Using *Circus* for Safety-critical Applications

J. C. P. Woodcock\(^1,\)\(^2\)

**Abstract**

*Circus* is a language that unifies Z, CSP, and the refinement calculus, and we describe its application in the development of safety-critical systems. We show the descriptive power of *Circus* with a fragment of the formalisation of the steam boiler problem. We then use *Circus*’s refinement calculus to bridge a semantic gap in development, where we eliminate a kind of abstract event.

**Keywords:** Unifying theories of programming, the Z notation, Communicating Sequential Processes (CSP), the refinement calculus, *Circus*, synchronisation protocols.

1 Introduction

The *Circus* notation [31,33,12,13] is being used in the development and verification of safety-critical systems. It is a semantic compound of Z [6,28,29,34], CSP [15,22], the Z refinement calculus [7,11], and the guarded-command language [14], providing a framework in which to discuss the correctness of state-based reactive systems; extensions are under development to include aspects of object orientation [10], time [25,26,27], probability, and lock-step synchrony.

In this paper, we illustrate the use of *Circus* by discussing a case study: the steam boiler, now a standard benchmark for formal methods [5,1,2]. In particular, we focus on an interesting “semantic gap”. In CSP, an abstraction is sometimes employed in which atomic synchronisations can be system-wide, between many processes, rather than being restricted to only two participants.

---

\(^1\) The WMF’2003 Formal Methods Europe Lecturer (www.fmeurope.org).

\(^2\) Email: J.C.P.Woodcock@kent.ac.uk
We deal with a simple instance of this phenomenon, which serves to show the power of Circus’s calculational approach to reasoning about reactive systems.

2 Circus

Processes in Circus are reactive and encapsulate state variables; the reactive behaviour is described using CSP, and states and their transitions are described in Z. Circus focuses particularly on techniques for refinement [8,9,24]. An objective is to use Circus to calculate reactive systems in a style reminiscent of the sequential refinement calculi of Back [4], Morgan [19], and Morris [20].

As a simple example of a Circus process, consider the modelling of a bank account. The environment can interact with this process through four channels: to open the account; to check the current balance; to deposit money; and to withdraw money. When the account is opened, an initial deposit is made and an overdraft limit is established. The description starts with the declaration of these four channels, with their types.

\[
\text{channel open : } \mathbb{N} \times \mathbb{N}; \text{ balance, deposit, withdraw : } \mathbb{N}
\]

The process consists of a series of paragraphs that introduce the state and various actions on the state; these declarations are given in a mixture of Z and CSP, and are protected from the outside world by the process’s encapsulation. The extensional behaviour is given by the main action.

\[
\text{process BankAcc } \triangleq \\
\text{begin}
\]

\[
\text{state Acc } \triangleq [b : \mathbb{Z}; o,f : \mathbb{N} \mid f = o + b]
\]

\[
\text{Init } \triangleq [\text{Acc} ; \text{init}_b?, \text{init}_o? : \mathbb{N} \mid b' = \text{init}_b? \land o' = \text{init}_o?]
\]

\[
\text{Deposit } \triangleq \text{deposit}? v \rightarrow b := b + v
\]

\[
\text{Deduct } \triangleq (a : \mathbb{N} \triangleright a \leq f \triangleleft b := b - a)
\]

\[
\text{Withdraw } \triangleq \text{withdraw}? v \rightarrow \text{Deduct}(v)
\]

\[
\text{Balance } \triangleq \text{balance}! b \rightarrow \text{Skip}
\]

\[
\text{main}
\]

\[
\text{open}? (\text{init}_b, \text{init}_o) \rightarrow \text{Init};
\]

\[
\mu X \triangleright (\text{Deposit} \triangleright \text{Withdraw} \triangleright \text{Balance}); X
\]

\[
\text{end}
\]
The state of the bank account contains the balance $b$, the overdraft limit $o$, and the funds available $f$, which is always fixed to be the sum of the balance and the overdraft limit. The value of $o$ is a limit, in the sense that $f$ must never be allowed to become negative. The main action ensures that the account is opened before it is used. The environment must supply the initial balance and the overdraft limit, after which the state is updated according to the initialisation schema $Init$. Notice that the variables bound by the communication ($init_b$ and $init_o$) are referred to as inputs to $Init$. Next, the process repeatedly offers the environment a choice of actions: to deposit, to withdraw, or to check the account’s balance. The $Deposit$ action is activated by a communication on the $deposit$ channel; the balance is updated accordingly. $Withdraw$ is similar, except that the action uses another, parametrised action $Deduct$, which contains a guard: if the amount to be deducted is greater than the funds available, then the action deadlocks. This example of reactive behaviour is impossible to express in the Oxford-style of using $Z$ [34].

