Circus Models for Safety-Critical Java Programs

Frank Zeyda, Lalkhumsanga Lalkhumsanga, Ana Cavalcanti and Andy Wellings

Department of Computer Science, University of York, Deramore Lane, York, YO10 5GH, UK
Email: frank.zeyda@york.ac.uk, ana.cavalcanti@york.ac.uk, andy.wellings@york.ac.uk

Safety-Critical Java (SCJ) is a restriction of the Real-Time Specification for Java to support the development and certification of safety-critical applications. The SCJ technology specification is the result of an international effort from industry and academia. In this paper, we present a formalisation of the SCJ Level 1 execution model, formalise a translation strategy from SCJ into a refinement notation, and describe a tool that largely automates the generation of the formal models. Our modelling language is part of the Circus family; at the core, we have Z, CSP, and Morgan’s calculus, but we also use object-oriented and timed constructs from the OhCircus and Circus Time variants. Our work is an essential ingredient for the development of refinement-based reasoning techniques for SCJ.

Keywords: Circus; real-time systems; formal models; translation; refinement; RTSJ

1. INTRODUCTION

Java is currently one of the most popular programming languages. Its use in the software industry is extensive. Java, however, has not been widely adopted for development of high-integrity systems, in general, and safety-critical systems, in particular. Concerns about common programming mistakes mean that safer subsets of languages like Ada and C are normally the favoured option. Java, in its full generality, is far too rich a language, and inadequate for time-critical applications due to its heap model based on garbage collection and problems related to prioritisation of threads [1, 2].

As Java implementation technology has matured, the efficiency of the generated code has improved, and new real-time garbage collection algorithms have been developed. As a consequence, some industries have been using Java for their mission-critical applications. Financial trading systems, where real-time performance is critical and applications must be of high-integrity, are, for instance, discussed in [3].

Vendors that support these real-time Java implementations (Atego’s Pere Pico product is an example [4]) point out the advantages of using a subset of Java along with highly efficient virtual machines for hard real-time and safety-critical applications. In addition, the supplement DO-332 [5] of the recently released DO-178C certification guidance [6] for the production of airborne software has included more details on how object-oriented programming and virtual machine techniques should be used. This has provided extra encouragement for those interested in using Java in this domain [7, 8].

Most of the proposed approaches to using Java in safety-critical systems build upon real-time extensions of Java. Initially, real-time extensions to Java were ad hoc, until the US National Institute of Standards and Technologies brought the communities together to define the requirements for a common standard [9]. As a result, the Real-Time Specification for Java (RTSJ) [10] emerged. This is a version of Java that includes the notion of real-time threads and adopts a region-based memory model [11]. RTSJ has been supported by academia and industry [12, 13, 14], including Oracle (Sun) [15] and IBM [16].

RTSJ, however, is still a very rich language, that encompasses the whole of Java, and includes additional concepts and constructs. This imposes severe challenges in the context of applications that require certification, for instance. As a result, an expert group has been formed to design SCJ, a Java-based language tailored for programming certifiable safety-critical systems.

Safety-Critical Java (SCJ) [17] restricts the Java API, program execution, and memory model in such a way that programs can be effectively analysed for real-time requirements, memory safety, and concurrency issues. This facilitates certification and development of tools that support analysis and verification. SCJ reuses some of RTSJ’s concepts and actual API components, but restricts the programming interface. The SCJ technology specification [2] comprises informal descriptions and a reference implementation. Analysis tools have also been developed to establish compliance with the restrictions imposed by SCJ [18].

In recognition of the fact that safety-critical software varies considerably in complexity, there are three compliance levels for SCJ programs and VM
implementations. In this work, we are concerned with Level 1, which, roughly, corresponds in complexity to the Ravenscar profile for Ada [19]. Level 1 applications support periodic as well as aperiodic event handlers.

The informal account of SCJ [2] relies on text and UML diagrams, and there currently exists no formal account of a semantics for SCJ. The purpose of our work is firstly to define a semantics for SCJ in a language that can be used for refinement (Circus). Secondly, we support the automatic generation of formal models of SCJ programs to enable practical use of the semantics for analysis and refinement-based verification. In defining a formal semantics, we clarify subtle aspects of the SCJ programming paradigm, including, for instance, handler interaction and termination. Our formalisation, in particular, targets the mission-based execution model of SCJ.

Circus [20, 21] is a process algebra that integrates well established notations, namely Z [22], CSP [23], and Morgan’s refinement calculus [24], to support the development of state-rich reactive systems. Significantly, in Circus we can take advantage of mathematical proof to verify concurrent systems that are too large for model checking. Circus is currently being used to verify software in aerospace applications, including software for the Chinese manned lunar lander, and novel virtualisation software by the US Naval Research Laboratory. Circus has a formal semantics [25], and a refinement theory and strategy [21]. A specialised Circus-based refinement technique permits the analysis of control systems specified in Simulink [26, 27].

The semantics of Circus is based on the Unifying Theories of Programming (UTP) [28]. The UTP supports well the combination of notations like Z and CSP, and also allows us to consider constructs from other paradigms. Extensions and variants of Circus cover, for instance, aspects of time and mobility. We use its object-oriented variant, OhCircus [29], as our base notation. OhCircus can be used to model both data objects and the active behaviour of the SCJ components. The UTP-based semantics of OhCircus enables us to combine OhCircus with Circus Time, a version of Circus with support for timed behaviours.

Our work firstly elicits the conceptual behaviour of the SCJ framework, and secondly formalises how the translation of actual SCJ programs into their OhCircus specifications can be achieved in a traceable manner. We ignore certain aspects of SCJ, such as the memory model, which we discuss in a separate paper [30], and scheduling policy. Our focus is the top-level design and execution of SCJ programs, and SCJ’s primary framework and application components.

In our view, the SCJ framework as designed in Java embeds a general programming paradigm. SCJ adopts a particular approach to data operations, memory management, and event-based versus thread-based program designs [31]. The fact that it can be realised on top of Java and the RTSJ is a bonus. It is conceivable to implement specific support based on other mainstream languages, or even define an entirely new language. Our model identifies the fundamental concepts of SCJ at a level at which it can be itself regarded as a language.

Regarding imperative constructs, there are a number of features of the Java language that reduce clarity or are otherwise challenging to describe and analyse formally. An additional contribution of our work is to identify and exclude such constructs, which are often similar to those prohibited by subsets of C and Ada [32] used in the safety industry. We note that the design of SCJ [2] does not address constraints on statements. Although we do not claim here to identify all constructs (the ones that have simple models in Circus we admit), our work can nevertheless be seen as a first step in defining a safe subset for SCJ.

We formalise the translation from safety-critical Java into Circus using a collection of compositional translation rules. To automate the translation process, we present an annotation framework and a tool that can generate models for arbitrary SCJ programs that satisfy our restrictions and are suitably annotated.

Our work shows that Circus is adequate for capturing faithfully the semantics of SCJ programs respecting our restrictions, and that the construction of Circus models can be automated. This is provided the program code has been annotated, which requires human interaction. No in-depth knowledge of Circus is required to drive the model generation process and the models we produce can act as the targets for a refinement strategy whose application provides opportunities for automation, too.

We have validated our Circus models in FDR [33]....

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{Life-cycle of a safelet during execution of a Level 1 application}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig2.png}
\caption{A simplified view of the Circuit model}
\end{figure}
after translating them into CSP. In doing so, we managed to show livelock and deadlock freedom of simple applications. We also used the CZT parser and type-checker [34] to ensure that the Circus specifications generated by our tool are valid, and the tool itself validates the feasibility of our automatic approach. Recent work [35, 36] reports on a refinement strategy that transforms abstract, centralised Circus specifications that are structured in terms of behavioural and timing requirements into concrete models that adhere precisely to the structure of models presented here.

In summary, what we describe in this paper is first a precise semantics for core elements of SCJ. This enables formal verification of SCJ applications beyond the informal validation of statically-checkable properties currently available [18]. OhCircus provides a notion for refinement, and our work is an essential step to justify future development and verification methods that can produce high-quality SCJ implementations. For verification, we can construct models of particular programs, and use the Circus and UTP techniques for reasoning. For development, we can start from an abstract specification, and develop implementations that respect the restrictions of our models [36]. The latter approach can also be used for verification of a given program with respect to a specification. For that, we need to guide the refinement strategy to produce a Circus model that is syntactically equivalent to the model of the SCJ program, as it is generated by our technique and tool. Preliminary results are reported in [35], and we note that this approach is more flexible than mere code generation as it enables the verification of arbitrary programs, and, in particular, supports hand-coded optimisations.

In comparison to our previous work [37], here we elaborate and make precise our modelling approach and formalise its construction. We also modularise and, in several places, simplify the framework model, which captures the generic behaviour of the SCJ paradigm.

The structure of the article is as follows. Section 2 discusses preliminary material: SCJ, a cruise controller, which is used as a running example, and the Circus family of languages. The next three sections discuss in detail the Circus model of SCJ: Section 3 explains the top-level architecture; Section 4 presents the fixed framework model; and Section 5 presents the program-specific application model. In Section 6 we present a formalised translation strategy from SCJ into Circus, and Section 7 examines issues related to automation and tool support. Lastly, in Section 8 we conclude and address related and future work.

2. PRELIMINARIES

Here, we give an overview of the SCJ execution model and introduce an example: an automotive cruise controller. Afterwards, we present Circus and OhCircus, the formal notations in which our models are written.

2.1. Safety-Critical Java

The SCJ programming paradigm is based on the notion of missions. They are sequentially executed by an application-defined mission sequencer provided by a safelet, the top-level entity of an SCJ application. The life-cycle of a safelet is illustrated in Fig. 1. Conceptual
entities are realised by either interfaces or abstract classes. Namely, they are the Safelet interface, and the abstract classes MissionSequencer and Mission (see Fig. 2 for a UML diagram).

As already mentioned, in this work, we consider only SCJ Level 1 applications. A Level 1 mission executes in parallel a set of asynchronous event handlers (both periodic and aperiodic handlers are supported). Each aperiodic handler is associated with a set of events: firing one of them causes a handler method to be scheduled for execution. Periodic event handlers, on the other hand, are controlled by a timer. Event handlers are defined by extending abstract classes whose handling method must be implemented by a concrete subclass. These classes are, in particular, PeriodicEventHandler, AperiodicEventHandler and AperiodicLongEventHandler (see Fig. 2).

2.2. A cruise control system

As an example of an SCJ Level 1 program, and to illustrate our modelling approach, we present an implementation of the automotive cruise control system (ACC) in [10]. The example was first published as a case study in [38]. It therefore does not reflect the current state-of-the-art in automotive technology, but is nevertheless sufficient for illustrating our method.

The purpose of an ACC is to maintain the speed of a vehicle to a value set by the driver. In Fig. 3 we give an overview of its main components and commands. Explicit commands are given by a lever whose positioning corresponds to the following instructions: activate, to turn on the ACC if the car is in top gear, and maintain (and remember) the current speed; deactivate, to turn off the ACC; start_accelerating, to accelerate at a comfortable rate; stop_accelerating, to stop accelerating and maintain (and remember) the current speed; and resume to return to the last remembered speed and maintain it. When the driver operates the brake pedal, changes gear, or switches off the engine, the ACC is deactivated. Besides, when the engine is switched on, the ACC is initialised in such a way that the resume command cannot be issued as no speed is initially recorded.

The speed of the vehicle is measured via the rotations of a shaft that is connected to one of the wheels. The speed of the car is controlled by the ACC using the throttle position, which is determined by the depression of the accelerator pedal and a voltage supplied by the ACC. The combination of these values is performed by a mechanism outside the ACC.

Sensors detect external events and generate appropriate interrupts, as shown in the diagram in Fig. 3. Their service routines in the SCJ program determine the precise interrupting event and fire a corresponding SCJ event that releases one of the aperiodic handlers. For the setting of the throttle voltage, communication of the new voltage value to the throttle actuator is realised in the program using a hardware data register.

Fig. 2 presents a UML class diagram that gives an overview of the design of the ACC as an SCJ Level 1 safelet. In Fig. 1 we also highlight the sequence of method calls that are carried out by the SCJ run-time environment (virtual machine) to execute a safelet. We next discuss the entities of the ACC individually.
We note that in the ACC there is only one mission. These instances determine the mission sequentially executed by the safelet. As part of the termination process, the release of the handler is realised by an interaction mechanism that is implemented at the level of interrupt service routines (ISRs). The mechanism queries the particular sensor that caused the interrupt and releases the corresponding handler while passing the corresponding event identifier.

Beyond the ACC example. Fig. 2 does not show all components of the SCJ API. There are eight classes that realise the mission framework, twelve classes in the handler hierarchy, five classes that deal with real-time threads, seven classes concerned with scheduling, and ten classes for the memory model. The formal model that we present here abstracts from all these details of the realisation of the SCJ Level 1 programming paradigm in Java. We capture the main concepts of this novel execution model. This enables reasoning based on the core components of the SCJ paradigm.

The memory model of SCJ employs the region-based approach of RTSJ. Since SCJ does not support garbage collection, a restricted version of scoped memory is permitted, but not heap memory. Scoped memory has a limited life-span that is controlled by the SCJ run-time environment. Memory scopes form a tree, and restrictions on references between scopes effectively alleviate the problem of dangling references.

At the root of the tree we have immortal memory. It contains objects that are never deallocated during the execution of the safelet. Below, mission memory is created and exists for the duration of executing a mission, and is used to store objects that are shared between handlers. Further below, each handler executes in its own per release memory area whose life-time is limited to the execution of the handler’s handleAsyncEvent() method. Additionally, handlers may create their own private memory areas as needed.

Before considering the formalisation of SCJ programs, we present our modelling notation next.

2.3. The Circus family of languages

Like in CSP, the key elements of Circus models are processes that interact with each other and their environment via communication channels. Unlike CSP, Circus processes may encapsulate a state. This renders Circus useful for both model-based and behavioural specification [39]. In what follows, we introduce standard Circus and its derivatives OhCircus and Circus Time. We recall that our modelling notation is indeed a combination of these three languages.

```
public void initialize() {
  /* Create SCJ events and interrupt handlers. */
  createEvents();
  createISRs();
  registerISRs();
  /* Create event handlers and shared data. */
  WheelShaft shaft = new WheelShaft(shaft_event);
  Controller cruise = new Controller(throttle, speedo);
  Lever lever = new Lever(cruise, lever_event);
  Engine engine = new Engine(cruise, engine_event);
  /* Register event handlers with the mission. */
  shaft.register();
  cruise.register();
  engine.register();
  /* ... */
}
```


Safelet. ACCSafelet is the entry point for the SCJ application. This class provides the method getMissionSequencer() that returns the application’s mission sequencer. The other two methods setUp() and tearDown() are provided for initialisation and cleanup tasks.

Mission Sequencer. The ACCMissionSequencer class constructs instances of the Mission class by implementing getNextMission(). These instances determine the missions sequentially executed by the safelet. We note that in the ACC there is only one mission.

Missions. Concrete subclasses of Mission have to implement the initialize() and missionMemorySize() methods. The former creates and registers the periodic and aperiodic event handlers of the mission. Fig. 4 includes the definition of the initialize() method in the ACC implementation. We first have calls to methods that create SCJ events and interrupt service routines (ISRs). The SCJ events are held by instance variables of the class and we omit a detailed discussion of the ISRs. The subsequent statements create the application code for mission-specific cleanup tasks.

The two extra methods requestTermination() and terminationPending() of the mission class are provided for initialisation and cleanup tasks.

Handlers. Periodic event handlers implement the method handleAsyncEvent(), and aperiodic event handlers implement either handleAsyncEvent() or handleAsyncLongEvent(int) to specify their behaviour when the handler is released, depending on whether the handler class is derived from AperiodicEventHandler or AperiodicLongEventHandler. The difference between the latter two is that AperiodicLongEventHandler supports the passing of a long parameter to the handler method, whereas in AperiodicEventHandler the handler method is parameterless.

In the ACC, we use AperiodicLongEventHandler for all aperiodic handlers, except only for WheelShaft, and use the parameter to identify the external event that caused the release of the handler. Based on its value, the handler method selects a method to call on the shared Controller object. The passing of the value identifying the event to the handler is realised by an interaction mechanism that is implemented at the level of interrupt service routines (ISRs). The mechanism queries the particular sensor that caused the interrupt and releases the corresponding handler while passing the corresponding event identifier.
process $ProcName \triangleq p : T \bullet \text{begin}$

\begin{align*}
\text{state } & \text{State} \\
& c_1 : T_1 \\
& c_2 : T_2 \\
& \ldots \\
\text{Init} & \triangleq \\
& P_{\text{Init}}(\epsilon'_1, \epsilon'_2, \ldots) \\
\text{Op}_1 & \triangleq \\
& \Delta \text{State} \\
& P_1(c_1, c_2, \epsilon'_1, \epsilon'_2, \ldots) \\
\text{Op}_2 & \triangleq \\
& \Delta \text{State} \\
& P_2(c_1, c_2, \epsilon'_1, \epsilon'_2, \ldots) \\
\text{Act}_1 & \triangleq \ldots \\
\text{Act}_2 & \triangleq \ldots \\
\bullet & \text{MainAct}(\text{Init}, \text{Op}_1, \text{Op}_2, \text{Act}_1, \text{Act}_2, \ldots) \\
\text{end}
\end{align*}

class $ClassName \mid \text{extends BaseName} \triangleq \text{begin}$

\begin{align*}
\text{state } & \text{State} \\
\text{private } & c_1 : T_1 \\
\text{private } & c_2 : T_2 \\
& \ldots \\
\text{initial } & \text{Init} \\
& \text{State} \prime \\
& C_{\text{Init}}(\epsilon'_1, \epsilon'_2, \ldots) \\
\text{logical } & \text{Meth}_1 \\
& \Delta \text{State} \\
& M_1(c_1, c_2, \epsilon'_1, \epsilon'_2, \ldots) \\
\text{logical } & \text{Meth}_2 \\
& \Delta \text{State} \\
& M_2(c_1, c_2, \epsilon'_1, \epsilon'_2, \ldots) \\
\text{public } & \text{Meth}_3 \triangleq \ldots \\
\text{private } & \text{Meth}_4 \triangleq \ldots \\
\text{end}
\end{align*}

FIGURE 5. Typical examples of a $Circus$ process (left) and an $OhCircus$ class (right).

