




# Temporal Reasoning Through Automatic Translation of *tock-CSP* into Timed Automata

Abdulrazaq Abba<sup>1,2</sup>(✉) , Ana Cavalcanti<sup>1</sup>, and Jeremy Jacob<sup>1</sup>

<sup>1</sup> University of York, York, UK

<sup>2</sup> University of East London, London, UK  
a.abba@uel.ac.uk

**Abstract.** We present an approach for automatic translation of *tock-CSP* into Timed Automata (TA) to facilitate using UPPAAL in reasoning about temporal specifications of *tock-CSP* models. The process algebra *tock-CSP* provides textual notations for modelling discrete-time behaviours, with the support of tools for automatic verification. Automatic verification of TA with a graphical notation is supported by UPPAAL. The two approaches provide diverse facilities for automatic verification. For instance, liveness requirements are difficult to specify with the constructs of *tock-CSP*, but they are easy to specify and verify in UPPAAL. We have developed a translation technique based on rules and a tool for translating *tock-CSP* into a network of small TAs for capturing the compositional structure of *tock-CSP*. For validating the rules, we begin with an experimental approach based on finite approximations of trace sets. Then, we consider using structural induction to establish the correctness.

**Keywords:** Translation · *tock-CSP* · Timed-Automata

## 1 Introduction

Communicating Sequential Processes (CSP) is an established process algebra that provides a formal notation for both modelling and verifying concurrent systems [17, 31, 33]. The use of CSP for verification has been supported by several tools including powerful model-checkers [13, 31, 35].

Interest in using existing tools of CSP motivated [31] the introduction of support for modelling discrete timed systems: *tock-CSP* provides an additional event *tock* to record the progress of time. As a result, *tock-CSP* has been used to verify real-time systems, such as security protocols [11] and railway systems [19]. Also, recently *tock-CSP* has been used to capture the semantics of RoboChart, a domain-specific language for modelling robotics applications [25].

In this work, we present a technique for automatic translation of *tock-CSP* into Timed Automata (TA) to enable using UPPAAL[5] and temporal logic to verify *tock-CSP* models. UPPAAL is a tool suite for modelling and verification of

hybrid systems using a network of TAs. We describe the translation rules and their implementation into a tool.

Both temporal logic and refinement are powerful approaches for model checking [23]. The refinement approach models both the system and its specifications with the same notation [31, 33]. Temporal logic enables asking whether a system captures logical formulae of the requirements specification in the form of  $system \models formula$  [8].

Lowe has investigated the relationship between the refinement approach (in CSP) and the temporal logic approach [23]. The result shows that, in expressing temporal logic checks using refinement, it is necessary to use the infinite refusal testing model of CSP. The work highlights that capturing the expressive power of temporal logic to specify the availability of an event (liveness specification) is not possible in the trace refinement model. Also, due to the difficulty of capturing refusal testing, automatic support becomes problematic, and FDR stops supporting refusal testing in its recent version [13].

Additionally, Lowe’s work [23] proves that simple trace refinement checks cannot match the expressive power of temporal logic, especially of the three operators: *eventually* ( $\diamond p$ : *p will hold in a subsequent state*), *until* ( $p\mathcal{U}q$ : *p holds in every state until q holds*) and their *negations*:  $\neg(\diamond p)$  and  $\neg(p\mathcal{U}q)$ . These three operators express behaviour captured by infinite traces. Our contribution presented here facilitates an alternative way of checking such specifications.

*Example 1.* Consider an Automatic Door System (ADS) that opens a door, and after at least one-time unit, closes the door in synchronisation with a lighting controller, which turns off the light. In *tock-CSP*, this is expressed as:

```

1      ADS = Controller [|{close}|] Lighting
2  Controller = open -> tock -> close -> Controller
3  Lighting = close -> offLight -> Lighting

```

The process ADS has two components—Controller and Lighting—that synchronise on the event `close`<sup>1</sup>, which enables Lighting to turn off the light after closing the door. In *tock-CSP*, there is no direct way of checking if the system eventually turns off the light. However, temporal logic provides a direct construct for specifying liveness requirements, supported in UPPAAL, as follows.

