Traceability and Evidence of Correctness of EDSL Abstractions

Martin Sulzmann
Hochschule Karlsruhe - Technik und Wirtschaft
martin.sulzmann@hs-karlsruhe.de

Jürgen Nicklisch-Franken
ICS AG
juergen.nicklisch@ics-ag.de

Axel Zechner
ICS AG
axel.zechner@ics-ag.de

Abstract

One of the main advantages of an EDSL (embedded domain-specific language) is that new abstractions can be coded quickly and easily in the EDSL's host language and are automatically transformed to the basic EDSL primitives. In the context of formal software certification, it is paramount that evidence for the correctness of these abstractions is provided and that the low-level code resulting from the EDSL primitives can be traced to some higher-level artifacts, i.e. some concrete programming abstractions, software requirements etc. We have built an EDSL-based tool-chain for implementing and testing mission critical applications which supports measures to guarantee traceability and provides evidence of correctness of EDSL abstractions. We give an overview of our EDSL approach and practical experiences applying them in the industrial context.

1. Introduction

The application domain of our EDSLs are mission critical embedded control and simulation software for reactive systems. The functionality of these systems increasingly relies on software which must meet high safety standards to guarantee their correct functioning. To ensure predictable performance and memory consumption, such systems are often implemented by following the synchronous execution paradigm. That is, given some input values the application shall produce some output values in every cycle. The cycle time is fixed, so that it needs to work within some predictable amount of time.

The EDSLs we describe here have emerged out of a software project in the Aerospace& Defense area. In the following, we have a quick run through the various aspects of our EDSLs.

EDSL Technology

Our design decision was to use a rule-based language, in essence guarded actions, where in each cycle every rule is tried sequentially. If the guard of a rule is satisfied the rule’s action will be executed.

The rule-based language, referred to as Rules EDSL, is embedded in Haskell. We chose Haskell because of familiarity with the language and Haskell’s well-known ability to be a good host for embedded languages.

The architecture and compilation of the basic Rules EDSL to simple if-then statements in C is straightforward. We apply a deep embedding where running the program generates an abstract syntax tree (AST) which can then be processed further in several ways (i.e. generate code, generate documentation, check for correctness). We use singleton types together with phantom types to reflect the AST at the level of types. Technically, we follow [1] and represent constructors of our EDSL via values (type class methods). The meaning of programs is then specified by defining the appropriate type class instances. Thus, we obtain a strongly typed EDSL language.

EDSL Abstractions

The Rules EDSL offers additional type-safety compared to C but programming in the bare Rules EDSL is still very low level. So far we have built various abstractions using Haskell as our macro language. For standard signal processing we provide operations like detection of rising and falling edges, basic counter operations, temporal primitives such as a duration, primitive delays for switch-on and switch-off operations etc.

We also offer various kinds of state machines to better capture the semantics of the problem domain. The state machine abstractions range from simple cases to timed-state-machines, hierarchical state-machines and state machines with parallel branches.

Traceability

For us, the EDSL and its abstraction are only a means to an end. Ultimately, we are only interested in the resulting C code. In our largest industrial application, we find about 2000 primitive rules. Of course, by looking at the resulting C code we hardly can recognize the structure which is present at the higher EDSL level. However, in the context of mission-critical applications which are typically regulated by safety standards, every single line of code needs to be justified and traced back to some higher-level artifact.

The approach pursued by commercial tools such as SCAD is to have a qualified code generator [3]. The upshot of this approach is that the final C code doesn’t need to be inspected anymore. It suffices to inspect the software models out of which the C code is generated. For us this is not a viable option. Firstly, formal software qualification [6] is very costly. Secondly, our language model, that is the EDSL abstractions, can change rapidly depending on the problem domain. But this then would require re-qualification.

Our approach is to attach meta data to each rule which explains why this rule was generated. For example, nodeMachine transitions are translated to rules which maintain the link to the original construct.

Testing and Verification

To ensure the correctness of EDSL abstractions we make use of an expressive test and verification system which we have integrated into our framework. At its core we find a Test EDSL which consists of a temporal property language to specify the expected outcome of a test and another language to set the inputs of the (synchronous) system under test. Both languages share the sensor signal language with the Rule EDSL. Our interest is mainly in run-time verification (i.e. testing) where we execute the system under test by fixing the set of inputs over a certain number of cycles. We obtain a trace log which consists of the input/output values at each cycle. We then perform an off-line analysis of the trace log by matching the trace log against a test property specified as a linear temporal logic (LTL) formula [5].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright © ACM [to be supplied] . . . $5.00.

