \( o; \)

\text{node move2 (c : bool) returns (o : int32 \text{last} = 0)}
\text{activate if} \( c \) \text{then} \( o = \text{last} \rightarrow o + 1; \)
\text{else} \( o = \text{last} \rightarrow o - 1; \) \text{returns} \( o; \)

\begin{array}{cccccccc}
\text{o} & \text{true} & \text{true} & \text{false} & \text{false} & \text{true} & \text{false} & \ldots \\
\text{move1(c)} & 1 & 2 & -1 & -2 & 3 & -3 & \ldots \\
\text{move2(c)} & 1 & -1 & 0 & 1 & 0 & \ldots \\
\end{array}
```
In this mode, \( o \) is incremented by 2 until \( o \geq 12 \). Then, the next state is Down. In this state, \( o \) is decremented until it reaches value 0 and the next state is Up, etc.

```java
node up_down() returns (o : int32 last = 0)
automaton
  initial state Up
  o = last 'o + 2;
  until if o >= 12 resume Down;

state Down
  o = last 'o - 1;
  until if o = 0 resume Up;
returns o;
```

Because the transitions are weak, the guards can involve the current value of \( o \). Hence, replacing the weak transition \( (\text{until}) \) by a strong transition \( (\text{unless}) \) would lead to a causality error.

The second example is a two inputs node: tic and toc.

```java
node tic_toc_tic (tic, toc : bool) returns (o : int32 last = 0)
automaton
  initial state WaitTic
  unless if tic restart CountTocs;

state CountTocs
  unless if tic resume WaitTic;
  o = 0 -> if toc then (last 'o + 1) else last 'o;
returns o;
```

The initial state WaitTic waits for an occurrence of tic then immediately goes to the state CountTocs. This state is entered by restart which reinitializes all of its state variables (in particular the initialization \( \rightarrow \)) and thus \( o \). Because WaitTic does not provide a definition for \( o \), its last value must be declared. The value of \( o \) stay unchanged in the initial state.

3) A complete example: The last example is a simple version of the digital watch written in ESTEREL [33] limited to watch and stopwatch mode. It has four input buttons:

- `stst`: start/stop button
- `rst`: reset button
- `set`: set time button
- `md`: mode selection button

and it displays the following information:

- `HH, MM, SS`: time information
- `L`: lap time indicator
- `S`: setting time mode active indicator
- `Sh`: setting hour mode (minutes otherwise)

Basically, three automata run in parallel. Two are simple counters, one for the time (automaton Stopwatch) and the other for the stop watch (automaton Watch). There is also a process that manages the display and the Lap time (automaton Display). The watch has two modes, one where it counts time; the other where the current time is set. This program is supposed to be executed periodically with a base clock of 10ms. When a variable is declared, it can be given a last value and/or a default value (e.g., \( \text{var isStart : bool default = false} \)). The default value is the definition of the variable in the sub-scopes that omit its definition. If no default value is specified, the implicit definition for a variable \( x \) is \( x = \text{last '}x; \) participates to the imperative flavor of these constructs.

```java
node watch (stst, rst, set, md : bool)
returns (HH, MM, SS : int8;
  L, S, Sh : bool default = false last = false)
var
  isStart : bool default = false; -- is chrono started?
  is_w : bool default = false; -- is in clock mode?
  m, s, d : int8 last = 0; -- chrono timers
  wh, wm, ws, int8;
  -- clock timers
let
  w = 0 - (pre w + 1) mod 100;
  ws = 0 - (if w < pre w
     then pre ws + 1 else pre ws) mod 60;
automaton Stopwatch
  initial state Stop
  unless if stst and not is_w resume Start;
  if rst and not (false -> pre l)
    and not is_w restart Stop;
  m, s, d = (0, 0, 0) -> (last 'm, last 's, last 'd);

state Start
  unless if stst and not is_w resume Stop;
  let
    d = (last 'd + 1) mod 100;
    s = (if d < last 'd
      then last 's + 1 else last 's) mod 60;
    m = if s < last 's
      then last 'm + 1 else last 'm;
    isStart = true;
  tel
returns m, s, d, isStart;