The semantics of $Circus$ [33] follows Hoare & He’s unifying theories of programming [16]: each construct in the language is given a denotational semantics in a predicative style in an alphabetised extension of Tarski’s relational calculus. The language corresponds to their model in the imperative, reactive subtheory, and provides the setting for an extensive refinement calculus.

3 A safety-critical application: the steam boiler

The problem given in [5] is to model a steam boiler, where water is removed from the boiler at a measured rate, and replaced by the action of four pumps delivering a supply from a reservoir of water. Such devices are important components of nuclear reactor systems, amongst other things. The steam boiler’s controller is given the task of maintaining the boiler’s water level within the range $N_1..N_2$, and to shut the system down if there is a risk that the water level could go outside the wider bounds $M_1..M_2$. If the wider bounds are exceeded, then there is a possibility of flooding the boiler or allowing it to boil dry, either of which might lead to an accident with unacceptable consequences.

$Circus$ has been used to describe the steam boiler in [32]. In that paper, an interesting separation is made between handling messages with complex data from sensors, and the rather simpler finite-state machine that controls the boiler’s operation, in a manner reminiscent of abstract interpretation. This separates the question of validating the controller’s interface from the question of verifying its correctness.

In this paper we use another formalisation based on that of O’Halloran [21]. In his work, the approach to identifying critical requirements is to express
functional requirements as firing rules, of the form “if \( a \) then \( b \)”, where event \( a \) enables event \( b \), subject to environmental constraints. The implicit inference engine defined by these firing rules is non-monotonic, as it must forget previously inferred facts as the system evolves.

The model of the steam-boiler plant and the inference engine share communication channels that represent communications with actuators and sensors in the real system. The plant consists of a number of components, and we give a brief description of some of them: the water reservoir, the boiler, and a sensor. The reservoir is a model of the body of water that the pumps feed, and that the boiler turns into steam by heating, according to the dynamics of the system. First, the quantity in the body of water, the state variable \( L \), is set to an arbitrary initial level between \( N_1 \) and \( N_2 \).

\[
\begin{align*}
\text{process } \text{Water} & \equiv \\
& \text{begin main} \\
& \text{var set} : \mathbb{P} \text{Source, } L : \mathbb{N} \bullet \\
& \text{set} := \text{Source}; \ L \in N_1 \ldots N_2; \\
& \mu X \bullet \min < L < \max & \text{write?} x : \text{set}\? \delta \rightarrow \\
& \text{set, } L := \text{set} \setminus \{x\}, L + \delta; \ X \\
& \varnothing \\
& \text{set} = \emptyset & \land \min < L < \max & \text{read.sensor!} L \rightarrow \\
& \text{tock} \rightarrow \\
& \text{set} := \text{source}; \ X \\
& \varnothing \\
& \text{set} = \emptyset & \text{tock} \rightarrow \text{set} := \text{source}; \ X \\
& \varnothing \\
& L \leq \min & \text{boom} \rightarrow \text{Stop} \\
& \varnothing \\
& L \geq \max & \text{flood} \rightarrow \text{Stop} \\
& \varnothing \\
& \text{emergency-stop} & \text{Emergency-stop}
\end{align*}
\]
The process maintains two state variables: a set of water sources, and the water level in the boiler. Time moves forward whenever the clock tocks; within each time period, water is transferred from each source. Once all the sources have been accounted for, the current level is output on the channel \textit{read.sensor}. If the level drops below the minimum, there is an explosion, signalled by the event \textit{boom}; if it goes above the maximum, there is another catastrophic event \textit{flood}. The process shuts down following the emergency stop event.