2.3.1. $Circus$

The typical syntax of a $Circus$ process is sketched in the left diagram of Fig. 5. The name of the process is $ProcName$ and $p$ is a parameter of type $T$ (in a parameterless process, $p$ is absent). The process state is determined by the $Z$ schema in the state paragraph. This schema is called State here and has the components $c_1$, $c_2$, and so on, of types $T_1$, $T_2$, and so on. Because the state is local to the process, it is only visible by the local schema operations and actions. Here, they are $Init$, $Op_1$, $Op_2$, $Act_1$, $Act_2$, and so on, as well as the main action $MainAct$ at the end after the $\bullet$.

A process usually contains an initialisation action ($Init$ above). It is typically specified by a $Z$ operation schema whose predicate constrains the values of dashed variables only. Dashed names, as common in $Z$, are used to refer to the value of variables after execution of some operation. Dashing a schema, as in the declaration $State \prime$ in $Init$, renames the components of that schema to their dashed counterparts.

Actions can be defined using $Z$ data operation schemas, constructs from CSP, as well as commands from Morgan’s calculus to modify the state. Data operations typically change the state, and their specification constrains the values of the state components $c_1$, $c_2$, and so on, and of the corresponding variables $\epsilon'_1$, $\epsilon'_2$, and so on. The former refer to the values of the state components before the operation, and the latter, as mentioned above, represent the values of the state components after the operation. All these variables are implicitly declared by $\Delta \text{State}$. We note that data operations are always atomic in $Circus$.

The main action ($MainAct$ in Fig. 5) defines the behaviour of the process. It may reference local actions, which are introduced primarily for structuring purposes. Similarly, local actions may reference other local actions in their bodies, too.

The language of actions provides a rich set of constructs. Table 1 includes all action constructs inherited from CSP that are relevant for the models in this article. As a notational convention, $A$ stands for an action, $c$ for a channel, $x$ for a variable, $T$ for a type, $cs$ for a set of channels, $ns$ for a set of variables, and $E$ for an expression yielding a value. We provide a brief explanation of each action operator in the sequel, but postpone a more detailed discussion to where the operators are first used in our models.

We first have the $\text{skip}$ action, which terminates immediately without changing the state. Next, the action $\text{abort}$ is the bottom of the refinement lattice for actions and thus represents (program) failure. Prefixes are used for communication with the environment or other processes. They can take the form of simple synchronisations ($c \rightarrow A$), inputs ($c ? x \rightarrow A(x)$), or outputs ($c! E \rightarrow A$).

Actions may be combined in various ways. External choice ($A_1 \sqcup A_2$) is a choice that is resolved by the environment. This means that the first interaction determines which of the two actions is chosen, and the communications offered are the ones offered by either $A_1$ or $A_2$. If the same communication is offered by both actions, the choice becomes nondeterministic. Sequential composition ($A_1 ; A_2$) has its usual meaning.

Parallelism ($A_1 \parallel ns_1 \mid cs \mid ns_2 \parallel A_2$) executes
two actions concurrently. That is, they may progress independently but have to synchronise on the channels in the synchronisation set cs. Importantly, parallel actions must write to disjoint parts of the process state to avoid write conflicts. To achieve this, the name sets ns1 and ns2 determine the state components that each parallel action is allowed to modify. For the operator to be well formed, the name sets hence have to be disjoint. Interleaving of actions, written as A1 ||| ns1 | cs | ns2 ||| A2, is a special case of parallelism where the set of synchronisation channels is empty. We also have an iterated interleaving that interleaves all actions A(x) where x ranges over the elements of some set S.

There are two noteworthy points about Circus parallelism and interleaving. Firstly, both operators terminate only when all parallel actions have terminated. Secondly, they enforce non-interference: state changes become visible only after termination of the operator. This is important to preserve monotonicity.

An interrupt A1 \triangle c \rightarrow A2 is used to transfer control from one action A1 to another action A2 at any point during the execution of A1. This happens as a consequence of a synchronisation on the channel c. In A \setminus cs, the channels in the set cs are hidden in the execution of the action A. Synchronisations on hidden channels take place internally and as soon as they are enabled, without visibility or participation of the environment. Lastly, the recursion construct μX ⋅ F(X) names the action F(X) in its body X, and so uses of X in F(X) are recursive calls.

State operations can be specified either by Z operation schemas such as Op1 and Op2 in Fig. 5, or guarded commands. A list of all guarded commands used by our models is given Table 2. Assignments change the value of a state component or local variable. Local variables are introduced by way of a local variable block of the form var x : T ⋅ A(x), where x becomes a local variable of type T that A may refer to.

The conditional statement is in Dijkstra’s generalised form [40], taking a list of guarded commands (the qi are predicates). A binary conditional if b then A1 else A2 is hence written if b → A1 \[¬ b → A2. fi. Lastly, a value parameter p of type T can be introduced using val p : T ⋅ A(p). This is useful in order to define parametrised actions.

Processes can be defined explicitly in the form sketched in Fig. 5, or alternatively, similar to actions, by virtue of CSP operators over existing process definitions, like those presented in Table 1. The only difference in comparison to the action operators is that parallel composition and interleaving do not require name sets, since processes fully encapsulate their state.

### Table 1. Circus action constructs derived from CSP.

<table>
<thead>
<tr>
<th>Action</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip</td>
<td>skip</td>
<td>Immediately terminates without changing the state.</td>
</tr>
<tr>
<td>Diverge</td>
<td>abort</td>
<td>Divergent action: it may not terminate and represents failure.</td>
</tr>
<tr>
<td>Synchronisation</td>
<td>c ↦ A</td>
<td>Simplest form of an interaction: no value is communicated.</td>
</tr>
<tr>
<td>Input Prefix</td>
<td>c?x ↦ A(x)</td>
<td>Binds the variable x to the value read through the channel c.</td>
</tr>
<tr>
<td>Output Prefix</td>
<td>c!E ↦ A</td>
<td>Outputs the value of the expression E on the channel c.</td>
</tr>
<tr>
<td>External Choice</td>
<td>A ⊕ A2</td>
<td>A choice that is resolved by the environment.</td>
</tr>
<tr>
<td>Sequence</td>
<td>A ⊔ A2</td>
<td>Executes the two actions A1 and A2 in sequence.</td>
</tr>
<tr>
<td>Parallelism</td>
<td>A1</td>
<td></td>
</tr>
<tr>
<td>Interleaving</td>
<td>A1</td>
<td></td>
</tr>
<tr>
<td>Iterated Interleaving</td>
<td>μx : S ⋅ A(x)</td>
<td>Interleaving of all actions A(x) where x ∈ S.</td>
</tr>
<tr>
<td>Interrupt</td>
<td>A1 \triangle c ↦ A2</td>
<td>A synchronisation on c interrupts the execution of A1 and subsequently transfers control to A2.</td>
</tr>
<tr>
<td>Hiding</td>
<td>A \setminus cs</td>
<td>Interactions via channels in cs are hidden and take place immediately when they are enabled.</td>
</tr>
<tr>
<td>Recursion</td>
<td>μX ⋅ F(X)</td>
<td>Occurrences of X in F constitute recursive calls.</td>
</tr>
</tbody>
</table>
to instantiate new data objects, invoke methods, access object fields, and support inheritance. Table 3 includes all OhCircus constructs that are relevant for the material in this article. We have the new construct to create a new class object, and the this and super keywords to refer to fields and methods of the current and superclass. In summary, the notation for methods is similar to the notation for actions, but lacks the CSP operators. Besides, methods can be declared as synchronised using the modifier sync. Synchronised methods are an extension we introduce to the OhCircus language. This enables us to treat method execution as atomic, just like Z data operations.

2.3.3. Circus Time
Circus Time [41] is an extension of Circus to model timed behaviours. Subsequently, we make use of two further operators of Circus Time. They are the wait t and wait \( t_1 \ldots t_2 \) statements, also included in Table 3. The first delays execution by \( t \) time units, and the second is a nondeterministic delay that may wait between \( t_1 \) and \( t_2 \) time units. Apart from the use of Circus Time, object references from our previous SCJ memory model in [30] are also used. They are specified at the level of the Unifying Theories of Programming [28], the common semantic framework of Circus and its extensions.

In the next three sections, we present our model for SCJ programs. We have given here a brief overview of the main features of the Circus family of languages used in formulating those models. Extra details of the notation are explained as we discuss the models.

3. MODEL ARCHITECTURE
Our models factor into two dimensions: a generic framework model, and an application model that corresponds to a particular concrete SCJ program. In the framework model, we specify the semantics of the safelet, mission sequencer, missions, and event handlers. They are the fundamental building blocks of Level 1 applications. To illustrate the architecture of application models, we make use of the cruise controller example presented in the previous section.

Fig. 6 presents an overview of the structure of the complete model of a typical SCJ Level 1 application — here the cruise controller. Each box represents a Circus process and is labelled by the process name. Boxes inside the large surrounding rectangle denote a process that belongs to the framework model. These processes capture the generic behaviour of the SCJ programming paradigm. Boxes outside (highlighted in grey) denote processes that belong to the application model. These are in direct correspondence with the classes of an SCJ program. While framework processes (suffix FW) have fixed names, application processes (suffix App) carry the names of their respective Java classes. The three dots indicate that a few of the event handler framework and application processes of our case study are omitted. They integrate into the model in a similar fashion as the handler processes shown in Fig. 6.

The Circus model of the entire SCJ application is obtained by parallel composition of the framework and application models. The framework model is itself a parallel composition, namely of all framework processes. Similarly, the application model is defined by a parallelism involving all application processes.

Arrows in Fig. 6 indicate the channels on which the processes communicate (synchronise). The framework processes SafeletFW and MissionSequencerFW, for instance, synchronise on start sequencer and done sequencer. These two channels control the execution of the mission sequencer.

We distinguish between control channels and method channels; the latter are identified by the suffixes Call and Ret. To give an example, start mission is a control channel whereas requestTerminationCall and requestTerminationRet are method channels. All calls to infrastructure methods are modelled by channel

<table>
<thead>
<tr>
<th>Action</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment</td>
<td>( x := E )</td>
<td>Changes the value of a state component or local variable.</td>
</tr>
<tr>
<td>Local Variable</td>
<td>( \text{var } x : T \bullet A(x) )</td>
<td>Declaration of a local variable ( x ).</td>
</tr>
<tr>
<td>Conditional</td>
<td>if ( g_1 \rightarrow A_1 \parallel g_2 \rightarrow A_2 \parallel \ldots \parallel g_n \rightarrow A_n ) fi</td>
<td>Executes an action whose guard ( g_i ) is true.</td>
</tr>
<tr>
<td>Value Parameter</td>
<td>( \text{val } p : T \bullet A(p) )</td>
<td>Action with a value-parameter ( p ) of type ( T ).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Construct</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Object</td>
<td>this</td>
<td>References the current object.</td>
</tr>
<tr>
<td>Superclass Object</td>
<td>super</td>
<td>References the superclass object.</td>
</tr>
<tr>
<td>Selection</td>
<td>( \text{obj}.[\text{field/method}] )</td>
<td>Accesses a field or method of an object ( \text{obj} ).</td>
</tr>
<tr>
<td>Object Creation</td>
<td>( \text{new } \text{Class(args)} )</td>
<td>Creates a new object of class type ( \text{Class} ).</td>
</tr>
<tr>
<td>Synchronised Method</td>
<td>( \text{sync Meth(args)} ) = ( \ldots )</td>
<td>Declares a method ( \text{Meth} ) as atomic.</td>
</tr>
<tr>
<td>Simple Delay</td>
<td>wait ( t )</td>
<td>Waits for ( t ) time units.</td>
</tr>
<tr>
<td>Nondeterministic Delay</td>
<td>wait ( t_1 \ldots t_2 )</td>
<td>Waits between ( t_1 ) and ( t_2 ) time units.</td>
</tr>
</tbody>
</table>

TABLE 2. Circus action constructs used from Morgan’s calculus.

TABLE 3. Relevant OhCircus and Circus Time constructs.
Fig. 7 presents a more application-centred view of the Circus model. Here, the framework model is characterised by a single process Framework, which corresponds to the large enclosing box in Fig. 6. Synchronisations on method channels are, for brevity, subsumed into single arrows. Fig. 7 also illustrates some of the data objects. For the mission sequencer, the mission and each handler, we have an OhCircus class (suffix Class) that encodes an underlying data object, and a ControllerClass, which models the Controller class. All shared data objects are created by ACCMissionApp during initialisation of the mission. We omit some of the event handler classes for brevity.

At the system level, all method and control channels are hidden. The only observable interactions are the ones with the external environment. We can see in Fig. 7 that, specifically, the application processes for handlers engage in these interactions. The external channels are application-specific and define the interface of the system. For example, we declare basic channels engine_on and engine_off in the cruise controller model to represent the events that occur when the engine is switched on and off. Table A.1 in Appendix A includes all channels that are used for external events of the cruise controller. The free type LEVER is introduced to represent the five positions of the command lever. In the program, these interactions correspond to device accesses and hardware interrupts (see Fig. 3).
In what follows, we describe each of the processes of our model in more detail.

3.1. System Process

The System process models the entire application. Its uniform definition is sketched below.

\[
\text{process System } \triangleq \frac{\text{Framework}}{\text{Application}} \left( SCJ\text{MethodChan} \cup \text{AppControlChan} \right) \setminus \left( SCJ\text{MethodChan} \cup \text{AppControlChan} \right)
\]

Above, Framework and Application refer to the individual composite processes that model the framework and application classes. Two channel sets are used to define the synchronisation set of the parallelism. They are SCJMethodChan for all method channels and AppControlChan for control events used by the framework to control the application processes. Internal control channels of the framework are already hidden in the Framework process. We hide all method and application control channels so that only the channels that constitute the external interface are exposed.

To define the Application process, we first specify a process HandlersApp, which combines all handler application processes in parallel. For the ACC model, this process is defined as shown below.

\[
\text{process HandlersApp } \triangleq \\
\begin{cases}
\text{WheelShaftApp } \{\text{end\_mission\_fw}\} \\
\text{EngineApp } \{\text{end\_mission\_fw}\} \\
\text{BrakeApp } \{\text{end\_mission\_fw}\} \\
\text{GearApp } \{\text{end\_mission\_fw}\} \\
\text{LeverApp } \{\text{end\_mission\_fw}\} \\
\text{SpeedMonitorApp } \{\text{end\_mission\_fw}\} \\
\text{ThrottleControllerApp}
\end{cases}
\]

The only synchronisation required is on the channel end\_mission\_fw which, beyond other purposes discussed later on, cumulatively terminates the handler application processes when the program terminates.

With the above, the Application process is defined by way of an interleaving (operator |||) as follows.

\[
\text{process Application } \triangleq \\
\begin{cases}
\text{ACCSafeletApp} \\
\text{ACCMissionSequencerApp} \\
\text{ACCMissionApp} \\
\text{HandlersApp}
\end{cases}
\]

In defining Application for the cruise controller, we account for all grey boxes in Fig.7. The definition...
reflects the four main entities in the mission model: the safelet, mission sequencer, missions and handlers. In applications where there is more than one mission, we construct a process MissionsApp for them just like HandlersApp. The use of interleaving in the application model highlights that, although application processes individually synchronise with the framework, they do not synchronise with each other. The exception to this are handlers that are released by the same external event or handlers that release other handlers. In the cruise controller, however, there are no such handlers.

Having presented the top-level model view, in the next two sections we elaborate on the detailed specification of each framework (Section 4) and application (Section 5) process.

4. FRAMEWORK MODEL

In this section, we present the framework model for the safelet, mission sequencer, missions, and handlers. We recall that the Circus processes in this model are fixed: they are the same for every SCJ application and embody the generic behaviour of the SCJ paradigm.

4.1. Safelet

The framework process SafeletFW is given in Fig. 8. It has no state. The main action sequentially executes the SetUp, Execute and TearDown local actions. They initiate and wait for completion of the initialisation, execution and cleanup phases of the safelet. This is followed by a synchronisation on end_safelet_app to terminate the safelet application process, after which the safelet framework process itself terminates.

The actions SetUp and TearDown synchronise in sequence (prefix operator \( \rightarrow \)) on the SetUp[Call/Ret] and tearDown[Call/Ret] channels, before terminating. The synchronisations model calls to the methods SetUp() and tearDown() of the SCJ application class that implements the Safelet interface. To illustrate the calling mechanism, we recall that in the system model (Fig. 6), all framework and application processes are composed in parallel, and in that parallel composition, SafeletFW and the respective safelet application process (ACCSSafeletApp in Fig. 6) synchronise on the aforementioned method channels. Hence, we obtain a behaviour that can be described as sketched by the parallel action fragment below, though the actions are embedded in processes.

\[
\begin{align*}
\text{SetUp} & \equiv \text{setUpCall} \rightarrow \text{setUpRet} \rightarrow \text{skip} \\
\text{Execute} & \equiv \text{start_sequencer} \rightarrow \text{done_sequencer} \rightarrow \text{skip} \\
\text{TearDown} & \equiv \text{tearDownCall} \rightarrow \text{tearDownRet} \rightarrow \text{skip}
\end{align*}
\]

\[
\bullet \text{SetUp} ; \text{Execute} ; \text{TearDown} ; \text{end_safelet_app} \rightarrow \text{skip}
\]

The left action of the parallelism comes from the SetUp action of the SafeletFW process, and the right action is in the safelet application process. The parallel actions first synchronise on the channel SetUpCall, after which the right parallel action executes the action MethBody of the method body of the SetUp() method. Only then can the left action make further progress, resulting in a synchronisation on SetUpRet with the left-hand parallel action terminating.