Related Work

As already mentioned, the EDSL technology we employ is now fairly standard [1]. Our rule-based language is inspired by the Atom DSL [2]. A noteworthy extension is our support for a user-configurable sensor signal type language.

Thus, we verify the essential building blocks, i.e. the EDSL abstractions. Besides providing strong guarantees about the correctness of the EDSL abstractions, this has the additional benefit that the test properties serve as concise specification of the EDSL abstractions.

But who verifies the verifier, in our case the run-time verification system? Our take on this issue is as follows. The test framework creates detailed reports which allows us to follow each step of the run-time verification system. Technically, we apply a constructive finite trace LTL matching algorithm which provides evidence in form of a proof why a match exists. In doubt, the proof can then be manually inspected. We also collect coverage info to provide feedback if further test cases are required. The formal details are described in [7].

Besides run-time verification we also support model-checking by verifying the C code generated out of the EDSL against the LTL specifications. We make use here of a feature of the SPIN model checker to integrate native C code. For details, we refer to [8].

EDSL Toolchain Overview and Paper Outline

Figure 1 summarizes our EDSL toolchain. Section 2 explains our EDSL with a simple example. Sections 3 and 4 demonstrate traceability and testing. Section 5 reports practical experiences and lessons we have learned.

An extended version of this paper with further details (e.g. on testing which we only briefly mention here due to space constraints), the complete set of EDSLs, as well as an example from the Automotive area are freely available via http://www.home.hs-karlsruhe.de/~suma0002/REDSL.html

Related Work

As already mentioned, the EDSL technology we employ is now fairly standard [1]. Our rule-based language is inspired by the Atom DSL [2]. A noteworthy extension is our support for a user-configurable sensor signal type language.

The most interesting aspect of an EDSL is the kind of new abstractions one invents for specific problem domains. As far as we know, the issue of traceability and correctness of EDSL abstractions has so far been largely overlooked. For example, the focus of the work in [4] is on ensuring correctness of the basic EDSL constructs in durationGtEq condIn limitIn = node "durationGtEq" $ do

\[\text{cond} <\gets \text{inVar} \ "\text{cond}\" \text{condIn}\]

\[\text{res} <\gets \text{outVar} \ "\text{res}\" \ (\text{undefined} :: \text{Bool})\]

\[\text{counter} <\gets \text{stateVar} \ "\text{counter}\" \ (\text{constE} \ (\text{1}::\text{Int}))\]

\[\text{mode} <\gets \text{localVar} \ "\text{mode}\" \ (\text{undefined} :: \text{DurationState})\]

\[\text{mode} \ .\mathbin{=\mathbin{=}\mathbin{>}}\]

\[\text{modeMachine} \ "\text{durGtEq}\" \text{Idle}\]

\[\begin{cases} (\text{Idle} \ .\mathbin{=}\mathbin{<}\mathbin{>}. \text{InProgress}) \hfill & (\text{cond} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE True}) \\ (\text{InProgress} \ .\mathbin{=}\mathbin{<}\mathbin{>}. \text{DurationGtEq}) \\ (\text{(cond} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE True}) \\ (\text{limit} \ .\mathbin{<\mathbin{=}\mathbin{=}\mathbin{>}\mathbin{>}\mathbin{>}\mathbin{>}\mathbin{>} \text{constE False}) \\ (\text{DurationGtEq} \ .\mathbin{=}\mathbin{<}\mathbin{>}. \text{Idle}) \hfill & (\text{cond} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE False}) \end{cases}\]

\[\begin{cases} \text{ifEq} \ & (\text{res} <\gets \text{=}\mathbin{=}\mathbin{>} \ (\text{(valueVar} \ \text{mode} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE InProgress}) \ .\mathbin{=\mathbin{=}\mathbin{>}}} \\ (\text{inc} \ \text{counter}) \\ (\text{elseIf}) \ & (\text{(valueVar} \ \text{mode} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE DurationGtEq}) \\ .\mathbin{=\mathbin{>};} \\ (\text{valueState} \ \text{counter}) \\ (\text{defaultCase}) \\ \text{one} \end{cases}\]

\[\begin{cases} \text{ifEq} \ & (\text{res} <\gets \text{=}\mathbin{=}\mathbin{>} \ (\text{(valueVar} \ \text{mode} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE Idle}) \\ (\text{cond} \ .\mathbin{=\mathbin{=}\mathbin{>}\mathbin{=}}. \text{constE False}) \\ (\text{defaultCase}) \\ (\text{constE True}) \end{cases}\]

\[\text{return res}\]

Thus, we verify the essential building blocks, i.e. the EDSL abstractions. Besides providing strong guarantees about the correctness of the EDSL abstractions, this has the additional benefit that the test properties serve as concise specification of the EDSL abstractions.