Next, we model the action of the boiler as a separate process that interacts with the body of water. The boiler consumes \( v \) litres of water in each time period, and communicates this fact to \textit{Water}.

\[
\text{Boiler} \triangleq \begin{array}{l}
\text{begin} \\
\text{write.boiler.}(-v) \rightarrow \text{tock} \rightarrow \text{Boiler} \end{array}
\]

Finally, we model the behaviour of a sensor, which interacts with the body of water, and emits events that abstract the state of the boiler.

\[
\text{process Sensor} \triangleq \\
\text{begin main} \\
\mu X \bullet \text{tock} \rightarrow \text{tock} \rightarrow \text{tock} \rightarrow \text{tock} \rightarrow \text{read.sensor}?L : \mathbb{N} \rightarrow \\
\hspace{1cm} L < M_1 \& \text{level.lt}_M_1 \rightarrow X \\
\hspace{1cm} \Box \\
\hspace{1cm} M_1 \leq L < N_1 \& \text{level.lt}_N_1 \rightarrow \text{tock} \rightarrow X \\
\hspace{1cm} \Box \\
\hspace{1cm} N_1 \leq L \leq N_2 \& \text{level.between}_N_1N_2 \rightarrow \text{tock} \rightarrow X \\
\hspace{1cm} \Box \\
\hspace{1cm} N_2 < L \leq M_2 \& \text{level.gt}_N_2 \rightarrow \text{tock} \rightarrow X \\
\hspace{1cm} \Box \\
\hspace{1cm} M_2 < L \& \text{level.gt}_M_2 \rightarrow \text{tock} \rightarrow X
\end{array}
\]

Every fourth time period, the sensor takes a reading from the water level and enables an appropriate event.

Although we have shown only a small part of the specification of the steam boiler, it is sufficient to demonstrate the approach. The model consists of a number of parallel processes interacting through shared channels and events. We would like to be able to implement this model as a controller for a real steam boiler. A suitable language for this implementation is \textit{occam}, given
its close relationship with CSP; however, we immediately face a semantic gap: CSP allows the synchronisation of events to be between many processes, but *occam* restricts this, for efficiency reasons, to just two participants. In the next section, we apply *Circus’s* refinement calculus to bridge this semantic gap for a specific kind of multi-way synchronisation.

### 4 A simple protocol for multi-way synchronisation

Suppose that we have a collection of parallel processes indexed over $I$, that each process repeatedly executes some individual transaction, represented by the event $t.i$, and that we synchronise the transactions by alternating them with the globally shared event $m$. This is modelled by the *Circus* process:

\[
( \parallel_{\{m\}} i : I \bullet ( \mu X \bullet m \rightarrow t.i \rightarrow X ) ) \ \setminus \ \{m\}
\]

This is the parallel combination of a collection of processes, where the $i$-th process alternates forever between engaging in the multi-way synchronisation $m$ and the independent event $t.i$. Notice that every process participates in the multi-way synchronisation, whereas only the $i$-th process participates in the independent event $t.i$. Also notice that $m$ is hidden from the environment. Thus, crucially for this development, we know the identities of all of $m$’s participants. If the membership were dynamic, then we would need to develop a protocol to manage its membership.

We now use *Circus’s* refinement calculus to derive a protocol that is equivalent to this system, but where there is no multi-way synchronisation. Our first step is to convert the $i$th process into an action system [3]. An action system is a process consisting of a loop containing the choice between events guarded by firing conditions in terms of the process’s state. Following each event, there is an action that updates the state.

At present, the flow of control in our process is described by the operators of *Circus’s* process algebra; when we convert to an action system, we record the current control position explicitly in the new variable $p$, the program counter.

\[
( \parallel_{\{m\}} i : I \bullet ( \mu X \bullet m \rightarrow t.i \rightarrow X ) ) \ \setminus \ \{m\}
\]

\[= \{ \text{action-system-conversion} \} \]
Our next step is to widen the scope of the local variables; to avoid confusing their values, we index each of the variables as an element of the new array-valued variable $p$. The choice of locality of scope is familiar to programmers.

$$= \{ \text{parallel-state} \}$$

$$\begin{align*}
\text{array } p &: I \rightarrow PC \\
( &\|_{\{m\}} i : I \bullet \\
p[i] &: \equiv m; \\
\mu X \bullet \mu X \cdot p[i] &= m \land m \rightarrow p[i] := t; X \] \{m\} \\
p[i] &= t \land t.i \rightarrow p[i] := m; X )
\end{align*}$$