Since the methods of the safelet are parameterless and do not return any values, the communications are synchronisations: there is no input or output. As noted, the methods themselves are specified in the application process for the safelet, which is discussed in the next section. As a convention, we use capitalised names for actions and lower-case names for channels. In cases where the names of model entities are derived directly from identifiers in the program, this does not apply.

Execute also performs synchronisations, but instead raises two framework events: start_sequencer to start the mission sequencer, and done_sequencer to wait for its termination. The framework process for the mission sequencer component is specified next.

4.2. Mission Sequencer

The mission sequencer process communicates with the safelet process to determine when it has to start, and also to signal its termination. Its specification in Circus is presented in Fig. 9. The main action executes Start, which waits for the mission sequencer to be started, as signalled by a synchronisation on start_sequencer. Afterwards, execution proceeds as specified by the recursion in the action Execute. In each iteration, we synchronise on the channels getNextMissionCall and getNextMissionRet to obtain the next mission next. This corresponds to a call to the SCJ method getNextMission() of the concrete MissionSequencer application class. Since this call returns a (mission) object, getNextMissionRet receives as an input a value
process MissionSequencerFW ≜ begin
    Start ≜ start_sequencer → skip
    Execute ≜ μX • getNextMissionCall → getNextMissionRet ? next →
        if next ≠ nullMId → start_mission . next → done_mission . next → X
        [ ] next = nullMId → skip
    fi
    Finish ≜ end_sequencer_app → end_mission_fw → done_sequencer → skip
        • Start ; Execute ; Finish
end


next of type MissionId which contains identifiers for the missions of an application. Mission identifiers are introduced for all instances of classes of an application that extend the Mission infrastructure class. They allow us to uniquely identify objects of those classes. A special mission identifier nullMId is used to model the case when the method returns a Java `null` reference to signal that there are no more missions to execute.

Again, to illustrate the modelling approach, below we extract a parallel fragment that captures the behaviour that emerges from the composition of the mission sequencer framework and application processes.

\[
\text{μX • getNextMissionCall} → \text{getNextMissionRet ? next → A} \text{cond}(next) \]
\[
[\varnothing | \{ \text{getNextMission[Call/Ret],...}] | ...] \]
\[
...; \]
\[
\text{getNextMissionCall} → \text{skip}; \]
\[
\text{getNextMissionRet ! ACCMId} → \text{skip}; ...\]

As before, the left action of the parallelism originates from the framework process, here the `Execute` action of MissionSequencerFW (whose conditional has been abbreviated by `A`cond). The right action of the parallelism is provided by the mission sequencer application process `ACCMissionSequencerApp` as part of implementing the `getNextMission()` method. Notably, in this example, we have a synchronisation between an input prefix (`getNextMissionRet ? next → ...`) and an output prefix (`getNextMissionRet ! ACCMId → ...`). It results in a value being communicated, namely of a constant `ACCMId` of type `MissionId`. The value is locally bound by the input prefix to the variable `next` and hence can be accessed by the action `A`cond.

In `Execute`, a conditional checks the value of `next`. If it is not equal to nullMId, synchronisations on `start_mission . next` and `done_mission . next` control the mission framework process MissionFW (defined below) that manages execution of the mission next, and then `Execute` recurses to handle the next mission. If `next` is equal to nullMId, `Execute` finishes. We note that semantically, there is no difference between a synchronisation `c . E → skip` and `c ! E → skip` — they both result in outputting the value of `E` on channel `c`.

In the `Finish` action at the end, first a synchronisation on `end_sequencer_app` is used to terminate the mission sequencer application process. Next, a synchronisation on `end_mission_fw` terminates the mission framework process. Finally, synchronisation on `done_sequencer` acknowledges to the safelet process that the mission sequencer has finished.

4.3. Mission

The purpose of the mission framework process, MissionFW, is to record the mission’s event handlers, execute the mission by synchronously starting these handlers, controlling their termination, and afterwards finishing the mission. Termination of a mission can be initiated by a handler at any point during the mission’s execution phase, via a call to `requestTermination()`. The MissionFW framework process thus communicates with the mission sequencer process (MissionSequencerFW), the mission application processes, and the event handler processes.

Fig. 10 presents the definition of MissionFW. Its state has three components: the identifier mission of the mission being executed, if any, its finite set handlers of event handlers, and a flag terminating that records whether the current mission is in the process of termination. As previously mentioned, the handlers are identified by values of a type HandlerId. As with missions, we statically associate instances of classes that implement event handlers with unique identifiers.

The action `Init` defines that, initially, there is no mission executing, so that `mission` equals `nullMId`, and therefore, the set of handlers is empty. We also set `terminating` to `FALSE` reflecting that, to begin with, there is no termination request.

In the main action, we use again a modelling pattern where we have a sequence of actions that define the different phases of the entity life-cycle, as we already did in the safelet and mission sequencer models. In the case of the mission framework process, however, a recursion (operator `μX • F(X)`), where occurrences of `X` in `F` are recursive invocations) perpetually calls this sequence of actions, because MissionFW controls
process MissionFW ≜ begin
  state State ≜ [mission : MissionId; handlers : ∏ {HandlerId}; terminating : boolean]
  Init ≜ [State’ | mission’ = nullMId ∧ handlers’ = ∅ ∧ terminating’ = FALSE]
  Start ≜ Init ; start_mission? m → mission := m
  AddHandler ≜ val handler : HandlerId • handlers := handlers ∪ {handler}
  Initialize ≜ initializeCall . mission →
                   (µX • (request? h → AddHandler(h) ; X))
  StartHandlers ≜ || h : handlers • start_handler . h → skip
  StopHandlers ≜ || h : handlers • stop_handler . h → done_handler . h → skip
  Execute ≜ StartHandlers ; activate_handlers →
             (stop_handlers → StopHandlers ; done_handlers → skip)
             [Ø | ∪ stop_handlers, done_handlers | {terminating}]
            (Methods ∧ done_handlers → skip)
  Cleanup ≜ cleanupCall . mission → cleanupRet . mission → skip
  Finish ≜ end_mission_app . mission → done_mission . mission → skip
  requestTerminationMeth ≜
    requestTerminationCall →
    if terminating = FALSE → (terminating := TRUE ; stop_handlers → skip)
    fi ;
    requestTerminationRet → skip
  terminationPendingMeth ≜
    terminationPendingCall → terminationPendingRet ! terminating → skip
  Methods ≜ µX • (requestTerminationMeth △ terminationPendingMeth) ; X
            • (µX • Start ; Initialize ; Execute ; Cleanup ; Finish ; X) △ end_mission_fw → skip
end

FIGURE 10. Mission framework process.
of handler termination. The name set of the left parallel action is empty, since it does not modify the state, whereas the right parallel action may set the terminating flag. The mission identifier and its handlers cannot be changed at this stage of mission execution.

As part of the control behaviour, first of all, all handlers are started with a call to the action StartHandlers, which uses synchronisations start_handler. h to start, all handlers h recorded in the state in interleaving. Each process corresponding to a handler h synchronises with the mission process on start_handler. The interleaving terminates after all synchronisations are performed.

The handlers do not immediately become active after they are started, that is, they do not respond to external events immediately. This is because they have to start execution synchronously, and the action Start uses a channel activate_handlers to ensure this. All handler processes synchronise on it, but only those that previously synchronised on start_handler proceed to execute their active behaviours. In this way, handlers can be registered asynchronously, but start execution (enter their dispatch loops) synchronously.

Termination of the handlers is initiated by the requestTerminationMeth action, with a synchronisation on stop_handlers. This action is one of the choices offered by the Methods action and corresponds to the requestTermination() method. Handler application processes call this method by synchronising on requestTermination[Call/Ret]. This causes the left parallel action in Execute to call the action StopHandlers after synchronising on stop_handlers. In case of multiple calls to requestTermination(), the stop_handlers event is only raised once. For each handler h of the mission, StopHandlers uses stop_handler. h to stop the handler, and then waits for the event done_handler. h acknowledging termination of the handler. Finally, when all handler processes of the mission have acknowledged termination, the interleaving in StopHandlers terminates, and the done_handlers event is raised. This last event forces the Methods action in the parallelism to be interrupted due to the interrupt action done_handlers → skip, so that Execute altogether terminates, and the mission can proceed to the cleanup phase.

We note that the use of terminating = TRUE and terminating = FALSE instead of just terminating and ¬ terminating in the guards of the conditional is due to the fact that Z distinguishes between predicates and values. As a consequence, boolean values have to be introduced by virtue of a free type definition, such as boolean ::= TRUE | FALSE in our model.

The framework process also supports method calls to terminationPending() during the execution phase. This method can be used by a handler to check if we are currently in the process of terminating a mission. It simply returns the value of terminating.

Finally, the Cleanup action calls the action of the mission application process corresponding to its cleanup() method. Finish is then invoked to report to the mission sequencer framework process that the current mission has terminated; this is via a synchronisation on done_mission, mission.

The interrupt in the main action enables the mission sequencer to terminate the mission framework process via a synchronisation on end_mission, fw, namely when it is no longer needed. This happens during termination of the mission sequencer and, subsequently, the safelet.

4.4. Event Handlers

The framework process EventHandlerFW for an event handler is presented in Fig. 11. This process is the same

![FIGURE 11. Framework process for event handlers.](image-url)
for periodic and aperiodic handlers. EventHandlerFW is parametrised by an identifier that must be provided when the framework process is instantiated for a particular handler. For the engine handler, for example, we use EventHandlerFW(EngineHId).

The state component active of EventHandlerFW records whether the handler is active in the current mission or not. The main action defines an iterative behaviour that is interrupted and terminated by the event end_mission_fw, which, as mentioned before, indicates the end of mission execution.

Each iteration defines the behaviour of the handler during one mission. First, the state is initialised using Init, so that the handler is marked as inactive by default. Afterwards, the handler waits to be started, which is captured by the action Start. This action calls StartHandler in external choice with a synchronisation on activate_handlers, offered by ActivateHandlers. StartHandler synchronises on a particular start_handler event that is determined by the current handler identifier. Next, StartHandler also offers a synchronisation on activate_handlers (calling ActivateHandlers), which always occurs prior to entering the execution phase.

If the start_handler event of the handler occurs before activate_handlers, the value of active is TRUE. In this case, the behaviour of the handler, as defined by Execute, is to call DispatchHandler, which raises the enter_dispatch_event of the particular handler to notify the respective application process that it has to enter the dispatch loop. The dispatch loop can be interrupted after the stop_handler_event, by synchronising on leave_dispatch_event. The subsequent done_handler_event notifies the mission framework process that the handler has terminated.

If active is FALSE, Execute terminates, as in that case the handler is not part of the current mission and remains idle during its execution. The subsequent recursive call ensures that the same handler can be run by multiple missions. Just like the mission process, a handler process perpetually offers its service until there are no more missions to be executed, and the mission framework terminates it by synchronisation on end_mission_fw, typically during the course of terminating the framework and application processes.

We observe that, unlike the case of the safelet, the mission sequencer, and the mission framework processes, there is one instantiation of a handler framework process for each individual event handler of an application. The handler framework model is accordingly the parallel composition of all those process instances. For readability, we define a parametrised process HandlersFW that applies to a set of handler identifiers and yields the aforementioned composition.

\[
\text{process } \text{HandlersFW} \equiv \text{handlers} : \mathbb{F} (\text{HandlerId}) \bullet \\
\text{HandlersFW(handlers)} \\
\text{\{\{ activate_handlers, end_mission_fw \}} \bullet \\
\text{EventHandlerFW(h)}
\]

Here, we have an iterated parallelism over the handler identifiers \(h\). We recapture that this is an iteration in the mathematical, and not the Java sense. It composes in parallel the processes \(\text{EventHandlerFW}(h)\), where \(h\) ranges over the set \(\text{handlers}\) provided by the process parameter. All handlers synchronise on the channels \(\text{activate_handlers}\) and \(\text{end_mission_fw}\). The handler framework processes essentially evolve independently, jointly synchronising only on the these two channels.

### 4.5. Overall SCJ Framework

To conclude, we define a process \(\text{Framework}\) that specifies the entire framework model. It is obtained by parallel composition of all framework processes. Like the \(\text{HandlersFW}\) process, the \(\text{Framework}\) process is parametrised by the handler identifiers for a particular application. For instance, in the ACC model they are WheelShaftHId, EngineHId, GearHId, LeverHId, SpeedoHId and ThrottleHId.

The composite framework process is presented in Fig. 12. The control events that start or stop one of the SCJ components are hidden. Other framework events, like \(\text{end_mission_fw}\) are, however, exposed as we require application-level processes to synchronise on...
them. Table A.2 in Appendix A includes a summary of the channels that are associated with methods, including their parametrisation.

To illustrate the instantiation of Framework for a particular application, we define the corresponding framework process $ACCFW$ for the ACC model.

$$\text{process } ACCFW \equiv \text{Framework}(\{\text{WheelShaftHId, EngineHId, BrakeHId, GearHId, LeverHId, SpeedoHId, ThrottleHId}\})$$

Here, we assume that WheelShaftHId, EngineHId, BrakeHId, and so on, have been introduced as unique identifiers of type HandlerId. The name of each constant is derived from the handler’s class name. The constants themselves correspond to instances of a handler in a mission. For example, if we had two sensors and thus two instances of the WheelShaft class (counting the rotations of the wheel shaft), we would require two constants, WheelShaftHId1 and WheelShaftHId2, chiefly because in this case we require two separate handler framework processes.

So far, we have presented a formal model for the general SCJ programming paradigm in executing missions as realised by a compliant virtual machine. This model already provides useful insight into the exact mechanisms that underly the execution of Level 1 safelets, for instance, with regards to subtle details of the termination mechanism. Importantly, our model captures those mechanisms abstractly and independently of Java. In the next section, we discuss in detail how models for particular SCJ applications are constructed and expressed by a collection of Circus processes and OhCircus classes.

### 5. APPLICATION MODEL

Our presentation of the application model of SCJ is yet informal in this section and illustrated using the cruise controller. As before, we individually discuss the application processes for the safelet, mission sequencer, missions, and event handlers. We also discuss the model for data objects. The purpose of this section is to highlight the main principles and ideas of the modelling approach. In Section 6 we take these principles further by formalising the construction of models for arbitrary programs by virtue of a translation strategy, captured by a set of compositional translation rules.

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Classes belonging to Category</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMMC</td>
<td>active classes</td>
<td>Safelet, mission sequencer, and mission classes.</td>
<td>$Circus$ process + $OhCircus$ class</td>
</tr>
<tr>
<td>HC</td>
<td>active classes</td>
<td>Periodic and aperiodic event handler classes.</td>
<td>$Circus$ process + $OhCircus$ class</td>
</tr>
<tr>
<td>DC</td>
<td>data objects</td>
<td>Classes that model application data.</td>
<td>$OhCircus$ class</td>
</tr>
<tr>
<td>IC</td>
<td>interaction classes</td>
<td>Classes for interaction with I/O devices.</td>
<td>—</td>
</tr>
</tbody>
</table>

**TABLE 4.** Encoding of different types of Java classes in the application model.

5.1. Categories of Classes

For our modelling technique, we distinguish between four kinds of classes in an SCJ program (see Table 4). We consider

1. classes corresponding to the application’s safelet, mission sequencer or missions;
2. classes corresponding to event handlers;
3. classes corresponding to data objects; and
4. classes for device interaction and I/O.

For readability, we refer to these categories by the names SMMC, HC, DC, and IC, respectively. The first and second categories cater for classes that either implement or extend an SCJ abstract class or interface for a Level 1 entity. For example, in the ACC we have ACCSafelet, ACCMissionSequence, and ACCMission belonging to SMMC, and Engine, Brake, ThrottleController, and so on, belonging to HC. The third category comprises all other classes that do not belong to IC. Lastly, classes in IC implement interactions with external devices. They are not directly modelled and should, together with extra knowledge about the environment, justify assumptions regarding those interactions such as synchronicity, atomicity and instantaneousness. These assumptions are explained in more detail in the next section. In the ACC, we have only the Controller class in DC. Classes in IC include interrupt service routines for hardware interrupts raised by the sensors.

We label the classes in SMMC and HC as active classes, since their models have to interact directly with framework processes by way of channel communications. Such active behaviour is, for instance, responding to calls to SCJ infrastructure methods that the application classes override. Therefore, SMMC and HC classes require process models. The classes in DC have OhCircus class models, thus they do not interact through communications with an active class. Generally, modelling SCJ classes as OhCircus classes has the advantage that we can treat their instances as values. On the other hand, in cases where data objects do interact with devices or the external hardware, we propose to refactor the code in a such a way that all interactions are moved into the handler classes; this seems to be usually possible in our experience so far.
process SCJClassApp ≡ begin
state State == [this : SCJClassClass]
Init ≡ [State | this' = new SCJClassClass]
Meth1 ≡ Meth1Call → (..; Meth1Ret → skip)
Meth2 ≡ Meth2Call → (..; Meth2Ret → skip)
Meth3 ≡ ...
Methods ≡ μX • (Meth1 □ Meth2 □ ...) ; X
  • Init ; (Methods △ end_entity_app → skip)
end

FIGURE 13. Basic process model for the safelet, mission sequencer and mission application classes.