–  $A \langle \rangle \text{offLight}$     - - *The system eventually turns off the light*

UPPAAL uses a subset of Timed Computation Tree Logic (TCTL) based on the notions of path and state [5]. A path *formula* quantifies over paths (traces), whereas a state *formula* describes locations. There are different forms of path formulae. Liveness is either  $A \langle \rangle q$  (*q is eventually satisfied*) or  $p \dashv\dashv q$  (*a state satisfying p leads to a state satisfying q*). A reachability *formula* in the form of

<sup>1</sup> Here, the event *close* is asynchronisation event using the CSP operator ( $[|Event|]$ ) for synchronising multiple concurrent processes, such that all the processes have to synchronise on the all the elements of the set *Event* before they can proceed.

$E \langle \rangle_{\mathcal{Q}}$  (*a state satisfying  $q$  is reachable from the initial state*). Safety is expressed as either  $A []_{\mathcal{Q}}$  ( *$q$  holds in all reachable states*) or  $E []_{\mathcal{Q}}$  ( *$q$  holds in all states on at least one path*).

To verify the correctness of the translation technique, first, we use the developed translation technique and its tool to translate the formulated processes into TA for UPPAAL. Next, we use another tool we have developed to generate and compare finite traces of the input *tock-CSP* models and the traces of the translated TA models.

We use Haskell [18], a functional programming language, to express, implement and evaluate the translation technique. The expressive power of Haskell helps us provide formal descriptions of the translation technique as a list of translation rules, which is also suitable for developing a mathematical proof.

The structure of this paper is as follows. Section 2 provides background material. Section 3 summarises the translation technique. We discuss an evaluation of the translation technique in Sect. 4. In Sect. 5, we highlight related works and present a brief comparison with this work. Finally, we highlight future extensions of this work and conclude. Additional details of this work including proofs, implementation and additional examples are available in [1, 2].

## 2 Background

As an extension of CSP, *tock-CSP* provides notations for modelling processes and their interactions, such as the basic processes: SKIP and STOP, for successful termination and deadlock, respectively. Operators include prefix ( $\rightarrow$ ) for describing availability of an event. For example, the process  $\text{move} \rightarrow \text{SKIP}$  represents a mechanism that moves once and then terminates.

There are binary operators such as sequential composition ( $;$ ), which combines two processes serially. For instance, the process  $P3 = P1; P2$  behaves as process P1, and after successful termination of P1, P2 takes over and P3 behaves as P2. There are other binary operators for concurrency, choice and interruption. Also, CSP has a special event *tau* ( $\tau$ ) for representing invisible actions that are internal to a system. The collection of these operators provides a rich set of constructs for modelling untimed systems [31, 33].

For modelling time, *tock-CSP* has a special event *tock* [31], which specifies that the process waits for one time unit before it engages with its environment. For example, the following process  $Pt$  specifies behaviour that moves and then after at least two time units, turns and terminates.

$$Pt = \text{move} \rightarrow \text{tock} \rightarrow \text{tock} \rightarrow \text{turn} \rightarrow \text{SKIP}$$

Timed Automata for UPPAAL model hybrid systems as a network of TA. Mathematically, a TA is a tuple  $(L, l_0, C, A, E, I)$ , where  $L$  is a set of locations such that  $l_0$  is the initial location,  $C$  is a set of clocks,  $A$  is a set of actions,  $E$  is a set of edges that connects the locations  $L$ , and  $I$  is an invariant associated to a location  $l \in L$  in the form of  $I : L \rightarrow B(C)$ . So, edges  $E \subseteq (L \times A \times B(C) \times 2^C \times L)$  from a location  $l \in L$  triggered by an action  $a \in A$ , guarded with a

guard  $g \in B(C)$  where  $B(C)$  is the set of guards, and associated clock  $c \in C$  that is reset on following the edge to a location  $l \in L$  [5, 7].

A system is modelled as a network of TAs that communicate via either synchronous channel communication or shared variables. A sending channel is decorated with an exclamation mark ( $c!$ ) while the corresponding receiving channel is decorated with a question mark  $c?$ . A TA performs an action  $c!$  to communicate with another TA that performs the corresponding co-action  $c?$ . There are also broadcast channels for communication among multiple TAs, in the form of one-to-many communications (one sender with multiple receivers).

For expressing urgency, there are urgent channels and urgent locations that do not allow delay. There are also committed locations; urgent locations that must participate in the next transition, which is useful for expressing atomicity; a compound action spanning multiple transitions that must be executed as a unit. Invariants specify precise delay and enforce progress [5]. In UPPAAL, networks of TAs model system's components and an explicit operating environment. Additional details with examples are available in [5, 6, 22].