The initialisation of the position counters can be moved out from the individual processes to form a simultaneous assignment that takes place after the declaration of the array, but before the execution of any of the individual processes, as an interleaving of individual assignments.

$$= \{ \text{parallel-assignment} \}$$

$$\begin{align*}
\text{array } p &: I \rightarrow PC \\
( &\|_{\{m\}} i : I \bullet \\
p[i] &: \equiv m; \\
\mu X \bullet p[i] &= m \land m \rightarrow p[i] := t; X \] \{m\} \\
p[i] &= t \land t.i \rightarrow p[i] := m; X )
\end{align*}$$

Now the parallel composition can be flattened into a sequential action system. The event $m$, shared between the individual processes, gives rise to an action
whose guard is the conjunction of all the individual processes’ guards. The events \( t_i \) may occur independently.

\[
= \{ \text{action-system-parallel} \}
\]

\[
\begin{array}{c}
\text{array } p : I \rightarrow PC \bullet \\
( \|\| i : I \bullet p[i] := m ); \\
\mu X \bullet (\forall i : I \bullet p[i] = m) \& m \rightarrow \\
(\|\| i : I \bullet p[i] := t); X \\
\Box \\
\Box i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m; X \\
\end{array}
\]

The operation of hiding the event \( m \) distributes through the array declaration, the outermost sequential composition, and the fixed-point operator. Since the event \( m \) doesn’t occur in the simultaneous assignment, hiding \( m \) is vacuous.

\[
= \{ \text{hiding-distribution} \}
\]

\[
\begin{array}{c}
\text{array } p : I \rightarrow PC \bullet \\
( \|\| i : I \bullet p[i] := m ); \\
\left(\forall i : I \bullet p[i] = m\right) \& m \rightarrow \\
\left(\|\| i : I \bullet p[i] := t\right); X \\
\Box \\
\Box i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m; X \\
\end{array}
\]

Hiding also distributes through the action system. The hidden event’s guard is either true or false. If the guard is false, then its internalised action is irrelevant. If the guard is true, then the hidden action may occur; but the other actions may or may not be available.

\[
= \{ \text{hiding-conditional-external-choice-distribution-2} \}
\]
array $p : I \to PC \bullet$

$(\|\| i : I \bullet p[i] := m);$

$\mu X \bullet (\forall i : I \bullet p[i] = m) \&$

$(\|\| i : I \bullet p[i] := t); X$

$\square$

$(Stop \sqcap \square i : I \bullet p[i] = t \& t.i \to p[i] := m; X)$

$\square$

$\neg (\forall i : I \bullet p[i] = m) \& \square i : I \bullet p[i] = t \& t.i \to$

$p[i] := m; X$

The recursive process is not an action system, but can be transformed into one. First, we push the guard $(\forall i : I \bullet p[i] = m)$ through the external and internal choices, and notice that $g \& Stop$ is simply $Stop.$

$= \{ \text{guard-external-choice-distribution, guarded-$Stop$} \}$

array $p : I \to PC \bullet$

$(\|\| i : I \bullet p[i] := m);$

$\mu X \bullet (\forall i : I \bullet p[i] = m) \& (\|\| i : I \bullet p[i] := t); X$

$\square$

$(Stop)$

$\square$

$(\forall i : I \bullet p[i] = m) \&$

$(\square i : I \bullet p[i] = t \& t.i \to p[i] := m; X)$

$\square$

$\neg (\forall i : I \bullet p[i] = m) \& \square i : I \bullet p[i] = t \& t.i \to$

$p[i] := m; X$

Notice that the process $(\square i : I \bullet p[i] = t \& t.i \to p[i] := m),$ which is to be found in the second external choice, has the guard $(\exists i : I \bullet p[i] = t).$ This says that there is an individual process waiting to do its independent transaction. But the outer guard says that every process is waiting to do
the multi-way synchronisation. These two guards are contradictory, so if we combine them, we get \( \text{false} \& p[i] := m \), which may again be simplified to the deadlocked process \( \text{Stop} \).