A general basic pattern for the process model of the classes in SMMC is presented in Fig. 13. The name of the process is derived from the SCJ class by appending the class name with App. The state of the process contains a single component this whose type is that of an OhCircus class. This class is in direct correspondence with the respective SCJ class. Whereas the process SCJClassApp models calls to infrastructure methods, the class SCJClassClass models the actual data object and non-infrastructure methods that do not require interaction with the framework or external devices. We can hence think of the process as ‘wrapping’ the class object. Fig. 13 describes the general wrapping pattern.

The behaviour of an application process is first to initialise the state component this with a new OhCircus data object (using the action Init) and then to offer calls to all infrastructure methods (using the action Methods), until a communication end_entity_app occurs that terminates the process. The actual name of this channel depends on the particular SCJ component. For instance, for the safelet it is end_safelet_app, and for the mission sequencer, end_sequencer_app.

If the SCJ class does not have any instance variables, the corresponding process can be simplified by removing the state paragraph and the Init action. Constructors of the SCJ class are modelled in the OhCircus class, by OhCircus constructors. For now, we assume the presence of only parameterless constructors in SMMC classes (safelet, mission sequencer, and mission classes). Handler classes (in HC), as discussed later on, have a different model and can make unconstrained use of parametrised constructors.

Specific method actions Meth1, Meth2, and so on, must be present depending on the SCJ component. Table A.2 in Appendix A indicates the methods that are required in each class. The choice offered by Methods is exercised by the associated framework process or other application processes that call those methods. We note that method calls in our model have to respect the behavioural restrictions of SCJ [2]. That is, certain methods should only be called during the initialisation or finalisation phase of the safelet or of a mission.

A method action Methi in Fig. 13 synchronises on the channel that represents a call to the method and then executes actions that correspond to the method implementation, indicated by the dots. If the method is a pure data operation, we invoke the OhCircus model of the method using a call this.Methi(args). If the method interacts through communications, we embed a model of the method as an action directly into the process. Before termination, the method action synchronises on the Methi.Ret channel to signal the return of the call. As previously noted, for methods that have parameters or return a value, the call and return channels are used to communicate these values. In that case, the shape of the corresponding Methi action is more elaborate, following the pattern illustrated below.

\[
\text{Methi} \equiv \left( \text{MethiCall} \? \text{args} \rightarrow \left( \begin{array}{c}
\text{var ret : T} \bullet \text{MBodyi(args, ret)};
\text{MethiRet}! \text{ret} \rightarrow \text{skip}
\end{array} \right) \right)
\]

Instead of a simple synchronisation, the call is modelled by an input prefix that receives the arguments args of the call. The local variable ret holds the return value and is initialised by the action MBodyi. The return value is communicated as an output through the return channel Methi.Ret, which is also parametrised.

The basic model in Fig. 13 assumes that there is only a single instance created for each class. This is the case for the safelet and mission sequencer, however the same mission class may potentially be instantiated more than once by the mission sequencer. To support multiple instances, we modify the main action of the basic application process as shown below.

\[
(\mu X \bullet \text{Init} ; \text{Methods} \& \text{end_entity_app} \rightarrow X) \\
\& \text{end_mission_fu} \rightarrow \text{skip}
\]

Here, raising the end_entity_app event causes the application process to be restarted rather than its termination because of the recursive call to X. The framework event end_mission_fu is used instead to terminate the process during safelet shutdown.

We next discuss the application model for the various infrastructure classes of the ACC in detail.
5.2. Safelet

We present the application process for the ACC safelet in Fig. 14. It is in direct correspondence with the ACCSafelet class. The specification is trivial here since setUp() and tearDown() in ACCSafelet do not contain any code (the actions are just skip). The process nevertheless illustrates the modelling approach for SCJ classes belonging to the category SMMC. The actions offered by Methods are setUpMeth and tearDownMeth. Termination occurs when the safelet framework process raises the end_safelet_app event. The process definition follows the general pattern in Fig. 13, however, simplifications have been possible as the resulting process lacks a state and an initialisation.

5.3. Mission Sequencer

The mission sequencer application process is given in Fig. 15. It more completely illustrates our approach to modelling SCJ classes as OhCircus classes and Circus processes. ACCMissionSequencerApp utilises the definition of the OhCircus class in Fig. 16. The OhCircus class is in direct correspondence with the ACCMissionSequencer SCJ class, shown in Fig. 17. The instance variables of the SCJ class become state components of the OhCircus class. Here, we have only one state component mission_done, corresponding to a variable of the same name in the SCJ class. The action Init that follows specifies the constructor behaviour.

Methods that are called by the SCJ infrastructure are defined in both, the Circus process and OhCircus class, whereas methods that are not called by the infrastructure are defined in the OhCircus class only if they are data operations. A special case are methods that interact with external devices. Those methods have mere action models, defined in the process.

The method getNextMission(), for instance, is called by the infrastructure, so it has to be specified in the application process too (Fig. 15). In the class definition of the method, we have a conditional that, depending on the value of mission_done returns the next mission whose identifier is either ACCMId or nullMId. The result parameter ret of type MissionId is introduced to hold the return value. The action model of the method synchronises on the respective Call channel to wait for a call from the framework, then invokes the method on the aggregated this class object, and finally synchronises on the Ret channel to finalise the method call and communicate its result.

In general, we model methods of SCJ classes by OhCircus methods where this is possible: methods that perform data operations become OhCircus methods, whereas methods that are called by the framework or interact with external devices become actions.
class ACCMissionSequencerClass \equiv \begin{align*}
\text{begin} \\
\text{state} \; \text{State} \equiv [\text{private} \; \text{mission} \_ \text{done} : \text{boolean}] \\
\text{initial} \, \equiv \, \text{mission} \_ \text{done} \, \equiv \, \text{false} \\
\text{public} \; \text{getNextMission} \, \equiv \, \text{res ret} : \text{MissionId} \cdot \text{if} \, \text{mission} \_ \text{done} \, \equiv \, \text{FALSE} \rightarrow \text{mission} \_ \text{done} \, \equiv \, \text{TRUE} \; \text{ret} \, \equiv \, \text{ACCMId} \\
\text{fi} \\
\end{align*}
end

FIGURE 16. OhCircus class for the mission sequencer of the cruise controller.

public class ACCMissionSequencer extends MissionSequencer {
    /* Records if the mission has already been executed. */
    private boolean mission_done;
    public ACCMissionSequencer() {
        super(...);
        mission_done = false;
    }
    public Mission getNextMission() {
        if (!mission_done) {
            mission_done = true;
            return new ACCMission();
        }
        else {
            return null;
        }
    }
}

FIGURE 17. Java class of the mission sequencer of the cruise controller.

5.4. Mission

For mission application processes, we use the modified form of the basic process model in Fig. 13 as discussed in Section 5.1. The main action of the ACCMission process accordingly has the following shape.

$$
\begin{align*}
\mu X \bullet \text{Init}; \\
\langle \text{Methods} \triangle \text{end} \_ \text{mission} \_ \text{app} \cdot \text{ACCMId} \rightarrow X \rangle \\
\triangle \text{end} \_ \text{mission} \_ \text{fw} \rightarrow \text{skip}
\end{align*}
$$

The end\_mission\_app channel is parametrised to enable the termination of particular mission application processes. Here, there is only one mission process which synchronises on end\_mission\_app \cdot ACCMId.

Java methods are encoded as before by a combination of OhCircus class methods and local actions. Notably, the encoding of initialize() is only possible as an action due to its communication with the framework when registering handlers. Thus, there is no model of this method in the underlying OhCircus class. Generally, initialize() creates objects for shared data and handlers, and registers those handlers with the framework, which subsequently executes them as part of the current mission. Below, we include an extract of its action model for the ACC implementation.

$$
\begin{align*}
\text{initializeMeth} \, \equiv \, \text{initializeCall} \cdot \text{ACCMId} \rightarrow \\
\text{var} \ldots ; \text{speedo} : \text{SpeedMonitorClass}; \\
\text{throttle} : \text{ThrottleControllerClass}; \\
\text{cruise} : \text{ControllerClass}; \\
\text{engine} : \text{EngineClass}; \ldots \cdot \\
\ldots ; \\
\text{throttle} : \text{new} \text{ThrottleControllerClass(speedo)}; \\
\text{ThrottleControllerInit} \! \text{throttle} \rightarrow \text{skip}; \\
\text{register} \cdot \text{ThrottleHId} \rightarrow \text{skip} \\
\text{cruise} : \text{new} \text{ControllerClass(throttle}, \text{speedo}); \\
\text{engine} : \text{new} \text{EngineClass(cruise)}; \\
\text{EngineInit} \! \text{engine} \rightarrow \text{skip}; \\
\text{register} \cdot \text{EngineHId} \rightarrow \text{skip} \\
\ldots ; \\
\text{initializeRet} \cdot \text{ACCMId} \rightarrow \text{skip}
\end{align*}
$$

The SCJ code of this method can be found in Fig.4. Like in the program, local variables are introduced for handler objects, such as speedo, throttle, and engine. These variables have a class type, and are initialised with newly created class objects using a
suitable constructor. Our modelling approach requires that handler objects are only created and registered inside this method. This is enforced by the behavioural restrictions of SCJ [2]. The two synchronisations on the channels ThrottleControllerInit and EngineInit link the handler processes to their underlying data objects. Specifically, the process ThrottleControllerApp synchronises on ThrottleControllerInit and the process EngineApp on EngineInit. Hence the instantiation of a handler in the program such as, for instance,

```
engine = new Engine(cruise);
```

is modelled by a sequence of two statements

```
engine := new EngineClass(cruise);
EngineInit! engine -> skip
```

where the assignment is implicitly a reference assignment to an object of (class) type EngineClass. The cruise object is an object of the class Controller that is shared between the handlers, hence it does not have a process model, nor do we require a synchronisation on a channel Init to model its creation.

The Init channels are introduced for all handler classes, but they are not needed for the safelet, mission sequencer and mission classes. This is due to the fact that for the latter classes, the link between a process and the underlying data object is static with respect to the model, whereas in case of handlers it is established dynamically during initialisation of the mission.

To record a periodic or aperiodic handler as part of the current mission, we have a communication such as register . EngineHId -> skip. In the program, this corresponds to a call to the register() method of the handler classes of the SCJ infrastructure.

The inherited methods of ACCMission, namely requestTermination() and terminationPending(), are provided by the MissionFW framework process since they cannot be overridden. The cleanup() method of ACCMission just unregisters ISRs, and hence is not discussed here.

Our modelling approach requires that there is a one-to-one relationship between instances of SCJ classes and their processes at any given time. For handlers, this assumption is justified if we consider a particular handler only to be instantiated once per mission. To cater for multiple instances of the same handler, multiple instances of both the underlying handler framework and application processes are necessary.

We recapture that not all classes of an SCJ program require process models. In particular, those belonging to DC have mere OhCircus class models, such as the Controller class. Conversely, SCJ components without any instance fields do not require a class model and thus have only a process model.

5.5. Event Handlers

Handler classes belong to the category HC and, as already noted, their application processes differ in terms of structure from those of the safelet, mission sequencer and missions (belonging to category SMMC). Most significantly, the application process for a handler may associate external events to it. In addition, it has a dispatch action Dispatch to release the handler either when one of these events occurs, or periodically in the case of periodic handlers. The general pattern, however, is still that described in Fig. 13.

As with classes belonging to the category SMMC, the application processes for handlers are factored into a data object modelled by an OhCircus class, and a process that aggregates the data object and releases the handler. Because we treat handlers as data objects, other data objects can hold a reference to them and directly call their methods or access and modify their fields. In the cruise controller, for instance, the Controller class holds a reference to the SpeedMonitor and ThrottleController handlers and thereby is able to acquire the vehicle's speed and set the throttle voltage. Since Controller is a data object (not wrapped by a process), these calls can be modelled by OhCircus method calls rather than synchronisations. This simplifies the overall application model.

Fig. 18 presents the OhCircus class for the Engine SCJ class, included in Appendix B.1. As before, we have a direct correspondence with instance variables defined as state components, and the constructor defined in the initial paragraph. The only difference

```
class EngineClass :: begin
  state EngineState ::= [private cruise : ControllerClass]
  initial EngineInit ::= val c : ControllerClass • cruise := c
  public handleAsyncLongEvent ::= val evt : long •
  if evt = EngineOn -> cruise.engineOn()
  | evt = EngineOff -> cruise.engineOff()
  fi
end
```

**FIGURE 18.** OhCircus class for the Engine handler.
is that to model the static fields Events.EngineOn and Events.EngineOff, we use the constants EngineOn and EngineOff. The Events class provides unique long values for all external events of the cruise controller as a collection of public, static and final fields. Although we do not consider models of static fields and methods in general, a static and final field that is initialised upon declaration is modelled by introducing a global axiomatic constant of the same name. (Issues related to name clashes, if present, are dealt with by prefixing the name of the constant with the name of the class in which the field resides in the program.)

The handler method is parametrised, mirroring the parameter of handleAsyncLongEvent(int). As explained in Section 2.2, the parameter is used to determine the external event that caused the release of the handler. Based on its value, the handler method decides by virtue of a switch statement which method to call on the controller object, and this is modelled by a conditional in Fig.18. The classes used to implement the interrupt service routines that identify external events and release the corresponding event, it has to be modelled in a different way. For events associated with the handler. In our example, they are engine_on and engine_off. When such an event occurs, Dispatch calls the handleAsyncEventMeth action, passing an input value identifying the event. It also offers a synchronisation on leave_dispatch, which is used to abandon the dispatch loop when the handler is terminated by its associated framework process.

The handleAsyncEventMeth action simply executes the corresponding data operation, preceded by a nondeterministic wait that sets a time budget: the permissible amount of time the program may take to execute the operation. Abstract global constants are introduced for all data operations to refer to their permissible amount of time. The nondeterministic wait that sets the budget is modelled by introducing a global axiomatic constant of the same name.

A consequence of our modelling approach is that

writeVoltageMeth in Fig. 20 cannot be invoked by an ObCircus method. In the cruise controller this is not a problem, since no other method except for handleAsyncEvent() calls it. This, however, hints at a more general issue: methods that carry out some device access inherently require an action model, and so do all methods that directly or indirectly call them. Our technique hence imposes certain restrictions on the SCJ program designs that we can cater for, and Section 6 examines those restrictions in more detail.

Application processes for periodic handlers differ only in the definition of Execute and in the presence of an additional action Release. As illustrated in Fig. 20, the handler behaviour in this case is defined by a parallelism between two actions Dispatch and Release. Here, the handler does not wait for the occurrence of an external event, but instead invokes handleAsyncEventMeth when an internal handler-specific timer event is raised.

The parallel action Release generates these timer events. In its definition in Fig. 20, we have a prefix that raises the release_handler . ThrottleHId event, which is the timer event for the throttle handler, followed by a wait this.period action to wait for the duration of the period. The recursion in Release ensures that timer events are generated continually until an interrupt occurs, causing the handler to leave its dispatch loop. If Dispatch is still executing handleAsyncEventMeth when Release is ready again to synchronise on release_handler . h, the synchronisation is delayed until the handler method is completed. Since the timer event is concealed (hidden) in the system model, it takes place autonomously and in fact as soon as possible, that is, when both Dispatch and Release are ready to synchronise on it.

To increase modularity, we take advantage of class inheritance by introducing a class for periodic handlers that has a state component period. This class somewhat corresponds to the abstract class PeriodicEventHandler in SCJ. We thus require that concrete periodic handler classes extend this class also in the model. The period is set by either passing a value to the constructor of the base class, or explicitly by changing the value of period in the subclass constructor.

We observe that the handler application processes in our example lack a Methods action. This is because in the ACC, the handlers do not define methods called by the framework. Furthermore, the call to handleAsyncLongEvent( int ) takes place within the process and is modelled by an action call. In general, however, we do not exclude the possibility of defining such methods, following the pattern in Fig. 13.
5.6. Data Objects

As already noted, data objects are modelled by an OhCircus class only. For illustration, Fig. 21 contains an extract from the OhCircus class definition for the Controller SCJ class. We observe that since this class holds a reference to two handler objects, we have state components of type SpeedMonitorClass and ThrottleControllerClass. All methods in this class are declared as synchronised using the OhCircus keyword sync explained in Section 2.3.2. Some state components and methods have been omitted or abbreviated for brevity.

The Controller class in essence implements a state machine. The methods are called by aperiodic handlers in response to external events such as the engine being switched on or the cruise mode being activated. For instance, the engineOn() method changes the values of some of the state components of boolean type. More interestingly, inside the activate() method we have calls to methods on the aggregated throttle and speedo class objects. These calls directly access and modify the data (state) of the class objects of the respective handlers.

To conclude, in the previous sections we have examined in detail the construction of a formal model for an SCJ program, elaborating and refining our account in [37]. In particular, we have unified the treatment of behavioural and data aspects by way of the general pattern in Fig. 13. In the next section, we formalise a translation strategy that constructs Circus models of SCJ programs using the approach described.

6. TRANSLATION STRATEGY

Given an SCJ program, the problem we address in this section is the automatic derivation of its application model. Not all SCJ programs are translatable by our approach, and, so far, we have been vague about the subset of SCJ that we handle, as well as the details of the model construction process. We now present a compositional translation strategy.