automaton Watch
  initial state Count
  let
    wm = 0 - (if ws < last 'ws
      then last 'wm + 1 else last 'wm) mod 60;
    wh = 0 - (if wm < last 'wm
      then last 'wh + 1 else last 'wh) mod 24;
  tel
  until if set and is_w restart Set;

state Set
let
  S = true;
  automaton SetWatch
  initial state SetHours
  let
    Sh = true;
    wh = (if stst then last 'wh + 1
      else if rst then last 'wh + 23
      else last 'wh) mod 24;
  tel
  until if set and is_w restart SetMinutes;

state SetMinutes
  let
    wm = (if stst then last 'wm + 1
      else if rst then last 'wm + 59
      else last 'wm) mod 60;
  until if set and is_w restart SetEnd;

final state SetEnd
returns Sh, wh, wm;

tel
  until synchro resume Count;
returns S, Sh, wh, wm;

automaton Display
  initial state DisplayWatch
  unless if md and not S resume DisplayStopwatch;
  HH, MM, SS, is_w = (wh, wm, ws, true);

state DisplayStopwatch
  unless if md and not S resume DisplayWatch;
  var lm, ls, ld : int8 last = 0; -- chronos display
  let
    HH, MM, SS = (lm, ls, ld);

automaton LapManagement
  initial state Stopwatch
  lm, ls, ld = (m, s, d);
```
The function \( \text{exists} \) which, given a static parameter \( n \) and a boolean array \( b \) of length \( n \), returns true if and only if one element is true.

\[
\text{function exists <<n>>(b : bool^n) returns (o : bool) o = (fold \text{Sor}5 <<n>>)(false, b);
\]

\( \text{Sor}5 \) is the operation or used in prefix notation. The function \( \text{exists} \) is combinatorial; hence, it can be declared with the keyword \( \text{function} \). The semantics is that of the full unfolding; yet, the compiler generates a for loop.

### A. A combinatorial example

Figure 3 gives a more complete example, with the scalar product of two vectors, the vector matrix product and the matrix product. All these functions are polymorphic and apply to any numerical type with vectors and arrays whose sizes are specified as a static input. Function \( \text{root} \) shows an instance of the matrix product for specific sizes and with type float64. The function \( \text{MatVectProd} \) uses a special primitive \( \text{transpose} \) that allows to permute two dimensions of an array of arrays.

### B. A statefull example

The following example is inspired by the interface present in a fighter plane, where, because of acceleration, the pilot may not be precise in selecting the right push button. To overcome this risk, command selection is done in two steps: a pre-selection that works as radio buttons (selecting one button un-selects the other) and a second step done with a single button (no choice, thus no possible selection error) to confirm the pre-selection. The logic to manage this interface is quite regular and independent on the number of buttons. We give an implementation in SCADE 6 where a state machine specifies the behaviour of one button and a parameterized number \( n \) that are composed in parallel.

Buttons have a background and a foreground color depending on their state. When a button is pre-selected, its background is yellow. When locked, the background of the pre-selected buttons becomes green. The node \( \text{Button} \) defines all these behaviours; its inputs are the position of the considered button, the lock command, the unlock command and a Boolean indicating if another button is pushed to implement the radio button behaviour.