\[
\begin{align*}
&= \{ \text{predicate calculus, guard-left-zero} \} \\
\text{array } p : I \rightarrow PC \bullet \\
&( \| i : I \cdot p[i] := m ) ; \\
&\mu X \bullet ( \forall i : I \cdot p[i] = m ) \& ( \| i : I \cdot p[i] := t ) ; X \quad \square \\
&( \text{Stop} \sqcap \text{Stop} ) \\
&\square \\
&\neg ( \forall i : I \cdot p[i] = m ) \& \square i : I \cdot p[i] = t \& t.i \rightarrow \\
&p[i] := m ; X
\end{align*}
\]

\(( \text{Stop} \sqcap \text{Stop} )\) is, once again, simply \( \text{Stop} \), which is a unit for external choice.

\[
\begin{align*}
&= \{ \text{internal-choice-idempotence, external-choice-unit} \} \\
\text{array } p : I \rightarrow PC \bullet \\
&( \|\| i : I \cdot p[i] := m ) ; \\
&\mu X \bullet ( \forall i : I \cdot p[i] = m ) \& ( \|\| i : I \cdot p[i] := t ) ; X \\
&\quad \square \\
&\neg ( \forall i : I \cdot p[i] = m ) \& \square i : I \cdot p[i] = t \& t.i \rightarrow \\
&p[i] := m ; X
\end{align*}
\]

The result of this transformation is now an action system; the second action’s guard can be simplified, using the existing reasoning about the guard.

\[
= \{ \text{guard simplification} \}
\]
array \ p : I \rightarrow PC \bullet

( \|\| i : I \bullet p[i] := m );

\mu X \bullet ( \forall i : I \bullet p[i] = m ) \& ( \|\| i : I \bullet p[i] := t ); \ X

\square

\square i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m ; \ X

Notice that the initialisation sets all the elements of \( p \) to \( m \). This results in
the first guard being enabled and the second being disabled; the first action
then sets all the elements of \( p \) to \( t \); these two assignments can be merged.

= \{ \text{ computation } \}

array \ p : I \rightarrow PC \bullet

( \|\| i : I \bullet p[i] := m );

\left( ( \forall i : I \bullet p[i] = m ) \& ( \|\| i : I \bullet p[i] := t ); \ Z \right)

\square

\square i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m ; \ Z

where

\ Z \triangleq \mu X \bullet ( \forall i : I \bullet p[i] = m ) \& ( \|\| i : I \bullet p[i] := t ); \ X

\square

\square i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m ; \ X

A useful assertion is based on a consequence of the simultaneous assignment:

\ [ ( \|\| i : I \bullet p[i] := m ) \Rightarrow ( \forall i : I \bullet p[i] = m ) \]

The assertion is designed to match the first guard and to contradict the second.

= \{ \text{ assignment-assertion-introduction } \}
array $p : I \rightarrow PC \bullet$

$\begin{align*}
& (\forall i : I \bullet p[i] = m) \perp; \\
& \left( (\forall i : I \bullet p[i] = m) \& (\forall i : I \bullet p[i] := t); \ Z \right) \\
& \left( \square i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m; \ Z \right)
\end{align*}$

where

$$Z \triangleq \mu X \bullet (\forall i : I \bullet p[i] = m) \& (\forall i : I \bullet p[i] := t); \ X$$

$\begin{align*}
& \left( \square i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m; \ X \right)
\end{align*}$

Now we can use the assertion to simplify the external choice. First, we distribute the assertion to the two branches of the choice. Next we simplify the resulting guards; the first becomes $true$ and the second $false$.

$$= \{ \text{assertion-external-choice, predicate calculus, guard-unit, guard-zero} \}$$

array $p : I \rightarrow PC \bullet$

$\begin{align*}
& (\forall i : I \bullet p[i] = m) \perp; \\
& (\forall i : I \bullet p[i] := t) \\
& \mu X \bullet (\forall i : I \bullet p[i] = m) \& (\forall i : I \bullet p[i] := t); \ X \\
& \square i : I \bullet p[i] = t \& t.i \rightarrow p[i] := m; \ X
\end{align*}$

The assertion can be absorbed back into the assignment, which may then be safely deleted, since it is followed by another assignment in sequence.

$$= \{ \text{assignment-assertion-introduction, assignment-sequence} \}$$
We can’t easily repeat this unfolding with the other guard, since its action is an external choice. However, we can exploit this asymmetry further by applying a law from the fixed-point calculus known as the diagonal rule, which allows us to separate the two recursive calls, naming them individually.