Figure 1. EDSL Toolchain Overview

2. EDSL Example

Figure 2 defines a temporal abstraction durationGtEq to check if the monitored Boolean value condIn (e.g. some door switch) is True for longer than the amount of cycles defined with limitIn. In this case the Boolean output res gets True. The process can start again when the input value becomes False, in which case the output becomes False too.

Function durationGtEq is a Haskell function and therefore we map the Haskell function parameters to some EDSL variables. EDSL primitive node introduces a new scope within the EDSL. This primitive is not strictly necessary but allows us to connect the variables and rules in its scope to the new abstractions, e.g. durationGtEq, we have built.

The modeMachine is a simple state machine. The three modes Idle, InProgress and DurationGtEq tell us if the monitored Boolean value has been true for longer than a certain amount cycles or not. Via EDSL primitive valueState we access the values of EDSL variables, via constE we turn Haskell constants into EDSL constants and via ifEq we represent switch-case statements. For example, the counter is incremented if we are in mode InProgress.

In fact, constructs ifEq and modeMachine are themselves abstractions. That is, we use Haskell as our macro language to express these constructs in terms of more primitive EDSL constructs. As pointed out in [4], one rarely uses the primitive EDSL language.
... from to \( \text{cond} \rightarrow \) (from, to, cond) modeMachine name init transitions = do
let mmPath x = appendPath (initPath $ modeMachine name) (initPath x)
mode <= outVar "mode"
            (mmPath OutVar)
machineState <= stateVar "machineState"
            (mmPath StateVar)
            (constE init)
trigger <= localVar "trigger"
            ((mmPath LocalVar)
            (undefined :: Bool)
simpEq (mmPath InitTrigger) $
trigger :=:= constE False
mapM_ \((\text{from}, \text{to}, \text{cond}) \rightarrow \text{do}\)
n <= freshName
rule meta\((\text{trace} = \text{Just} $ \text{mmPath Transition})\) $ do
  conditions $ 
  (valueVar trigger .==. constE False)
  .&&. (valueState machineState .==. constE from)
  .&&. cond
  machineState :=== constE to
  trigger :=:= constE True
) transitions
simpEq (mmPath SetMode) $
mode <= (valueState machineState)
return mode

Figure 3. Modemachine and Traceability

Instead, arbitrarily complex abstractions are built but ultimately the same simple code (in our case guarded actions) is generated.

However, in the context of formal software certification w.r.t. safety standards such as DO-178B and IEC 61508 it is required to provide “evidence” for every single line of source generated.

3. Traceability

Our goal is to maintain precise links (traces) between abstractions specified in the macro language and the code generated by the primitive EDSL. As a running example, we consider the modeMachine abstraction whose encoding in terms of the primitive EDSL is given in Figure 3. We first review the principles behind the encoding of modeMachine and then consider the issue of traceability.

We define a variable machineState represents the current mode we are in. Each mode transition translates into a primitive rule. A transition fires if none of the earlier transition has fired (see trigger). We are in the proper machineState and the conditions cond are satisfied. Then, we execute the transition by adjusting the machineState and remembering firing of a transition via trigger.

The primitive simpEq (a rule with an always true condition) the trigger is reset and the current machineState is assigned to the output mode.

Traceability here means that we can precisely identify which rule represents a transition, a simple equation etc. In a first step, we define a data type MMKind in Figure 4 to represent the various elements of a modeMachine. In essence, MMKind represents the explicit AST of a modeMachine.

Primitive constructs rule, simpEq, outVar, stateVar and localVar will be annotated with additional meta data to provide links to the AST elements which they shall represent. For example, consider an excerpt of Figure 3:

\[
\text{trigger} \leftarrow \text{localVar} \ "\text{trigger}" \\
\text{simpEq} \ (\text{mmPath InitTrigger}) $ \\
\]

... from to \( \text{cond} \rightarrow \) (from, to, cond) modeMachine name init transitions = do
let mmPath x = appendPath (initPath $ modeMachine name) (initPath x)
mode <= outVar "mode"
            (mmPath OutVar)
machineState <= stateVar "machineState"
            (mmPath StateVar)
            (constE init)
trigger <= localVar "trigger"
            ((mmPath LocalVar)
            (undefined :: Bool)