In Section 6.1, we first specify the admissible subset of SCJ programs. Section 6.2 then discusses the top-level translation process. The remaining Sections 6.3
to 6.5 examine in detail the translation of SCJ classes for the entities of the mission model and data objects.

6.1. Translatable Programs

The programs we accept foremost have to be compilable with a compliant SCJ class library. Since SCJ is still evolving, we consider the API published in the first official draft of the SCJ technology specification [2]. The generality of Java, however, enables us to write SCJ programs that do not reflect the clean architecture implied by the SCJ paradigm. To give an example, the same class can be used as the Safelet and MissionSequencer of an application. We disallow such designs and more generally require programs to adhere to design patterns that embody good programming practice. Finally, as already noted in the introduction, the design of SCJ [2] does not address constraints on statements that make certification (and formal analysis) feasible. We address this concern by taking restrictions of SPARK [32] as a guideline. We note that checking for compliance with the restrictions we introduce can be automated in a fairly straightforward manner.

In the sequel, we specify our restrictions in more detail. We divide them into three kinds: structural constraints, language constraints and feature constraints.

6.1.1. Structural Constraints

Our first structural constraint, as hinted above, is that the safelet, the mission sequencer, and each mission and event handler are modelled by a separate class. This ensures that there is a one-to-one correspondence between classes that represent components of the SCJ infrastructure and their respective process descriptions in the application model. Applications that initially do not satisfy this constraint can usually be refactored.

A second structural constraint is that we only consider one level of inheritance in the context of the SCJ classes. This means that the safelet, mission sequencer, mission and handler classes of an application have to be direct subclasses of the respective SCJ API class or interface. The rationale for this restriction is that, because these classes belong to either category SMMC or HC, they have a process model, and there is currently no notion of process inheritance in OhCircus. Other classes, namely those belonging to category DC can make unconstrained use of inheritance (class inheritance is well supported in OhCircus).

A third constraint is concerned with the places in the program where we allow interaction with the hardware and external devices. Confining external device interaction to the handler classes enforces good programming practice, resulting in cleaner application designs with more tractable formal models. We thereby obtain a clean separation of active classes that interact with the framework, having process models, and passive classes that record application data and carry out computational work. This may possibly be at the cost of reducing reusability, but, what is important, facilitates analysis and the refinement of models.

The fourth and last constraint is that we prohibit the use of inner and anonymous classes. This is not a serious limitation since such constructs are merely syntactic sugar and can always be eliminated through refactoring. Excluding them discharges the burden of having to define a semantics for them in OhCircus which, by default, does not cater for such classes.

Together the four constraints determine the structure of applications for which model generation succeeds.

6.1.2. Language Constraints

As already mentioned, the SCJ technology specification [2] does not prescribe what low-level language elements and constructions are permitted in SCJ programs. In a certification context, it is, however, not desirable to support the full generality of Java. Our language restrictions are similar in spirit to the ones defined by SPARK [32]. They do aid the clarity and analysability of SCJ programs, but ultimately account also for limitations implied by our translation strategy. The following list summarises the elements of the Java language that we exclude.

1. Expressions with side effects such as 
\((x++)*(y--)\). This applies to any type of expression, namely boolean expressions in conditional statements and loops. Likewise, none of the arguments of a method call may have side effects either.

2. Labels as well as stand-alone break and continue.

3. Arbitrarily placed return: a return statement must be the last statement in a method, if present.

4. Fall-through behaviour in switch statements. This means that every case statement must be properly terminated with a break statement.

5. Program exceptions and hence the use of try, throw and catch and, in general, also finally.

6. Blocks that are marked as synchronized as well as the wait() and notify() methods.

7. static methods; synchronized fields are only supported if they are final and initialised upon declaration.

From (1), it implicitly follows that we do not support assignments in expressions. We observe though that expressions with side effects can always be rewritten into statements to fulfil this constraint: this is by way of introducing local variables that hold intermediate results of a calculation. We also point out that (1) does not exclude assignment statements as stand-alone commands. For instance, \(x = x + y\); and \(x++\); are allowed as they do not occur in an expression.

The restrictions (2) and (3) also exist in safe subsets of Ada and C [32]. The precise reasons for them in terms of our modelling approach are discussed later on (page 28). The absence of exceptions (5) is related to issues of memory utilisation and predictability in SCJ. Although exceptions can be useful in designing error catching mechanisms, they may be less essential.
where formal verification techniques are consequently applied. A limited facility to model exceptions that raise program errors is provided by the divergent action **abort**. We observe that the blocking constructs in (6) are already excluded by SCJ Level 1. Support for static methods (7) is work in progress; **final** and **static** fields, on the other hand, can effectively be treated as constants and are thus already incorporated.

### 6.1.3. Feature Constraints

Some SCJ Level 1 classes are not covered by our translation strategy. These classes are typically either an artifact of the implementation of SCJ or of program interaction with devices and the external world. Excluded classes are in particular:

1. Classes such as **ManagedEventHandler**, which are an artifact of SCJ's design on top of RTSJ.
2. The **Clock** class and all timing-related classes except for **RelativeTime** and **AbsoluteTime**.
3. Classes of the input and output model, like, for example, **ConsoleConnection**.
4. The Java Native Interface (JNI).

To explain (1), we note that the original aim of SCJ was to design it as a restriction of the RTSJ class library. The RTSJ classes are, however, not directly relevant to SCJ programs. They merely facilitate the development of a reference implementation of the SCJ technology on top of RTSJ. (There are also inclinations in the SCJ community to depart from this design in future versions of SCJ, hence it is not desirable to model them here.)

The features (2) and (3) are in principle desirable to support as future work, but with regards to our current contribution out of scope. The concession we make for not supporting (2) is that we exclude applications that make more sophisticated use of time control. The classes **AbsoluteTime** and **RelativeTime** are nevertheless supported by way of data objects. They are used to set the period of periodic handlers.

Support for (3) seems not difficult to achieve, but is not essential for our case studies. In our experience so far, there also seems to be no need for (4). This is due to the abstract view of interactions in terms of CSP events. We envisage that native code is only significant in implementing low-level routines for device interaction and hardware access, and these are fundamentally not modelled in detail, but instead captured by events. Where JNI may be used in other ways, for instance, to exploit performance-enhancing hardware, future extensions of our translation strategy are conceivable that incorporate models of JNI methods that have to be explicitly provided by the user.

The following classes are allowed as part of the **IC** category, but we do not provide formal models for them:

1. Classes related to interaction with devices and external events such as **InterruptServiceRoutine**.
2. Classes related to signals and happenings, such as **POSIXSignal** and **Happening**.

Since we take an abstract view of device interactions as CSP communications, we do not model the above classes. We require though that their design justifies the assumption that device access is atomic. In other words, the program should not be able to make any observations about the mechanisms that read (or write) data from (or to) the hardware, only that the data is made available as a whole. In particular, this has to be the case if complex data is communicated via inputs and outputs. Device access, however, does not have to be instantaneous, like CSP communications. Common modelling techniques in CSP can be used to explicitly model device interactions that take time, namely, as a pair of communications. Where such interactions can be regarded as virtually instantaneous, by which we mean they take a negligible amount of time, we encode them as single events. Although the implementation in that case weakens the precise timing behaviour, we stipulate that a similar argument as devised in [42] for timed automata can be construed to formally justify correctness of implementations in Circus, that is, under weaker notions of refinement such as $\varepsilon$-bisimulation.

To summarise, the SCJ developer has to guarantee that the program code for device access establishes at least atomicity of data being read or written. Virtual instantaneity is required only if device interactions are modelled by single events. The choice to adopt the single-event approach is, however, even then an issue of design that rests with the user of our technique.

We discuss a few basic architectural patterns for device interaction in Section 7.2, but in general such patterns are per se not a concern of the translation strategy. We also note that the language constraints in Section 6.1.2 do not apply to classes in the category **IC** and interaction code, for the reason that they are not subject to compositional translation.

Despite the restrictions presented in this section, it turned out to be possible to support our case study here as well as those in [36, 43] after refactoring. In the next section, we present our translation strategy applicable to all programs that fulfil the above constraints.

### 6.2. Translation Process

Translation is carried out by a three-stage process.

1. Analysis and annotation of the program code.
2. Automatic rewriting to transform program statements into a canonical form.
3. Translation of classes by category-specific rules.

Stage (1) is organised in four steps (1a) to (1d). We explain each of them next. Stages (2) and (3) are fully automatable via the rules we present later on.

**Step (1a).** In the first step, we proceed with an analysis of the program structure. We categorise all

---

The Computer Journal, Vol. ??, No. ??, ????
classes of the SCJ program according to Table 4. To determine the active classes, namely those belonging to SMMC and HC, it is sufficient to examine the superclasses and implemented interfaces of a class. For the remaining classes, we have to make an intelligent decision whether they are data objects or interaction classes. Typically, interaction classes derive from classes of the ‘Interaction with Devices and External Events’ subclass hierarchy of the SCJ API [2]. There, we have classes such as InterruptServiceRoutine or Happening. Nevertheless, we do not categorically exclude non-SCJ classes being part of interaction patterns. Therefore, establishing membership of a class to either DC or IC in general requires insight and understanding of the program design and code, although there is scope for automation, too. In practical terms, the classification between DC or IC is encoded by custom Java annotations discussed in the next section. The annotations are an input for the translation in Stage (3).

Table 5 summarises the classification of the classes of the ACC. We observe that for each aperiodic handler (active class) we have a corresponding interrupt service routine (interaction class), suffixed with ISR, that releases (fires) the handler. In contrast, there is only one class Controller for a data object.

Step (1b). In the second step, we identify the instances (rather than classes) of missions and handlers of an application and introduce unique identifiers for each of them (of type MissionId and HandlerId). This constitutes a second input of the subsequent classification and again requires understanding of the SCJ program. As before, we encode this knowledge by way of special annotations in the program. For the ACC, we have a single identifier ACCId of type MissionId for the single instance of the ACCMission class, and the identifiers WheelShaftId, EngineId, and so on, of type HandlerId, for the various handler instances.

Step (1c). In a third step, we determine the external events that cause the release of aperiodic handlers in the program, and annotate the respective handlers classes accordingly. This requires inspection of the mission initialisation methods that create the handlers.

Step (1d). In a final step, all methods of the SMMC and HC classes are annotated as to whether their bodies perform device interactions or external hardware accesses. For methods that do so, our analysis also has to provide a model for the device access as an action. Those methods are not translated by our strategy: their explicit action model is used instead.

Stage (1) is completed when the program is fully annotated to provide all necessary information to facilitate the (automatic) translation of the classes in Stage (3). It is worth noting that although Stage (1) in general requires human assistance, essentially no knowledge of formal models and Circus is needed for the steps (1a) to (1c). We furthermore stipulate that a tool could be developed to automate the annotation process, and, if not fully complete it, at least yield a good approximation. This is ongoing work.

Stage (2). The rewriting rules we apply to program statements in Stage (2) are summarised in Table 6. We use the function \([\ldots]\) to capture the rewriting transformations. (Other functions \([\ldots]\) with different subscripts are defined later on when formalising the translation.) To highlight meta-variables, we underline them as in Expr and Meth. The name of the meta-variable also implicitly determines the syntactic category of the element matched. The abstract syntax we consider is the typical one of Java [44].

**RW1** deals with local variables (as opposed to class fields) being initialised upon declaration. **RW2a** and **RW2b** rewrite the shorthand forms for the increment and decrement operators, which we support as stand-alone statements. **RW3** rewrites compound assignments into standard assignments. Lastly, **RW4** and **RW5** deal with truncated forms of the conditional and switch statements.

In the remainder of this section, we individually discuss the translation of active classes and data objects in Stage (3). As mentioned before, interaction classes are not modelled and thus not translated.

### 6.3. Active Classes

We have one translation rule for each type of active class, namely for the safelet, mission sequencer, a mission or a handler. The translation rule for a safelet, for example, is presented in Fig. 22. It matches all classes that implement the Safelet interface. Meta-variables of the rule, which as before are underlined, are CName, FieldDefs, InitStmts, AMethDecl1, AMethDecl2, and so on.

The right-hand side of the rule constructs the process that models the class (that is, its active behaviour). We note that in this section, we only consider the process.
model of active components. The associated OhCircus class, capturing state and data operations, is generated by the same translation rule that we use for passive classes and discuss in Section 6.5.

The rule makes use of two auxiliary translation functions, \([\ldots]_{\text{Name}}\) for translating identifier names and \([\ldots]_{\text{Method}}\) for translating methods into actions. Suffixes in the translation functions are used for clarity and also to avoid ambiguities later on when presenting complementary rules for passive classes. The function \([\ldots]_{\text{Name}}\) is used to encode an identifier for a class, variable, or method into a valid Z identifier. For classes, this uses the fully-qualified name of the class and replaces \(\cdot\) separators by underscores. Other symbols not permitted in Circus are substituted suitably as well. The function furthermore ensures that method names are unique in the presence of method overloading. The function \([\ldots]_{\text{Method}}\) encodes a class method as a local action definition. It is applied to all methods of the class that are modelled by actions. Such methods are, first of all, the setUp() and tearDown() methods, but also possibly other methods that interact with devices and hardware and thus require action models.

Although not made explicit in the rules, rule matching exploits the presence of annotations that indicate whether a method is to be translated into an action or a data operation. We shall not specify the details of the annotation mechanism here as this is rather a technical issue for a tool and discussed in the next section. Instead, we implicitly assume that \([\text{MethodDec1}]_{\text{Method}}\), \([\text{MethodDec2}]_{\text{Method}}\), and so on, only match methods that are annotated to require action models. Other methods are simply ignored by the matching process and become significant only in constructing the class model. The FieldDecks meta-variable is matched with the declaration of instance variables of the class. In what follows, we individually discuss the elements of the process resulting from the translation, that is its State, Init action, method actions, and main action.

**Process State.** The translation constructs the state paragraph of the process using a schema State, which includes a single component this whose type
is that of the underlying data object. Whereas
the process name is defined by \([CName]_{Name\,App}\),
the name of the respective \(OhCircus\) class is defined by
\([CName]_{Name\,Class}\). This realises the wrapping
pattern described in Fig. 13. The result of the
translation for our example safelet is exactly the process
in Fig. 14 after a trivial simplification to remove the
empty state paragraph and initialisation action.

Init Action. The initialisation action assigns a new
instance of a class object to this. We note that the
creation of the class object also entails the constructor
being executed, so that the fields of the class object are
suitably initialised. The constructor itself, whose body
is visible by \(Init\,Stmts\), is modelled in the corresponding
\(OhCircus\) class rather than in the process in Fig. 22.

Method Actions. Interacting and infrastructure meth-
ods of an active class are translated, as already men-
tioned, by \([\ldots]\,A\,Method\). Each method results in the
declaration of a local action with suffix \(Meth\). The cor-
responding rule is in Fig. 23. The rule makes explicit
that we require all methods of active classes to be syn-
chronised. The rule is applicable to methods that have
both a return value and parameters. The name of the
local action is derived from the name of the method in
the program and so are the names of the \(Call\) and \(Ret\)
channels on which we synchronise to call the method
and to wait for its completion. (We also have translation
rules that introduce those channel pairs.)

We use two further translation functions in the safelet
rule: \([\ldots]\,Type\) and \([\ldots]\,Stmts\). The \([\ldots]\,Type\) function
encodes a Java type as a corresponding Z (and,
therefore, \(Circus\)) type. Its definition is included in
Appendix D.1. We support all primitive types of Java,
although we do not define a model for \(float\) and \(double\) at present. Future work may address this, using,
for instance, an axiomatisation of the real numbers
in Z like the one in [45]. Z types are introduced to
represent the various semantic domains for primitive
Java types. Reference types refer to \(OhCircus\) classes
that result from the translation of data objects and have
a suffix \(Class\). Arrays are modelled by sequences and
we provide generic functions to construct array types
and to get and set the elements of an array.

The \([\ldots]\,Stmts\) function translates a statement block
(here the method body) into an action term; we discuss
it in more detail in the remainder of this section.
The bound variables \(args\) and \(ret\) are visible by the
translation of the body, and can be used to refer to the
arguments of a call and to set the return value.

Returning from a method results in assigning the
return value to \(ret\). This is captured by the following
translation rule for a \(return\) statement.

\[
[return\,Expr]\,Stmts \equiv \, ret := \,[Expr]\,Expr
\]

The translation function \([\ldots]\,Expr\) translates a (side-
effect free) expression; we discuss it in the sequel. The
suitability of the rule above, as well as the one in Fig. 23
is contingent on no statement(s) following a \(return\).
This is, however, ensured by our structural constraints.

For methods that do not have parameters or a \(void\)
return type, we provide rules that take a simpler shape.
There, the input and output prefixes become simple
synchronisations as illustrated in Fig. 24.

Table 7 presents the most interesting rules for state-
ment translation. They cater for assignments (SR1),
local variables (SR2), conditional statements (SR3),
switch statements (SR4), while-loops (SR5) and
assertions (SR6). The remaining rules can be found in
Table D.5 of Appendix D. They deal with state-
ment sequences (SR7–SR8), blocks (SR9) and
for-loops (SR10) and are mostly straightforward.

We point out that in SR2, \(Stmts\) includes all
remaining statements of the current block. Also, in
the conditional of the right-hand action of SR4, no
nondeterminism can arise since compilation enforces the
values \(Value_{1}\), \(Value_{2}\), and so on, to be distinct.
While-loops (SR5) are modelled by a recursion. Depending
on the value of the loop condition, we either execute
the loop body and recurse, or terminate the loop via a \(skip\)
action. The absence of \(break\) and \(continue\) statements
ensure that this is a correct model.