Clearly, we could have applied the diagonal rule in another way; so why did we choose the first recursion? Because we can apply another fixed-point law: rolling. Notice that the recursion named $Y$ is preceded by an assignment, and all recursive calls are also preceded by the same assignment.

Now we’d like to localise the elements of $p$. First, we shift the declaration of
the array into the recursion, localising its scope.

\[
\begin{align*}
= \{ \text{declaration-recursion} \} \\
= \{ \text{action-system-parallel} \}
\end{align*}
\]

\[
\begin{align*}
\mu Y \cdot \\
\begin{array}{l}
( \| i : I \cdot p[i] := t ) ; \\
\| i : I \cdot \\
\mu X \cdot ( \forall i : I \cdot p[i] = m ) \& \text{Skip}
\end{array} \\
\mu X \cdot p[i] = m \& \text{Skip} \\
\square \\
\square i : I \cdot p[i] = t \& t.i \rightarrow p[i] := m ; X \\
\end{align*}
\]

The inner recursive process is actually an action system (actually, it is a degenerate kind of action system, with an action that is not event-guarded). More than this, it matches the right-hand side of the law that collapses a parallel combination of action systems into a single, sequential one. Using this observation as an inspiration, we start a series of transformations that mirror the ones at the start of the derivation, this time introducing parallelism.

\[
\begin{align*}
= \{ \text{action-system-parallel} \} \\
= \{ \text{parallel-assignment} \}
\end{align*}
\]

We are heading for an application of the action system conversion law; before this is applicable, we must push the initialisation of each element of the array into the individual action systems.
Now we push the declaration of the array into the individual action systems.

\[
\mu Y \bullet \begin{pmatrix}
\text{array } p : I \rightarrow PC \\
|| i : I \\
p[i] := t; \\
\mu X \bullet p[i] = m & \text{Skip} \\
\square \\
p[i] = t & t.i \rightarrow p[i] := m; X
\end{pmatrix} ; Y
\]

At last, we can apply the action system conversion law.

\[
\mu Y \bullet ( || i : I \\
\text{var } p := t \\
\mu X \bullet p = m & \text{Skip} \\
\square \\
p = t & t.i \rightarrow p := m; X ); Y
\]

The inner-most recursion has now disappeared, and so we remove the inner-most fixed-point operator, which is redundant.

\[
\mu Y \bullet ( || i : I \bullet ( \mu X \bullet t.i \rightarrow \text{Skip} )); Y
\]

And at last, we have reached our objective: a simple protocol that ensures that the transactions are synchronised, but that does not use an explicit multi-way synchronisation. It is now at the code-level of \textit{occam}.

\section{Conclusions and related work}

We have shown how \textit{Circus} can be used to describe and reason about safety-critical systems. In particular, we have shown how to use \textit{Circus}'s refinement
calculus to develop a program that implements an abstract multi-way synchronisation using only pairwise synchronisations. The example is simple, but it is representative of our style of using calculation to develop reactive programs.

Our implementation actually retains a special kind of multi-way synchronisation: distributed co-termination of the interleaved processes. This can easily be avoided with a different development pattern.

A more interesting problem occurs when the multi-way synchronisation is part of an external choice, and our solution is not applicable in such a situation. We have calculated efficient two-phase commit protocols to deal with these kinds of synchronisation patterns. Although these programs are much more complex than the one calculated in this paper, the same development strategy is used. The abstract program is reduced to normal form, which, since it is sequential, contains no multi-way synchronisations. This normal form is then partitioned into new parallel processes that implement a protocol for synchronising individual transactions.

Our colleague, Peter Welch, has implemented a range of these protocols in occam and in JCSP, a Java class library for CSP/occam primitives. These implementations give a feel for the cost of implementing the multi-way abstraction. On a 1GHz commodity processor, it takes about 10\(\mu\)s to synchronise ten processes using the two-phase commit protocol.

Our work exploits the simple properties of CSP action systems, which are clearly related to those of Back and Kurki-Suonio [3]. Our work differs in that we are interested in rich state and reactive behaviour, using action systems as a convenient stepping-stone during transformations.