```plaintext
function prod_sum (acc_in, ui, vi: 'T) returns (acc_out: 'T) where 'T numeric
acc_out = acc_in + ui * vi;
-- scalar product of two vectors: u . v
function ScalProd <<n>> (u, v: 'T^n) returns (w: 'T^n) where 'T numeric
w = (fold prod_sum <<n>>)(0, u, v);
-- product of a matrix by a vector: A(m,n) * u(n)
function MatVectProd <<m, n>> (A: 'Tˆmˆn; u: 'T^n) returns (w: 'T^n) where 'T numeric
w = (map (ScalProd <<n>>) <<m>>)(transpose (A; 1; 2), u^m);
-- matrix product: A(m,n) * B(n,p)
function MatProd <<m, n, p>> (A: 'Tˆmˆn; B: 'Tˆnˆp) returns (C: 'Tˆmˆp) where 'T numeric
C = (map (MatVectProd <<m, n>> <<p>>)(A*p, B);
function root (A: float64^3^7; B: float64^7^5)
returns (C: float64^3^5)
C = MatProd <<<3, 7, 5>>>(A, B);
```

Fig. 3. Example: matrix operations
A. Compiler Organization

The organization of the compiler (KCG) is rather classical. Static analysis are applied in sequence right after parsing. If they all succeed, code generation starts with a sequence of source-to-source transformations that rewrite all the constructs into the data-flow core. This core is extended with array iterators. Then, the data-flow core is translated into an intermediate sequential language. At last, target imperative code (mainly C and ADA) is emitted. Figure 4 summaries these steps at a coarse grain; corresponding bibliographic references are given on the arrows.

Among the transformation, many optimisations are done on the data-flow form (dead-code elimination, constant propagation, common sub-expression, iterator compositions, etc). The scheduling in the data-flow compilation implements heuristics to limit memory size. Control structures are merged in the sequential representation.

B. Qualified Development

Qualification is based on traceability between a specification and the implementation. The specification details the principles presented in this paper. The source and intermediate languages have been formally specified together with the static semantics (defined by inference rules) and source-to-source transformations (defined by rewrite rules). Those specifications are used by the development team to implement the compiler and by an independent verification team to test it.

For the implementation, we choose OCAML [34] which was quite a challenge for a qualified tool, in 2005. Indeed, certification standards often push companies to use well established technologies. We thus had to convince that OCAML was well adapted to write a compiler. The argumentation was built on the small distance between the formal specification and their implementation in OCAML. This industrial use of OCAML in a certified context is detailed in [35] and [36].

The current version of SCADE KCG is approximately fifty thousands lines of code (50 KLOC) and it uses a simplified OCAML runtime to satisfy the objectives of the standards. The formalized static semantics for the whole input language is about one hundred pages long and has been updated for more than ten years to integrate new language features. The detailed design is more than one thousand pages long.

C. Towards a Computer Aided Formal Qualification

The formalization made for SCADE 6 was an important step to get a qualified code generator. Yet, this formalization was done by hand and some important parts were not considered. The draft [22] was a first proof of correctness for the data-flow core down to sequential code. Extending it for the full language and with high confidence in the proof correctness without the help of a computer appeared out of reach.

Proof assistants like Coq [37] allow for writing both programs, properties and computer checked proofs. The CompCert C compiler [38], [39] is the first compiler that is developed this way. Its industrial application and qualification is now considered seriously but making a formal process match industrial certification standards is a new challenge that does not reduce to a scientific question.

The next step for SCADE 6 and KCG is now to go further by using computer aided tools to get a proof of correctness of the compiler. Then connecting this new object with the CompCert C compiler would lead to a mathematically proven translation from a high-level synchronous language to assembly code. A first step have been achieved recently for the data-flow core without the reset [40]. The prototype compiler is called VELUS. When compilation succeeds, the generated assembly is proved to be semantically equivalent to the data-flow program.

VIII. Conclusion

This paper has shown principal language features of SCADE 6 together with the main design choices for its compilation. It relates a long and fruitful collaboration between industry and academia and is a concrete example of transfer of state-of-the-art research work on computer language design and implementation.

If the core of the language remained on the same size as LUSTRE, the new rich features it proposes are a big improvement for the SCADE designers. The proposed mix of fine grain data-flow and hierarchical automata mix is quite unique. The language is now as convenient to develop the logic of a cockpit display than it is to develop a discrete control law.

SCADE and KCG have been used in about hundred DO-178B/C level A avionic systems all over the world, a quite significant result in this market.

And the story continues. The language offers a good coverage of discrete-time system programming, adding continuous time modeling capabilities could be an axis of development for the near future. Following the same collaboration framework, the work on ZÉLUS [41], [42] is opening the way.
ACKNOWLEDGMENT
This work owes a lot to Paul Caspi; and Gérard Berry for our living discussions. We also want to thank all the colleagues of the Core team for their hard work on SCADE 6 KCG and our CTO, Bernard Dion, for his confidence and support.

REFERENCES