As an example, we give the translation of part of the
\emph{handleAsyncEvent()} method in the \emph{Throttle-
Controller} class. An extract of this method, after
rewriting, is included in Fig. 25. The translation uses
the rule SR3 to translate the if statements, SR1
and SR2 to translate the assignment and variable
declaration, and SR10 and SR11 (Appendix D) to
translate statement sequences and blocks. The result of the translation is given by the following action.

\[
\text{handleAsycnEventMeth} \triangleq \\
\begin{array}{l}
\text{if }\text{this.schedule\_throttle} = \text{TRUE} \rightarrow \\
\text{if }\text{this.accelerating} = \text{TRUE} \rightarrow \\
\quad \text{increaseVoltageCall} \rightarrow \text{skip}; \\
\quad \text{increaseVoltageRet} \rightarrow \text{skip} \\
\quad \text{if }\text{this.accelerating} = \text{FALSE} \rightarrow \\
\quad \text{if }\text{this.maintainSpeed} = \text{TRUE} \rightarrow \\
\quad \text{var current\_speed : int } \bullet \\
\quad \quad \text{current\_speed} := \text{this.speedo\_get\_current\_speed}(); \\
\quad \text{if }\text{this.cruise\_speed} - \text{current\_speed} > 2 \rightarrow \\
\quad \quad \text{increaseVoltageCall} \rightarrow \text{skip}; \\
\quad \quad \text{increaseVoltageRet} \rightarrow \text{skip} \\
\quad \quad \text{if }\text{this.cruise\_speed} - \text{current\_speed} < -2 \rightarrow \\
\quad \quad \text{resetVoltageCall} \rightarrow \text{skip}; \\
\quad \quad \text{resetVoltageRet} \rightarrow \text{skip} \\
\quad \quad \text{fi} \\
\quad \text{if }\text{this.maintainSpeed} = \text{FALSE} \rightarrow \text{skip} \\
\quad \text{fi} \\
\text{fi} \\
\text{if }\text{this.schedule\_throttle} = \text{FALSE} \rightarrow \text{skip} \\
\text{fi}
\end{array}
\]

References to instance variables are via the aggregated class object this. The dots correspond to the translation of the code that has been omitted in Fig. 25. To translate calls to the methods \text{increaseVoltage() and resetVoltage()}, we require further rules. These are given in Table D.6 in Appendix D. The semantics varies depending on (a) the type of the target object and (b) whether the invocation assigns the return value to a variable. In the example above, we use the rule for a method call in an assignment where the target is the safelet or mission sequencer (SR11). Since there is only one safelet and mission sequencer in a valid SCJ program, the corresponding channels are not parametrised by a type-specific identifier.

For missions and handlers (SR13 and SR14), we require an additional channel parameter to identify the target object, as there potentially may be more than one, namely if we have multiple missions and handlers. The association of classes with identifiers is determined, as already explained, by annotations which are created during the analysis and configuration in Stage (1).

Finally, to define the behaviour of the application process, we generate an action \text{Methods} (Fig. 22) that offers to other processes the choice of calling one of the interacting methods of the class.

\text{Main Action}. The main action is completely generic and always has the same shape, firstly executing the initialisation action \text{Init}, and then offering a call to one of the methods until the process is terminated. Here, we take advantage of the structural constraint that all methods of active classes are synchronized. In cases where the class does not have instance variables, like the \text{ACCSafelet} class of the ACC, simplifications are possible. They are obvious and thus their translation rules are not further discussed here.

In addition to a process for each active class, we moreover have to introduce declarations for the method-channel pairs of non-infrastructure methods of the class, since those are application specific. The corresponding rules are applied independently of the rules for translating classes into processes and give rise to separate specification paragraphs in the generated models. These rules are not very interesting though, therefore a detailed discussion is omitted.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
Rule & Application & Result \\
\hline
SR1 & \[ \text{Var} = \text{Expr}; \] & \[ \text{Name} := \text{Expr}; \] \\
\hline
SR2 & \[ \text{Type} \text{Var}; \] & \[ \text{Name} : \text{Type}; \] \\
\hline
SR3 & \[ \text{if} (\text{Expr}) \] & \[ \text{if} (\text{Expr}) \] \\
\hline
SR4 & \[ \text{switch} (\text{Expr}) \{ \] & \[ \text{if} (\text{Expr}) \] \\
\hline
SR5 & \[ \text{while} (\text{Expr}) \] & \[ \mu X \bullet \] \\
\hline
SR6 & \[ \text{assert} \] & \[ \text{abort} \] \\
\hline
\end{tabular}
\caption{Translation rules for sequential statements.}
\end{table}
public void handleAsyncEvent() {
    if (schedule_throttle) {
        if (accelerating) {
            increaseVoltage();
        }
        else {
            if (maintainSpeed) {
                int current_speed;
                current_speed = speedo.getCurrentSpeed();
                if (cruiseSpeed - current_speed > 2) {
                    increaseVoltage();
                }
                else if (cruiseSpeed - current_speed < -2) {
                    resetVoltage();
                }
                else { /* Remainder of the code is omitted! */ }
            }
        }
    }
}

FIGURE 25. handleAsyncEvent() method of the ThrottleController class.

The translation rules for the mission sequencer and missions are included in Appendix C; they are very similar to the safest rule just discussed. We have a minor deviation in the main action of the translation rule for a mission that ensures that the mission application process is restarted after termination of the mission so that the mission can be executed more than once. The rule for handlers is more interesting: we discuss it in more detail in the next section.

6.4. Handler Classes

Handler classes are essentially active classes. Their model slightly differs though in terms of the process structure. The translation rule for an aperiodic handler is included in Fig. 26. It defines the translation of handler classes that either extend AperiodicEventHandler or AperiodicLongEventHandler.

Unlike in the process models for the safest and the mission sequencer, the coupling between process and data object in handler processes is dynamic. Hence, we introduce a channel communication \( [CName]_{Name_Init} \) upon construction of a handler instance (see Fig. 26). The handler process synchronises on this channel in the Init action to establish the link to the underlying OhCircus class object that captures the state and data operations of the SCJ class. In the model of the ACC, this is illustrated by the handler processes in Fig. 19 and Fig. 20. The initialisation channels these handlers synchronise on are EngineInit and ThrottleControllerInit. At the point of synchronisation, the OhCircus class objects have already been created with their fields initialised by a class constructor.

The execution behaviour of handlers (defined by Execute) is specified in a way that slightly differs from the pattern for classes belonging to SMMC. This is because we require additional active behaviour in order to release the handler, in addition to offering calls to interacting methods. As already said, Dispatch takes care of both method calls and handler releases. It also enables termination of the handler via a handler-specific leave\_dispatch.\_h event, parametrised by a handler identifier \( h \). Execution starts with a synchronisation on enter\_dispatch.\_h.

The function BoundEvents in Fig. 26 determines the bound events of a handler class. For each handler class of an application, we specify the bound events as part of the analysis and configuration in Stage (1c).

When an external bound event occurs, the action handleAsyncEvent, encoding the handler method, is invoked. Its behaviour is determined by the body HdlStmts of the handler method. We use an auxiliary translation function \( [\_]_{HdlBody} \) which is defined by

\[
[HdlStmts]_{HdlBody} \equiv \text{wait} [CName]_{Name}_\text{handleAsyncEvent}_{TB}; \text{this.handleAsyncEvent}(inp)
\]

if the handler method is a data operation, and by

\[
[HdlStmts]_{HdlBody} \equiv [HdlStmts]_{Stmts}
\]

if the handler method interacts with external devices or hardware. In the non-interacting case, translation uses the encoding of the handler method as an OhCircus method in the underlying OhCircus class. The constant that is obtained by suffixing the class name with handleAsyncEvent\_TB specifies the time budget of the handler. Otherwise, the method is given an action model using \( [\_]_{Stmts} \) like other interacting methods.

The application process for a periodic event handler requires a modification in the definition of Dispatch and
class CName extends AperiodicEventHandler {

FieldDecls
public CName() { InitStmts }
AMethDecl1
AMethDecl2
...
public void handleAsyncEvent() {
            HdlStmts
 }
}

process [CName]_{Name_App} \triangleq begin
state State \triangleq [this : [CName]_{Name_Class}]
Init \triangleq [CName]_{Init} \triangleright obj \rightarrow this := obj
[AMethDecl1]_{AMethod}
[AMethDecl2]_{AMethod}
...
Methods \triangleq ([AMethDecl1]_{Name_Meth} \square
[AMethDecl2]_{Name_Meth} \square
...
handleAsyncEvent \triangleq val inp \bullet [HdlStmts]_{HdlBody}
Execute \triangleq enter_{dispatch} . IdOf(CName) \rightarrow Dispatch
Dispatch \triangleq
\begin{align*}
\mu X \bullet & \left( \begin{smallmatrix}
\square \text{ext} : \text{BoundEvents}(CName) \bullet \\
\square \text{ext} ? \text{inp} \rightarrow \text{handleAsyncEvent}(\text{inp}) \\
\text{leave}_{\text{dispatch}} . \text{IdOf}(CName) \rightarrow \text{skip}
\end{smallmatrix} \right) ; X \\
\end{align*}
end

FIGURE 26. Translation rule for classes extending the AperiodicEventHandler class.

a supplementary action Release. The corresponding rule is included in Appendix C (Fig. C.5). There, the handler is released by an internal handler-specific timer event release_handler . IdOf(CName) rather than an external event, as it is the case for aperiodic handlers.

Having explained in detail how active classes are given a process model, in the next subsection we examine the translation of data objects.

6.5. Data Objects

We next define the translation of classes belonging to the category DC. They do not interact with the SCJ infrastructure or external devices. The high-level translation rule for such classes is presented in Fig. 27. The result of the translation is an OhCircus class. In the rule, we assume that the class extends another class CBase and explicitly calls one of its super constructors. An alternative rule also exists for the simpler case where we do not have inheritance. We omit its detailed specification, which can be obtained by removing the ‘extends’ clauses in Fig. 27. We recall that active classes, namely those in category SMMC and HC, are also translated using the rules for data objects since they give rise to both a process and an OhCircus class (see Table 5.1). In active classes, however, only the non-interacting methods are considered and neither do we consider methods called by other active components. The name of the OhCircus class is derived from the name of the of Java class, suffixed with Class. As in the rule for active classes, we first have a state paragraph that determines the state of a class object. The state paragraph is constructed from the declaration of non-static instance variables of the class. The translation functions [...]_Fields and [...]_FieldInit apply to (lists of) field declarations and are used to generate the state components and the initialisation schema of the class. Field initialisation takes place upon declaring the variables and is captured by the [CName]_{Name_Init} schema operation.

For [...]_Fields we have the rules in Table D.4 in Appendix D. They make use of the functions [...]_Name and [...]_Type that have already been mentioned, and are specified in Appendix D, too. For field initialisation, we have the rules in Table 8. There, [...]_FieldType_{DefaultInit} is defined to yield the default value of a primitive type. We omit its definition, which is in line with the Java language specification [44].

AccessModifier stands for any of the access modifiers public, protected or private. The translation of access modifiers is trivial as it merely replaces them by the corresponding OhCircus keywords: public, protected and private. These keywords enforce similar visibility restrictions as in the Java language. Notably, the private keyword reflects the particular class-based semantics of private access adopted by Java. We point out that we do not capture package access in our model. Chiefly, because OhCircus does not have a structuring notion equivalent to Java packages.

We recall that the function [...]_Expr translates an expression. An extract of its definition is in Table D.3 in Appendix D. This is done in the usual manner, encoding Java operators using corresponding Z operators on primitive types. Because of the restrictions in Section 6.1.2, and prior rewriting, an expression cannot have side effects unless it is the right-hand of an assignment. Therefore, all method calls that occur in
an expression can be modelled by OhCircus function invocations. The corresponding rule for translating method calls in expressions is as follows.

\[
\begin{align*}
\text{Obj, Meth(Args)} & \xrightarrow{\text{Expr}} \text{Obj} \text{Expr} \cdot \text{Meth} \text{Name}(\text{Args})_{\text{Expr}}
\end{align*}
\]

It only applies to methods that are data operations (non-interacting). Method calls that do provoke side effects can only occur in the restricted forms \text{Obj, Meth(Args)}; and \text{Var = Obj, Meth(Args)}; and a specific rule is applied to the latter that introduces the assigned value as a result parameter of the method.

The initial paragraph encodes the construction of the class object. This involves field initialisation, the invocation of the superclass constructor, and the statements of the constructor. As we support constructors with arguments, we have to account for them in the translation. The auxiliary \text{[..., Args] function yields the parameter declarations corresponding to the call signature of a constructor or method. If applied to an argument tuple, \text{[..., Args distributes through that tuple. If applied to a single argument, we have the rule below.

\[
\begin{align*}
\text{Type Var} & \xrightarrow{\text{Arg}} \text{Var} \text{Name} : \text{Type}
\end{align*}
\]

For example, \text{val ((String name, int age)) Args evaluates to val name : StringClass; age : int}.

The constructor, whose body is given by \text{InitStmts}, is translated into an OhCircus method. The function \text{[..., Stmts is used again for this purpose. As before, it translates a Java statement block. Here, however, the result is the description of an OhCircus method rather than an action. The rules in Table 7 nevertheless still apply; for the translation of method calls (Appendix D.6) we have a different rule that translates them into OhCircus method calls rather than synchronisations on \text{Call and Ret} channels.

In translating method declarations, we introduce the function \text{[..., DMethod} rather than \text{[..., AMethod since there is a fundamental difference with respect to active classes. It encodes a (non-static) class method as an OhCircus method rather than an action.

\[
\begin{align*}
\text{AccessModifier Type Meth(Args) \{ Body \}} \xrightarrow{\text{DMeth}} \text{val} \text{[... Args; res ret: [... Type} \text{Type} \bullet \text{[... Stmts}
\end{align*}
\]

The main difference is that we do not have channel communications as in Fig. 23. Instead, value and result parameters are used for passing arguments and setting the return value. The method body is translated by \text{[... Stmts (defined in Table 7). The rules for object creation and method calls in Tables D.6 and D.7, however, do not apply. Instead, we use the \text{new} and method call constructs provided by OhCircus.

To conclude our account on the translation strategy, we recall that certain methods are excluded from the application of the translation rules. Namely, these are the methods that carry out device or hardware accesses. Here, annotations explicitly provide action models for the methods, and these models are directly used in the processes rather than the result of \text{[... AMethod}.

In the next section we discuss implementation issues and examine how translation of the ACC program is
performed automatically by our tool.

7. AUTOMATIC TRANSLATION

To automate the translation of SCJ programs into Circus models according to the rules presented in the previous section, we have developed a translation tool. It takes a translatable program according to the restrictions in Section 6.1 as an input and produces a collection of Circus specification files, encoded in the \LaTeX\ mark-up format understood by the Circus parser of the Community Z Tools (CZT) [34]. Our tool is freely available from the hiJaC project page: http://www.cs.york.ac.uk/circus/hijac/tools.html.

The translator tool is implemented in Java and takes advantage of a number of third-party utilities and libraries. They are specifically the Compiler API of the JDK 7 [46], JSR 308, which extends the capabilities of Java’s annotation mechanism [47], and the FreeMarker template engine [48]. Our tool design facilitates modifications and extensions of the translator and defines a clean component framework in which the core translator is traceable to our rules.

The configuration of the translation in Stage (1), as already explained, is realised by a set of custom Java annotations. They are summarised in Table 9. We discuss their individual purpose in the next section.

7.1. Annotation Framework

We can categorise the annotations into four groups.

1. Annotations that determine the categories of Java classes. In this group, we have @ActiveData for both SMMC and HC, @PassiveData for DC and @InteractionClass for IC.

2. Annotations that specify identifiers of SCJ classes in the Circus model. Here, we have @MissionId and @HandlerId. These annotations apply to classes only and have to be provided for all mission and handler classes of an SCJ application.

3. Annotations that associate external events with the handlers that are released by them. These are @BoundEvent and @BoundEvents.

4. Annotations that specify action models for device access and hardware interaction code. These are @DeviceAccess and @InteractionCode.

In addition, we included an extra annotation @Ignore above to tag elements of the program that ought to be explicitly ignored during model construction. We apply it, for instance, to method parameters of type AperiodicEvent, which we do not model, or calls to super constructors of handlers. We observe that Java does not allow multiple annotations of the same type on an element, which is why we require @BoundEvents in addition to @BoundEvent. The former simply aggregates annotations of the latter type.

There are no annotations in group (1) to determine membership of classes to the categories SMMC and HC per se since this can be easily determined by examining the class types. Classes that are annotated by @InteractionClass are ignored by the translator.

We point out that our annotations at present assign handler and mission identifiers to classes rather than their instances. For the examples we consider, this is sufficient. The integration of instance-based identifiers is work in progress and complicated by the fact that Java does not permit the annotation of individual statements such as the construction of an object.