Acknowledgement

The author is grateful to the following: the Programme Committee of the Brazilian Workshop on Formal Methods, WMF’2003, for their invitation to present this paper; and to Formal Methods Europe for their financial support for the lecture. The Circus project is generously supported by QinetiQ Malvern and Bedford. The author has benefited from extensive technical discussions with Ana Cavalcanti, Alistair McEwan, Colin O’Halloran, and Peter Welch.

References

[1] Abrial, Jean-Raymond, Steam-boiler control specification problem. In [2].

[2] Abrial, Jean-Raymond, Egon Börger, and Hans Langmaack (editors). Formal Methods for Industrial Applications: Specifying and Programming the Steam Boiler Control. Lecture Notes in Computer Science 1165. Springer. 1996.
[3] Back, R. J. R. and R. Kurki-Suonio, Decentralization of process nets with centralized control. *Procs 2nd ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*. pp.131–142 1983.

[4] Back, Ralph-Johan and Joakim von Wright. *Refinement Calculus: a systematic approach*. Springer-Verlag 1998.

[5] Bauer, J. C., Specification for a software program for a boiler water content monitor and control system. Institute of Risk Research. Univ. of Waterloo. 1993.

[6] Brien, S. M. and J. E. Nicholls, *Z Base Standard* version 1.0. *PRG Technical Monograph PRG-107*, Oxford University Computing Laboratory. 1992.

[7] Cavalcanti, Ana, *A Refinement Calculus for Z*. DPhil Thesis. *Technical Monograph PRG-123*, Oxford University Computing Laboratory. 1997.

[8] Cavalcanti, A. L. C., A. C. A. Sampaio, and J. C. P. Woodcock. Refinement of Actions in Circus. *Proceedings of REFIN’E2002. Electronic Notes in Theoretical Computer Science*. 2002. *Keynote speech*.

[9] Cavalcanti, A. L. C., A. C. A. Sampaio, and J. C. P. Woodcock. A refinement strategy for Circus. *Formal Aspects of Computing*, 15(2–3): 146–181, 2003.

[10] Cavalcanti, A. L. C., A. C. A. Sampaio, and J. C. P. Woodcock. A unified language of classes and processes. Presented at *St.Eve: State-Oriented vs. Event-Oriented Thinking in Requirements Analysis, Formal Specification, and Software Engineering*. Satellite Workshop at FM’03. 2003

[11] Cavalcanti, A. L. C. and J. C. P. Woodcock, ZRC—A refinement calculus for Z. *Formal Aspects of Computing*, 10(3): 267–289, 1998.

[12] Cavalcanti, A. L. C. and J. C. P. Woodcock. A Weakest Precondition Semantics for Circus. *Communicating Process Architectures 2002*. J. S. Pascoe, P. H. Welch, R. J. Loader, and V. S. Sunderam (editors). IOS Press. 2002. pp.147–166.

[13] Cavalcanti, A. L. C. and J. C. P. Woodcock. Predicate transformers in the semantics of Circus. *IEE Procs Software* 150(1) February 2003. *Invited paper*.

[14] Dijkstra, E. W., Guarded commands, nondeterminacy and the formal derivation of programs. *Communications of the ACM* 18:453–457 1975.

[15] Hoare, C. A. R., *Communicating Sequential Processes*. Prentice Hall. 1985.

[16] Hoare, C. A. R. and He Jifeng. *Unifying Theories of Programming*. Prentice Hall International Series in Computer Science. 1998.

[17] inmos ltd. *occam Programming Manual*. Prentice Hall. 1984.

[18] Meisels, Irwin and Mark Saaltink. *The Z/Eves Reference Manual*. TR-1997-5493-2003d. ORA Canada. 1997.

[19] Morgan, Carroll, *Programming from Specifications* second edition. Prentice Hall International Series in Computer Science. 1994.

[20] Morris, J. M., A theoretical basis for stepwise refinement and the programming calculus. *Science of Computer Programming* 9:287–306 1987.

[21] O’Halloran, C., Identifying Critical Requirements. Systems Assurance Group. QinetiQ Malvern. 2002.