Figure 4. Metadata

trigger :=:= constE False

The first part declares that trigger is the modeMachine's local variable. The second part declares that the purpose of the simple equation is to reset the trigger variable to the initial false value. Meta data information is maintained during translation to low-level C code. The thus annotated EDSL code fragment translates to

```
// Trace: Node_durationGtEq::ModeMachine_durGtEq::LocalVar
bool s_LOCAL_GENtrigger7;
...

// Rule: simpEq$
// Trace: Node_durationGtEq::ModeMachine_durGtEq::InitTrigger
if(( 1 == 1 )) {
  bool __1;
  __1 = false;
  s_LOCAL_GENtrigger7 = __1;
}
```

From the trace information in the generated code we can derive that s_LOCAL_GENtrigger7 is the triggering variable of the modeMachine with name durationGtEq. The modeMachine itself is part of a bigger node abstraction with name durationGtEq.

As we can see, arbitrary abstractions can be built on top of each other. This requires us to maintain the precise trace/path through all the various abstractions which we have built. Hence, when adding the meta information that trigger represents LocalVar we possibly extend an already existing trace/path. Technically, we use the Path data type in Figure 4 to keep track of the various EDSL abstractions. To record elements of different (AST) types along a trace/path, constructor Prefix is given an existential type.

For the example in Figure 3 we generate overall 20 rules and 10 variables. Thanks to the trace information each rule and variable can be easily connected to the higher-level abstraction which gave rise to the variable/rule.

Of course, it is up the designer of the EDSL abstractions to provide the proper ‘semantic links’ between the abstractions and the EDSL primitives. If desired we can completely omit any meta data information. For example, in Figure 2 we only declare stateVar "counter" (constE (1::Int)) without providing further details. If omitted we only attach basic information about the surrounding scope to the EDSL variables declared, e.g.

```
// Trace: Node_durationGtEq
int s_STATE_GENcounter3;
```

4. Testing

A test consists of a part to execute the system under test (SUT) by setting the input variables at designated cycles. Our SUT here is the program from Figure 2 where we assume that the limit parameter is a constant. Here’s a simple test input specified in the Emit EDSL where we repeatedly set the Boolean input condition to true for limit+1 cycles.

```
input "alwaysTrue" $
```
Running the above inputs against the SUT results in a trace log. We analyze this trace log via a LTL-style property EDSL. Here are two sample properties.

**property "DurationReached" $**

always $ (valueIn in1 .==. constE True) $ .|=||=>. limit $ (valueOut out1 .==. constE True)

The above property makes use of some LTL pattern/abstraction where the pattern $A =||=>. n B$ denotes that if $A$ holds $n$ steps then the $n$th step $B$ must hold. Thus, we can specify concisely that the $duration\text{GtEq}$ shall yield true if for limit or more cycles the input condition is true.

The next set of properties state that the output shall be false if the input is set to true for less than limit cycles.

map (\i->
    property ("DurationNot"++show i) $ always $ (valueIn in1 .==. constE False) $ .|=||=>. i $ (valueOut out1 .==. constE False))

A test suite consists of a set of inputs and LTL properties. We first run all inputs against the SUT which results in a set of trace logs. Then, we match each trace log against each LTL property. Our constructive LTL matching algorithm provides us information about which parts of the formula have been matched and if there have been any failures.

5. Practical Experiences and Lessons Learned

**Industrial Projects** Our approach has so far been applied in two commercial projects and one case study. In the first commercial project we built a central control application in the Defense area which is connected to about ten subsidiary devices. This is a major application consisting of about 700 input/output sensor variables and compiles down to about 2000 primitive rules out of which we generate about 30,000 lines of C code (this includes some code instrumentation for coverage and logging). The second commercial project lies in the Transportation area. The EDSLs are applied to simulate external components of a central train control system. The simulations are used to perform a hardware-in-the loop test of the train system.

In both cases, the application/simulations went through a couple of major refactoring steps due to unknown or changing customer requirements. We wouldn’t have met the deadline without the flexibility of the EDSL approach and the possibility of implementing new abstractions/extensions quickly while guaranteeing their correctness.

The case study is an Automotive application and is freely available with the EDSL source code distribution.

**EDSL Toolchain Evolution** The EDSLs and its toolchain have evolved in various directions mainly due to customer requests. For example, for the Defense project, the customer demanded to import the test suite to DOORS, a popular commercial requirement engineering tool. Therefore, we had to customize the meta data information and turned LTL patterns into semi-formal English sentences. The result is an automatic import into DOORS where tests are immediately linked to high-level requirements as specified in the meta data.