In group (4), the @DeviceAccess annotation allows us to define an action model for an explicit device or hardware access. For instance, in the cruise controller, we have the function writeVoltage() in the ThrottleController class, which communicates on the set\_voltage channel to output a voltage value to the throttle. The model of the device access is provided to the annotation as a String, by the model parameter. It usually is a prefix with possibly additional timing constraints attached to it. The annotation enables us to abstract from the low-level mechanics of the

<table>
<thead>
<tr>
<th>Java Annotation</th>
<th>Parameters</th>
<th>Determines</th>
</tr>
</thead>
<tbody>
<tr>
<td>@ActiveData</td>
<td>none</td>
<td>classes in category SMMC or HC</td>
</tr>
<tr>
<td>@PassiveData</td>
<td>none</td>
<td>classes in category DC</td>
</tr>
<tr>
<td>@InteractionClass</td>
<td>none</td>
<td>classes in category IC</td>
</tr>
<tr>
<td>@MissionId(id:String)</td>
<td>id – mission identifier</td>
<td>identifier of a mission class</td>
</tr>
<tr>
<td>@HandlerId(id:String)</td>
<td>id – handler identifier</td>
<td>identifier of a handler class</td>
</tr>
<tr>
<td>@BoundEvent(channel:String, type:String)</td>
<td>channel – name of the channel type – type of channel if present</td>
<td>external event bound to a handler</td>
</tr>
<tr>
<td>@BoundEvents</td>
<td>BoundEvent[] events – set of events</td>
<td>multiple events bound to a handler</td>
</tr>
<tr>
<td>@DeviceAccess(model:String)</td>
<td>model – Circus model of the access</td>
<td>action that models a device access</td>
</tr>
<tr>
<td>@InteractionCode(model:String)</td>
<td>model – Circus model if applicable</td>
<td>fields and methods for interaction code</td>
</tr>
<tr>
<td>@Ignore</td>
<td>none</td>
<td>explicitly ignored program elements</td>
</tr>
</tbody>
</table>

TABLE 9. Java annotations to configure the translation of SCJ programs.
isr

process. For instance, certain SCJ classes could automatize a significant portion of the annotation stage normally reveals whether there is a need for it. always be achieved by refactoring, and the annotation code is encapsulated cleanly into methods. This can statements, we generally require that such interaction alternatively, single missions. Since standard Java service routines, either for the entire application, or identifies methods that create and register interrupt interrupts and hardware devices and thus usually ignored. It applies to methods and fields and typically identifies methods that create and register interrupt service routines, either for the entire application, or alternatively, single missions. Since standard Java does not support the annotation of individual program statements, we generally require that such interaction code is encapsulated cleanly into methods. This can always be achieved by refactoring, and the annotation stage normally reveals whether there is a need for it. As suggested earlier on, it should be feasible to automate a significant portion of the annotation process. For instance, certain SCJ classes could by default be annotated as active objects, like those derived from Safelet, MissionSequencer, Mission, and so on. Other classes may similarly be automatically annotated as interaction classes, like those deriving from InterruptServiceRoutine. The identifiers for missions and handlers could, in principle, also be derived automatically. We observe, however, that the process could be challenging to automate as a whole due to the fact that human insight and understanding of the technology is required to specify the models for device interaction and to testify that the assumptions of atomic and instantaneous interactions are met.

In the next section we illustrate the use of the annotations presented above in the ACC.

The @InteractionCode annotation enables us to make a finer distinction in tagging parts of the program that correspond to code that is needed to configure interrupts and hardware devices and thus usually ignored. It applies to methods and fields and typically identifies methods that create and register interrupt service routines, either for the entire application, or alternatively, single missions. Since standard Java does not support the annotation of individual program statements, we generally require that such interaction code is encapsulated cleanly into methods. This can always be achieved by refactoring, and the annotation stage normally reveals whether there is a need for it.

As suggested earlier on, it should be feasible to automate a significant portion of the annotation process. For instance, certain SCJ classes could by default be annotated as active objects, like those derived from Safelet, MissionSequencer, Mission, and so on. Other classes may similarly be automatically annotated as interaction classes, like those deriving from InterruptServiceRoutine. The identifiers for missions and handlers could, in principle, also be derived automatically. We observe, however, that the process could be challenging to automate as a whole due to the fact that human insight and understanding of the technology is required to specify the models for device interaction and to testify that the assumptions of atomic and instantaneous interactions are met.

In the next section we illustrate the use of the annotations presented above in the ACC.

7.2. Example: the Cruise Controller

In the ACC program, the classes ACCSafelet and ACCMissionSequencer require only @ActiveData annotations. This is because they have very simple implementations that do not include any code related to interaction with hardware or configuration of interrupt service routines. More interesting is the class ACCMission, which is presented in Fig. 28. Apart from the initialize() and cleanup() methods called by the infrastructure to initialise and finalise the mission, several additional methods deal with the creation and registration of interrupt service routines (ISRs). The ISRs are held by the instance variables shaft_isr.
@InteractionClass
public class EngineISR extends InterruptServiceRoutine {
    protected final AperiodicLongEvent engine_event;

    public EngineISR(AperiodicLongEvent event) {
        super("EngineISR");
        engine_event = event;
    }

    public void handle() {
        disableInterrupts();
        /* Determine external event that raised the interrupt. */
        long cause = ...
        ;
        engine_event.fire(cause);
        /* Interrupts are re-enabled by the aperiodic handler. */
    }

    public void disableInterrupts() {
        /* Disable further interrupts from arriving. */
    }
}

FIGURE 29. Example of an interaction class (ISR) in the cruise controller application.

engine_isr, and so on. The fields are annotated with @InteractionCode since we do not model them in the generated Circus application process and OhCircus class. Here, the ISRs essentially fire aperiodic (long) events that are bound to the aperiodic handlers of the mission. An example of a class for an interrupt service routine is included in Fig. 29. The constructor of the class is parametrised in terms of the AperiodicLongEvent instance that must be fired when the interrupt occurs, and the handler code defined by the handle() method simply fires this event prior to determining the cause of the interrupt (the actual code for this is omitted).

We observe that the class EngineISR is annotated with @InteractionClass to determine its membership to the category IC of interaction classes; in the model generation process, it is thus ignored. Likewise, the four methods createEvents(), createISRs(), registerISRs() and unregisterISRs() defined inside the ACCMission class (Fig. 28) are annotated with @InteractionCode. This tells the translator that we do not model these methods either.

Importantly, the implementation of the EngineISR class justifies the assumptions we make about atomicity of interactions, modelled by synchronisations. We have a call to disableInterrupts() at the beginning of the interrupt handler to disable further interrupts from the engine to guarantee atomicity of the interaction (the actual code for this is omitted for brevity). We can moreover think of a few appropriate design patterns for the ISRs, but ultimately it is the obligation of the engineer to validate the assumptions. Although this is an important issue in its own right, a detailed discussion is beyond the scope and contribution of this article.

Apart from identifying interaction code, we also have to annotate the ACCMission class with the identifier of the mission (here ACCMId). Likewise, all handlers have to be annotated with the identifier of the respective handler. An example of an annotated handler class is presented in Fig. B.1 in Appendix B. We have an annotation @HandlerId to specify the unique identifier of the handler. In addition, the @BoundEvent annotation determines the external event that the handler is bound to. We recapture it below.

    @HandlerId("EngineHId")
    @BoundEvent(value="engine", type="boolean")
    public class Engine extends AperiodicLongEventHandler {
        ...
    }

External events that release the handler are synchronisations on the channel engine of type boolean. Apart from this, the handler also contains interaction code that is not modelled. This is the method enableInterrupts(), which reenables the interrupts after they have been disabled by the interrupt service routine. This design ensures that no external event can intervene between the occurrence of an interrupt and release of the corresponding handler. As noted before, it justifies our assumption of atomic interactions. We note that this mechanism is essential for the correctness of the program in general. In other words, it was not introduced for reasons of applying our technique.

A second annotation we require is on one of the parameters of the constructor, namely engine_event of type AperiodicLongEvent. This is because we do not model SCJ event classes. In the program, they are used merely as a means to an end: whereas interrupts represent the actual external
event being raised, instances of AperiodicEvent and AperiodicLongEvent are used to release the aperiodic handler that is associated with the event.

A more interesting example is the periodic handler ThrottleController. Here, we have an explicit external device access, namely to write out the voltage to the throttle. This is done by a method writeVoltage() from within the class. Fig. 30 recaptures the definition of this method. Most importantly, we have an annotation @DeviceAccess that specifies the action model for the device access: here an output prefix on set_voltage. We observe that the use of a try/catch statement in the method body is not in contradiction with the language constraints in Section 6.1.2 because we permit such statements in interaction code. Runtime exceptions should, however, not be thrown beyond the entry point of interaction methods. Program error exceptions may be thrown, though, and are modelled by the divergent action abort.

In summary, we conclude that specifying the annotations for the ACC inherently does not require notable expertise in the formal modelling notation. It merely requires the developer to identify code for interaction and device access. The annotation framework, due to its generality, also paves the way for custom extensions to treat other features of SCJ that are currently not catered for by our modelling approach. For instance, the @InteractionCode annotation may be used to specify the behaviour of code that utilises console I/O. The general benefit of our approach is that it allows us to abstract from the details of a piece of SCJ code (encapsulated in a method) by providing a specification of its behaviour as an action. Exploring this further is an interesting topic for future work.

7.3. Implementation Issues

The translator takes as its input the annotated SCJ program, as for now we do not provide any support for automating the annotation process. In order to match the high-level translation rules (Appendix C), the tool has to determine the superclasses and implemented interfaces of active classes, namely those annotated with @ActiveData and thus belonging to either SMMC or HC. We recall that our annotations do not encode the precise type of an SCJ application class. Specifically, the type can be extracted from the annotated syntax tree that is obtained using the Compiler API of the JDK 7. We extend this analysis further by verifying the constraints defined in Section 6.1 and the consistency of the annotations introduced. Inconsistencies or violations detected by the tool are reported to the user and abort the model generation process. Such failures normally reveal the need for refactoring the code and reviewing the annotations that have been inserted. The main challenge is to determine whether methods require action models or can be given a model as a data operation. In general, action models are required for the following types of methods.

1. Methods that are called by the SCJ infrastructure. These are typically methods that override classes or interfaces of the SCJ component framework.
2. Methods that carry out device or hardware accesses and, therefore, are correspondingly annotated.
3. Methods that call, directly or indirectly, other methods that requires an action model.

With regards to (1), we can easily determine methods that fall into this category by examining their name and signature. For (2), we can determine the relevant methods by probing type information in the annotated syntax tree of the program, as this information retains annotations defined on the various kinds of program elements. In order to determine methods of the third type above, we have to perform a control flow analysis based on the call-dependency of methods. For this, we have implemented a general utility to encode binary relations over arbitrary types and to facilitate efficient calculation of their closure. Hence, it is possible to automate the decision whether a method requires an action model, eliminating the need for annotations.

Model generation combines Stage (2) and Stage (3) of the translation process. For technical reasons, we do not rewrite the code in Stage (2), but directly define translation rules that take the rewrite rules in Fig. 6 into account during low-level statement translation. APIs
for automatic code rewriting exist [49], but their use introduces unnecessary complexity in our tool.

Our tool consists of a number of components that perform essential processing tasks. They are illustrated in Fig. 31. The compiler package addresses the parsing and type-checking of the SCJ program; it uses existing JDK tools. The analysis package provides a facility for analysing the parsed program; it infers and records information that is later needed for the translation. The checker package performs a validity check of the SCJ program to ensure it belongs to the subset of translatable programs as defined in Section 6.1. The modelgen package provides components that carry out the actual generation of the model. Finally, apart from the four packages above, we also have the application package, which includes the top-level tool application, as well as the utils package, which provides various collections of utility functions. The remaining packages collections and comparators extend the Java collection API, most notably with an efficient implementation of mathematical relations.

The translator itself is implemented by virtue of a framework that realises a plugin architecture. The translator as a whole therefore consists of a collection of smaller translator plugins. Each translator plugin caters for the construction of a particular part of the model and exhibits a dependency on other translator plugins that have to be executed before it. Hence, we have, for instance, plugins that cater for the definition of channels, the introduction of axiomatic constants for handler and mission identifiers, and the construction of processes for active components and OhCircus classes for data objects. Translator plugins are provided by implementing an interface Translator in our tool framework: the implementation determines applicability of the translator, dependency to other translators, and the actual output produced, as well as the file(s) to which the output is appended.

**High-level Translation.** High-level translation implements the rules in Appendix C (there is a plugin for each rule). The plugins make use of string templates and the FreeMarker library. String templates, in general, offer a clean way of isolating static and dynamic aspects of any kind of textual patterns. Here, in particular, they offer traceability to the formal specification of the rules. Template models, which are certain kinds of classes of the FreeMarker API, make dynamic information available from within the templates that is needed by the rules, such as the functions IdOf, TypeOf or BoundEvents used in the right-hand side of the high-level translation rules. We take advantage here of the expressibility and extensibility of the FreeMarker template language to deal with special cases, and hence reduce the number of rules potentially needed.

**Low-level Translation.** Low-level translation realises the translation of statements, expressions, values and types. Although we specify these as templates as before, the translation is driven by visitors, which are used by the high-level translator plugins. Visitors are a general design pattern that supports the traversal of tree structures, and the JDK Compiler API comes with its own implementation of the pattern. We make use of two visitors, one that produces an action model and one that produces a data operation (OhCircus method).

Overall the translation process and tool seem to be robust and stable. Clean and sound software design principles, which isolate concerns like parsing, analysis, validation and translation into loosely-coupled components, ensure that the tool can be easily extended and modified, satisfying future needs of further elaborating our models by including features of SCJ that are currently not supported.
8. CONCLUSION

As far as we know, what we have presented here is the first formalisation of the SCJ paradigm. Our models capture the essence of its design, and are an essential asset for analysis and development techniques for SCJ programs based on refinement. There are a number of refinement-based techniques that are enabled by the availability of a formal model of SCJ in a state-rich process algebra. Particular techniques for Circus are reported in [21, 39, 50, 51], and techniques for languages of the same line are also reported in [52, 53, 54, 55]. The translation of the Circus model works with tools supporting these techniques is a much easier exercise than the translation from the SCJ program directly.

Our models are in line with the SCJ technology specification in the absence of deadline-miss situations, which we do not consider. We hence assume that scheduling analysis and environmental assumptions about external interactions ensure that these situations essentially cannot occur. Imperfection or imprecision of timing evidence therefore already has to be accounted for at the level of scheduling analysis, which is currently a caveat for using our models.

A notable achievement is our solution to encode active class behaviour and data objects as independent dimensions. This increases the modularity of models and provides opportunities for modular reasoning, but also emphasises the need for an integrated formalism including constructs of OhCircus and Circus Time.

To validate the framework and application models, we have translated the respective Circus processes into pure CSP models, which we then submitted to the FDR [33] model checker. The CSP translation encapsulates all Circus state into process parameters. Timing aspects are ignored, and so is the detailed application-level behaviour of handlers. Apart from this, the CSP model retains exactly the structure of the corresponding Circus model. CSP processes, like handlers_field below, are used to encapsulate individual state components of a Circus process.

\[
\begin{align*}
\text{channel handlers_get : Set(HandlerId)} \\
\text{channel handlers_set : Set(HandlerId)} \\
\text{handlers_field}(v) = \\
\quad \text{handlers_get!}v \rightarrow \text{handlers_field}(v) \quad \square \\
\quad \text{handlers_set?}v \rightarrow \text{handlers_field}(v)
\end{align*}
\]

The CSP process \(\text{handlers_field}(v)\) encapsulates, for instance, the state component \(\text{handlers}\) of the process MissionFW in Fig. 10, where \(v\) determines its initial value. Channel communications on \(\text{handlers_get}\) and \(\text{handlers_set}\) are now used to read and write to the state component. For each state component of a Circus process, we define a CSP process similar in shape to \(\text{handlers_field}(v)\). Their parallel composition yields a model for the entire state, and that model is further composed with a translation of the local actions and main action of the Circus process. (Local definitions can be easily supported in CSP via \text{let} constructs.)

The resulting CSP process, after hiding the channels used for reading and modifying state components, exhibits precisely the behaviour of the original Circus process under CSP's failure-divergence semantics, and besides is amenable to model checking and, in addition, animation via tools such as FDR [33] and ProB [56].

Properties that we examined and validated are deadlock freedom and termination of several simplified application scenarios. Carrying out these checks for the entire ACC model would have been theoretically possible, but is thwarted by the complexity of the CSP models due to state explosion. Assertions of the following form have been used to establish termination:

\[
\text{skip} \sqsubseteq_{PD} (\text{System [Events]} \setminus \text{TestEnv}) \setminus \text{Events}
\]

The System process refers to the process of the SCJ application, and Events are the channels used for external interactions. The TestEnv process provides a testing environment for the application scenario that interacts through the external channels.

Our validation efforts proved to be valuable in identifying subtle issues in earlier versions of our models. For instance, in the MissionFW process in Fig. 10, we formerly made use of an interrupt \((\ldots) \triangle \text{initializeRet}, \text{mission} \rightarrow \text{skip}\) in the Initialize action to terminate that action. Model checking revealed a race condition that can result in a registered handler not being recorded in the state. Problems like these are difficult to diagnose \textit{a posteriori} using testing-based validation approaches due to the amount of nondeterminism in SCJ program executions, as it naturally arises from the parallelism of handlers. Our models are essentially modular, and this enables and facilitates model checking to focus on particular parts of the model in isolation, both in terms of the framework and application processes.

More generally, there are nonetheless limitations to translating Circus into CSP. These apply, in particular, when modelling composite values and data operations. In our case, however, we could, model the entire SCJ framework. The feedback we obtained using FDR increases the confidence in our models; this is further enhanced by the many discussions we had with experts in the SCJ technology.

To validate the tool, we have used it to generate the model of the ACC. This produces a Circus model that can be parsed and type-checked. The implementation of the tool \textit{per se} supports our claim that models can be generated automatically. We are currently evaluating and testing the tool with further examples, in particular the collision detector in [36].

The direct correspondence between SCJ programs and our models enables automation in both directions: the framework processes are the same for all programs, and the application processes use a fixed modelling pattern. As part of our wider research agenda, we
are also developing a complementary tool that translates Circus models into SCJ programs. That tool will be useful if no implementation is a priori given, but can be designed ad lib from a specification. The reason we did not develop that tool first is that our current work is illuminating in identifying the features of SCJ that can be supported by our formalisms.