[22] Roscoe, A. W., *The Theory and Practice of Concurrency*. Prentice Hall. 1998.

[23] Saaltink, Mark, *The Z/Eves User’s Guide*. TR-1997-5493-2006. Odyssey Research Associates Canada. 1997.

[24] Sampaio, A. C. A., J. C. P. Woodcock, and A. L. C. Cavalcanti. Refinement in Circus. L. Eriksson and P. A. Lindsay, editors. *FME 2002: Formal Methods—Getting IT Right. Lecture Notes in Computer Science*. Volume 2391:451–470. Springer-Verlag, 2002.
A Some laws of Circus

This section contains a list of the laws used in the derivation. Each of these laws has been proved correct in the unifying theory of programming [16].

Law: action-system-conversion

\[
(\mu X \bullet x \rightarrow y \rightarrow X) = \begin{cases}
\text{var } p := x \bullet \\
\mu X \bullet p = x \& p := y; X \\
\square \\
p = y \& p := x; X
\end{cases}
\]

Law: action-system-parallel
\[
\left( \begin{array}{c}
\|_{(x)} i : I \bullet \\
\mu X \bullet g_i & x \to A_i; X \\
\Box \\
h_i & y_i \to B_i; X
\end{array} \right) = 
\left( \begin{array}{c}
\mu X \bullet (\forall i : I \bullet g_i) & x \to \\
(\| i : I \bullet A_i); X \\
\Box \\
\Box i : I \bullet h_i & y_i \to B_i; X
\end{array} \right)
\]

**Law: assertion-external-choice-distribution**
\[
c_\perp; (P \Box Q) = (c_\perp; P) \Box (c_\perp; Q)
\]

**Law: assignment-assertion-introduction**
\[
(x := e) = (x := e; (x = e)_\perp)
\]

**Law: assignment-sequence**
\[
(x := e; x := f) = (x := f)
\]

*providing* \(x\) is not free in \(f\)

**Law: computation**
\[
\mu F = F(\mu F)
\]

**Law: declaration-recursion**
\[
\text{var } x \bullet (\mu X \bullet x := e; F(X)) = \mu X \bullet (\text{var } x := e; F(X))
\]

**Law: fixed-point-constant**
\[
(\mu X \bullet K) = K
\]

*providing* \(X\) is not free in \(K\)

**Law: fixed-point-diagonal**
\[
\mu X \bullet F(X, X) = \mu X \bullet (\mu Y \bullet F(X, Y))
\]

**Law: fixed-point-rolling**
\[
G(\mu X \bullet F(G(X))) = \mu X \bullet G(F(X))
\]
Law: guard-external-choice-distribution
\[ g \land ( P \parallel Q ) = ( g \land P ) \parallel ( g \land Q ) \]

Law: guard-left-unit
\[ \text{true} \land P = P \]

Law: guard-left-zero
\[ \text{false} \land P = \text{Stop} \]

Law: guard-right-zero
\[ g \land \text{Stop} = \text{Stop} \]

Law: hiding-conditional-external-choice-distribution-2
\[
\left( b \land x \rightarrow P \right) \square \{x\} = \left( b \land ( P \setminus \{x\} \parallel c \land y \rightarrow Q \setminus \{x\} ) \right)
\]

Law: hiding-distribution
\[
\left( \text{var} \; x \cdot P \right) \setminus S = \left( \text{var} \; x \cdot P \setminus S \right) \\
\left( P ; Q \right) \setminus S = \left( P \setminus S ; Q \setminus S \right) \\
\left( \mu X \cdot F(X) \right) \setminus S = \left( \mu X \cdot F(X) \setminus S \right) \\
\left( x := e \right) \setminus S = \left( x := e \right)
\]

Law: internal-choice-idempotence
\[ ( P \parallel P ) = P \]

Law: parallel-assignment
\[ \left( \| i : I \cdot ( x[i] := e_i ; P_i ) \right) = \left( \| i : I \cdot x[i] := e_i \right) ; \left( \| i : I \cdot P_i \right) \]

Law: parallel-state
\[ \| i : I \cdot ( \text{var} \; x : T \cdot P_i ) = \text{array} \; x : I \rightarrow T \cdot \left( \| i : I \cdot P_i[x[i]/x] \right) \]