In the Transportation project, our first target system was .Net/C# which then later was changed to a real-time operating system(RTOS)/C system. For us, it was pretty straightforward to compile our primitive guarded actions to either C# or C. The higher-level simulation part remained unchanged.

**User Experience** Overall six Software/System Engineers have worked with the EDSLs and its toolchain so far. The Haskell syntax took some time to getting used to. However, once the proper EDSL abstractions are in place it was possible to write the code even for experts without Haskell knowledge.

For example, in the case of the Transportation project, portions of the simulations have been coded by a domain expert which had no prior exposure to Haskell and EDSLs before.

A well-known issue is the lack of reasonable customized error messages which our approach shares with other EDSLs. In our EDSLs we make heavy use of type classes to configure for example the signal type language and overload the various EDSL constructs. This results in long and hard to read types. We are in the process of simplifying parts of our EDSLs which then yields more comprehensible types.

**Comparison to Commercial Tools** Industrial-strength tools such as Simulink or SCADe offer a GUI interface and offer visual editors to facilitate the communication with domain experts. Our toolchain is currently operated from the command line and it can be hard to sell to customers.

Yet we see EDSLs as a secret weapon in case of software projects which require great flexibility (e.g. rapidly changing customer requirements etc). Thanks to the nature of EDSLs, new project specific abstractions can be coded quickly and easily. Moreover, we provide an expressive test system which is fully integrated into our EDSLs.

For the success of EDSLs in this domain we can make the user experience more convenient by integrating it into a GUI and by providing connectors to established commercial tools. For example, we are currently working on automatic transformations from our EDSLs to SCADe’s textual language. Thus, we can take advantage of the flexibility of the EDSL approach and at the same time we are able to integrate our approach into existing tool-chains.

**Acknowledgments** We thank the reviewers for their comments.

**References**


A. Traceability Example

In Figure 5, we show the generated code for parts of our running example.

A.1 Test Report Example

The following description relies on color information

As a part of our EDSL toolchain we have built a 'TestRunner' tool to automate test execution. The tool generates a HTML report which contains extensive information about number of input runs, LTL properties, accumulated coverage and specific coverage when matching pairs of inputs and LTL properties. Figure 6 shows a sample test report summary. Via hyper-links the user can inspect the details.

For example, Figure 7 displays the accumulated coverage result of property "DurationReached". We find here the 'primitive' AST representation of the LTL property where all abstractions have been unrolled.

In detail, at the Haskell level we unroll property "DurationReached" $
\text{always } \left( \begin{array}{c} 
\text{valueIn in1 == True} \\
\text{limit} \\
\text{valueOut out1 == True} 
\end{array} \right) 
$ into

property "DurationReached" $\text{always } \left( \begin{array}{c} 
\text{valueIn in1 == True} \\
\text{limit} \\
\text{valueOut out1 == True} 
\end{array} \right) 
$ where we assume that limit equals 3.

We still need one more step to reach the most elementary form. The expression

$x .==>. 1 \ \&\& \ (x .-->. 1 \ \&\& \ y)$
That is, either \( x \) doesn't hold or if \( x \) holds in the next step \( y \) holds.

At this level, we perform the constructive LTL matching and display the matching results.

For our example, all parts are 'black' which shows that the inputs have exercised all atomic parts of the LTL formula. This information provides some indication if the LTL properties are covered sufficiently by inputs.

Figure 8 shows the matching of the above input "alwaysTrue" against property "DurationReached". In each step, the input condition is true. For brevity, we only show the matching starting with the fourth step. The result of matching an input (i.e. the trace implied) against a LTL formula is represented by displaying the parse tree. The color 'green' highlights the matched parts whereas color 'blue' indicates that at this point the trace ended prematurely and a full parse tree couldn’t be build. The color 'red' highlights a violation which is not the case here.

We are in the process of improving the display of test results by mapping results at the most basic level to the EDSL abstraction level.

---

**Figure 8.** Input against LTL match

```plaintext
Seq: [Step 4]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{GOT\_GENout}(true) = \text{true}\]

Seq: [Step 5]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{IN\_GENin} = \text{true}\]
   \[\text{GOT\_GENout} = \text{true}\]

Seq: [Step 6]
   \[\text{IN\_GENin}(true) = \text{true}\]
   \[\text{IN\_GENin} = \text{true}\]
   \[\text{GOT\_GENout} = \text{true}\]
   \[\text{CHOICE}\]
   \[\text{Not: IN\_GENin} = \text{true}\]
   \[\text{IN\_GENin} = \text{true}\]
   \[\text{GOT\_GENout} = \text{true}\]
```