Related Work. Although there are many approaches and tools to reason about object-oriented programs and Java [57, 58], they do not cater for the specificities of concurrency in SCJ. Brooke et al. present a CSP specification for a concurrency model for Eiffel (SCOOP) [59]. Their CSP specification shares some basic ideas with our Circus models, but is necessarily more complex due to its generality. A recent work [60] examines test generation with strong coverage criteria; part of it is a formal specification of classes and methods in the Real-Time Java API.

Kalibera et al. [61] are concerned with scheduling and race conditions in SCJ programs, but do not use proof-based techniques. Instead, exhaustive testing and model checking is applied.

Annotation-based techniques for SCJ can be found in [18, 62]. In [18] annotations are used to check for compliance with a particular level of SCJ, and for safe use of memory. Haddad et al. define SafeJML [62], which extends JML [57] to cover timing properties. It reuses existing technology for worst-case execution-time analysis in the context of SCJ. Our model is a conceivable candidate to justify the soundness of checks supported by the annotations and tools above.

Future Work. Our primary future work is to elaborate the model and translation to account for additional features of SCJ that for now have been ignored. This is, in particular, memory management, timing-related classes, and the support for active objects, that is, data objects that interact with either the hardware or framework. So far we have excluded this possibility as it did not arise in our examples, but one might envisage cases where support for such objects is desirable, like, for instance, a file class that represents data and at the same time interacts with a physical disk. We are currently considering a solution that provides a limited facility to model data objects as a combination of class and process, just like active components of the SCJ mission model. Additional restrictions to be imposed on such objects are still largely an open issue.

Another future work is to tackle issues of robustness by dealing with missed deadlines. SCJ offers support to detect and react to such situations in the program. Or models, however, currently do not formally capture this feature, mostly as it appears to be more challenging to integrate and we do not have SCJ applications that exploit it. Modelling it, however, enables the support for a larger class of implementations.

Our structural constraints restrict program designs. In particular, they prevent us from making effective use of subclassing where SCJ components are involved. This may have implications on modularisation and reuse of verification arguments, for instance, in view of product lines. We also hope to address this issue in future research once more experience has been gained in constructing verification arguments.

Our long term goal is the definition of refinement-based techniques for SCJ program development. Like in the Circus standard technique [21], we will devise a refinement strategy to transform centralised abstract Circus Time models into an SCJ model as described here. The development of this strategy, and the proof of the refinement rules that it will require are a challenging aspect of this endeavour; initial results have been published in [35]. This involves the identification of refinement and modelling patterns. All this shall also provide further practical validation of our model.

ACKNOWLEDGEMENTS

We are grateful to Chris Marriott, Kun Wei, and Jim Woodcock for useful discussions of our models. This work is funded by the EPSRC grant EP/H017461/1.

REFERENCES


APPENDIX A. CHANNELS USED IN THE CRUISE CONTROLLER MODEL

<table>
<thead>
<tr>
<th>Channel</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wheel_shaft</td>
<td>–</td>
<td>occurs with each rotation of the wheel shaft</td>
</tr>
<tr>
<td>engine_on</td>
<td>–</td>
<td>engine is switched on</td>
</tr>
<tr>
<td>engine_off</td>
<td>–</td>
<td>engine is switched off</td>
</tr>
<tr>
<td>brake</td>
<td>boolean</td>
<td>brake pedal is pressed or released</td>
</tr>
<tr>
<td>top_gear_engaged</td>
<td>–</td>
<td>driver switches into top gear</td>
</tr>
<tr>
<td>top_gear_disengaged</td>
<td>–</td>
<td>driver switches out of top gear</td>
</tr>
<tr>
<td>lever</td>
<td>LEVER</td>
<td>driver operates the command lever</td>
</tr>
<tr>
<td>set_voltage</td>
<td>0.80</td>
<td>sets the voltage on the throttle actuator</td>
</tr>
</tbody>
</table>

**TABLE A.1.** Channels for external events of the cruise controller model.

<table>
<thead>
<tr>
<th>Method</th>
<th>Channel(s)</th>
<th>Class or Interface</th>
<th>Target</th>
<th>Param</th>
<th>Return</th>
</tr>
</thead>
<tbody>
<tr>
<td>setUp</td>
<td>Call/Ret</td>
<td>Safelet</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>tearDown</td>
<td>Call/Ret</td>
<td>Safelet</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>getNextMission</td>
<td>Call/Ret</td>
<td>MissionSequencer</td>
<td>–</td>
<td>–</td>
<td>MissionId</td>
</tr>
<tr>
<td>initialize</td>
<td>Call/Ret</td>
<td>Mission</td>
<td>MissionId</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>cleanup</td>
<td>Call/Ret</td>
<td>Mission</td>
<td>MissionId</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>requestTermination</td>
<td>Call/Ret</td>
<td>Mission</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>terminationPending</td>
<td>Call/Ret</td>
<td>Mission</td>
<td>–</td>
<td>–</td>
<td>boolean</td>
</tr>
<tr>
<td>register</td>
<td>Managed</td>
<td>EventHandler</td>
<td>HandlerId</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

Above Chan[Call/Ret] abbreviates a channel pair ChanCall and ChanRet.

**TABLE A.2.** Channel pairs for infrastructure methods.

The types of the channels in Table A.2 are determined by the classes that include the methods, and the types of their possible parameters and return values. The purpose of the target parameter is to disambiguate the use of the channel in the context of multiple objects. If there are no parameters or return values, the types simplify to Target. And if the method is only called with the same object as a target, the channels become typeless thus representing simple synchronisations.
APPENDIX B. SCJ PROGRAM CODE

```java
@HandlerId("EngineHId")
@BoundEvent(channel = "engine", type = "boolean")
public class Engine extends AperiodicLongEventHandler {
    private Controller cruise;

    public Engine(Controller cruise, @Ignore AperiodicLongEvent engine_event) {
        super(...);
        this.cruise = cruise;
    }

    public void handleAsyncLongEvent(long param) {
        int event = (int) param;
        switch (event) {
            case ENGINE_ON:
                cruise.engineOn();
                break;
            case ENGINE_OFF:
                cruise.engineOff();
                break;
        }
        enableInterrupts();
    }

    @InteractionCode
    public void enableInterrupts() {
        /* Program code to re-enable interrupts. */
    }
}
```

FIGURE B.1. Annotated version of the Engine handler class.

APPENDIX C. HIGH-LEVEL TRANSLATION RULES

We use three auxiliary functions in the high-level translation rules for SCJ components.

1. IdOf(type) yields the identifier of a mission or handler class;
2. TypeOf(obj) infers the type of a Java object; and,
3. BoundEvents(type) determines the external events bound to an aperiodic event handler.

```plaintext
\[
\begin{align*}
\text{class } \texttt{CName} & \text{ implements } \texttt{Safelet} \{ \\
& \texttt{FieldDecl} \\
& \texttt{public } \texttt{CName()} \{ \texttt{InitStmts} \} \\
& \texttt{AMethDecl1} \\
& \texttt{AMethDecl2} \\
& \ldots \\
& \texttt{public MissionSequencer getSequencer()} \{ \\
& \quad \texttt{return new MSName();} \\
& \} \\
\} \\ \\
\end{align*}
\]

\[
\begin{align*}
\text{process } \texttt{[CName]} & \texttt{_{Name App}} \cong \text{begin} \\
\text{state } & \texttt{State} \equiv \texttt{[this : [CName]} \texttt{_{Name Class}]} \\
\text{Init} \equiv & \texttt{[State | this’ = new [CName]} \texttt{_{Name Class}]} \\
& \texttt{[AMethDecl1]_{AMethod}} \\
& \texttt{[AMethDecl2]_{AMethod}} \\
& \ldots \\
\text{Methods} \equiv & \texttt{\left( \mu X \bullet \left( \texttt{[AMethDecl1]}_{x_{\text{num}}, \text{meth}} \bullet \texttt{[AMethDecl2]}_{x_{\text{num}}, \text{meth}} \right) ; X \right)} \\
& \bullet \texttt{Init} ; \texttt{(Methods } \triangleq \texttt{end_safelet_app } \rightarrow \texttt{skip)} \\
\end{align*}
\]

FIGURE C.1. Translation rule for classes implementing the Safelet interface.
FIGURE C.2. Translation rule for classes extending the MissionSequencer class.

FIGURE C.3. Translation rule for classes extending the Mission class.

FIGURE C.4. Translation rule for classes extending the AperiodicEventHandler class.
FIGURE C.5. Translation rule for classes extending the `PeriodicEventHandler` class.
APPENDIX D. LOW-LEVEL TRANSLATION RULES

**TABLE D.1.** Translation rules for Java types.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
<th>Addendum</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR1</td>
<td>boolean</td>
<td>boolean</td>
<td>where boolean ::= TRUE</td>
</tr>
<tr>
<td>TR2</td>
<td>byte</td>
<td>byte</td>
<td>where byte (\equiv -128 \ldots 127)</td>
</tr>
<tr>
<td>TR3</td>
<td>short</td>
<td>short</td>
<td>where short (\equiv -2^{15} \ldots 2^{15} - 1)</td>
</tr>
<tr>
<td>TR4</td>
<td>int</td>
<td>int</td>
<td>where int (\equiv -2^{31} \ldots 2^{31} - 1)</td>
</tr>
<tr>
<td>TR5</td>
<td>long</td>
<td>long</td>
<td>where long (\equiv -2^{63} \ldots 2^{63} - 1)</td>
</tr>
<tr>
<td>TR6</td>
<td>char</td>
<td>char</td>
<td>where char (\equiv 0 \ldots 2^{16} - 1)</td>
</tr>
<tr>
<td>TR7</td>
<td>float</td>
<td>float</td>
<td>where float is a given type</td>
</tr>
<tr>
<td>TR8</td>
<td>double</td>
<td>double</td>
<td>where double is a given type</td>
</tr>
<tr>
<td>TR9</td>
<td>RefType</td>
<td>RefType</td>
<td>where RefType is a reference type</td>
</tr>
</tbody>
</table>

**TABLE D.2.** Translation rules for literal Java values.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>VR1</td>
<td>([0, 1, 2, \ldots])Value</td>
<td>(0, 1, 2, \ldots)</td>
<td>unsigned numbers</td>
</tr>
<tr>
<td>VR2</td>
<td>([0, -1, -2, \ldots])Value</td>
<td>(0, -1, -2, \ldots)</td>
<td>signed numbers</td>
</tr>
<tr>
<td>VR3</td>
<td>trueValue</td>
<td>TRUE</td>
<td>boolean value true</td>
</tr>
<tr>
<td>VR4</td>
<td>falseValue</td>
<td>FALSE</td>
<td>boolean value false</td>
</tr>
<tr>
<td>VR5</td>
<td>('[c]'Value</td>
<td>ord(c)</td>
<td>where ord(c) gives the unicode of character c</td>
</tr>
<tr>
<td>VR6</td>
<td>&quot;Foo&quot;Value</td>
<td>(\langle 'F', 'o', 'o' \rangle)</td>
<td>strings are encoded as sequences</td>
</tr>
<tr>
<td>VR7</td>
<td>nullValue</td>
<td>null</td>
<td>encodes null-reference for data objects</td>
</tr>
</tbody>
</table>

**TABLE D.3.** Translation rules for Java expressions.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>ER1</td>
<td>ValueExpr</td>
<td>Value</td>
<td>where Value is a literal value</td>
</tr>
<tr>
<td>ER2</td>
<td>UnaryOpExpr</td>
<td>UnOp</td>
<td>where UnaryOp is a unary operator</td>
</tr>
<tr>
<td>ER3</td>
<td>Expr BinOp Expr</td>
<td>BinOp</td>
<td>where BinOp is a binary operator</td>
</tr>
<tr>
<td>ER4</td>
<td>(\star)Expr, (-)Expr, (\ast)Expr, (\ast)Expr, (\ast)Expr</td>
<td>+, -, *, ...</td>
<td>arithmetic operators</td>
</tr>
<tr>
<td>ER5</td>
<td>[]Expr, [], []Expr</td>
<td>&amp;, \lor, \neg</td>
<td>translation of logical operators</td>
</tr>
<tr>
<td>ER6</td>
<td>Expr ? Expr : Expr</td>
<td>if Expr then Expr else Expr</td>
<td>translation of conditional expressions</td>
</tr>
<tr>
<td>ER7</td>
<td>Obj.Meth(Args)</td>
<td>Obj</td>
<td>side-effect free call on a data object</td>
</tr>
<tr>
<td>ER8</td>
<td>((Arg1, Arg2, \ldots))Expr</td>
<td>((Arg1)Expr, (Arg2)Expr, ...)</td>
<td>translation of argument tuples</td>
</tr>
</tbody>
</table>
We note that in FR3, we ignore the expression $Expr$ initialising the variable since at this point we only consider the default initialisation of variables; the function $\ldots [FieldDecl]$ deals with explicit initialisations separately.

TABLE D.4. Translation rules for field declarations.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>FR1</td>
<td>$\text{FieldName}:\text{FieldType}$</td>
<td>$\text{FieldName}:\text{FieldType}$</td>
</tr>
<tr>
<td>FR2</td>
<td>$\text{AccessType}:\text{FieldName} = \text{Expr}$</td>
<td>$\text{FieldName}:\text{Name} = \text{FieldType}:\text{Type}$</td>
</tr>
<tr>
<td>FR3</td>
<td>$\text{AccessType}:\text{FieldName} = \text{Expr}$</td>
<td>$\text{FieldName}:\text{Name} = \text{FieldType}:\text{Type}$</td>
</tr>
</tbody>
</table>

TABLE D.5. Supplementary translation rules for Java statements.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR7</td>
<td>$[\\text{Stmts}]$ (empty list of statements)</td>
<td>skip</td>
</tr>
<tr>
<td>SR8</td>
<td>$[\text{Stmts}_1; \text{Stmts}_2; \text{Stmts}]$</td>
<td>$[\text{Stmts}_1; \text{Stmts}_2; \text{Stmts}]$</td>
</tr>
<tr>
<td>SR9</td>
<td>$\lbrace \text{Stmts} \rbrace$ (statement block)</td>
<td>$[\text{Stmts}]$</td>
</tr>
<tr>
<td>SR10</td>
<td>$\lbrace \text{Stmts}_1; \text{Expr}; \text{Stmts}_2 \rbrace \text{Stmts}$</td>
<td>$[\text{Stmts}_1; \text{Stmts}_2; \text{Expr}; \text{Stmts}_3]$</td>
</tr>
</tbody>
</table>

The function $TypeOf(\text{Obj})$ determines the type of an object, and $\text{IdOf}$(type) the mission or handler identifier of a class type.

TABLE D.6. Translation rules for calls to interacting methods.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR11</td>
<td>$\lbrace \text{ObjMeth(Args)} \rbrace$</td>
<td>$\lbrace \text{Meth} \rbrace$ Name Call $\lbrace \text{Args} \rbrace$ Expr $\rightarrow$ $\lbrace \text{Meth} \rbrace$ Name Ret $\rightarrow$ skip</td>
</tr>
<tr>
<td>SR12</td>
<td>$\lbrace \text{Var = ObjMeth(Args)} \rbrace$</td>
<td>$\lbrace \text{Meth} \rbrace$ Name Call $\lbrace \text{Args} \rbrace$ Expr $\rightarrow$ $\lbrace \text{Meth} \rbrace$ Name Ret $\rightarrow$ $\lbrace \text{Var} \rbrace$ Name $\rightarrow$ ret</td>
</tr>
<tr>
<td>SR13</td>
<td>$\lbrace \text{ObjMeth(Args)} \rbrace$</td>
<td>$\lbrace \text{Meth} \rbrace$ Name Call $\lbrace \text{IdOf}$(TypeOf(Obj)) $\rbrace$ $\lbrace \text{Args} \rbrace$ Expr $\rightarrow$ $\lbrace \text{Meth} \rbrace$ Name Ret $\rightarrow$ $\lbrace \text{Var} \rbrace$ Name $\rightarrow$ ret</td>
</tr>
<tr>
<td>SR14</td>
<td>$\lbrace \text{Var = ObjMeth(Args)} \rbrace$</td>
<td>$\lbrace \text{Meth} \rbrace$ Name Call $\lbrace \text{IdOf}$(TypeOf(Obj)) $\rbrace$ $\lbrace \text{Args} \rbrace$ Expr $\rightarrow$ $\lbrace \text{Var} \rbrace$ Name $\rightarrow$ ret</td>
</tr>
</tbody>
</table>

The function $\text{Class}$ is a safelet or mission sequencer class.

TABLE D.7. Translation rules for the creation of active objects.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Application</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR15</td>
<td>$\lbrace \text{Var = new Class(Args)} \rbrace$</td>
<td>$\lbrace \text{Var} \rbrace$ Name $\rightarrow$ new $\lbrace \text{Class} \rbrace$ Name $\rightarrow$ Class $\lbrace \text{Args} \rbrace$ Expr</td>
</tr>
<tr>
<td>SR16</td>
<td>$\lbrace \text{Var = new Class(Args)} \rbrace$</td>
<td>$\lbrace \text{Var} \rbrace$ Name $\rightarrow$ new $\lbrace \text{Class} \rbrace$ Name $\rightarrow$ Class $\lbrace \text{Args} \rbrace$ Expr; $\lbrace \text{Class} \rbrace$ Name Init $\rightarrow$ $\lbrace \text{Var} \rbrace$ Name $\rightarrow$ skip</td>
</tr>
</tbody>
</table>