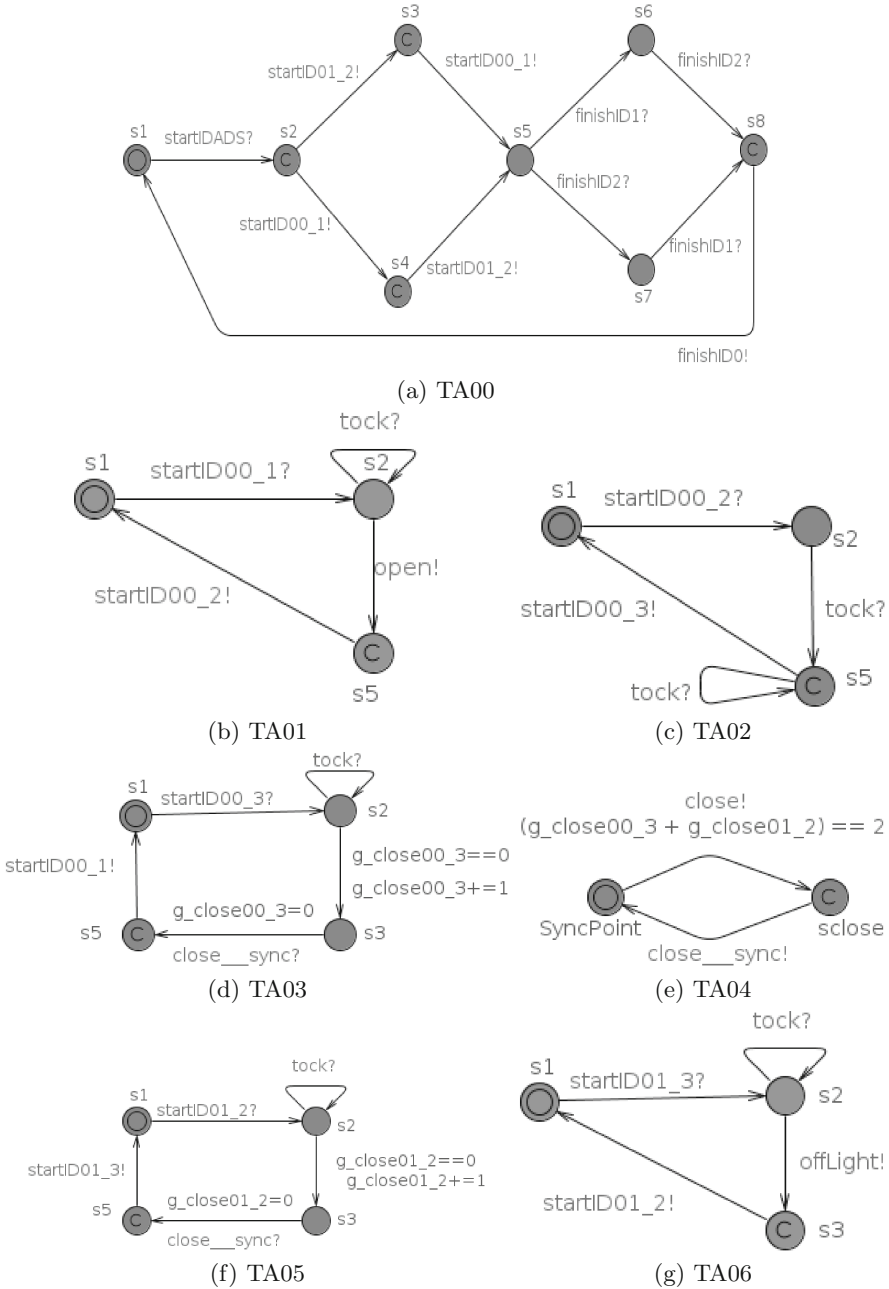
### 3 An Overview of the Translation Technique

In this section, we describe the translation of the main constructs of *tock-CSP* via examples. The formal rules are omitted due to space restrictions, but are available in [1, 2]. Our translation technique takes an input *tock-CSP* model and produces a list of TAs. The occurrence of each *tock-CSP* event is captured in a small TA with an UPPAAL action, which records an occurrence of the translated event. The small TAs are composed into a network of TAs that capture the behaviour of the input *tock-CSP* model. The network of small TAs give us enough flexibility to capture the compositional structure of *tock-CSP*.

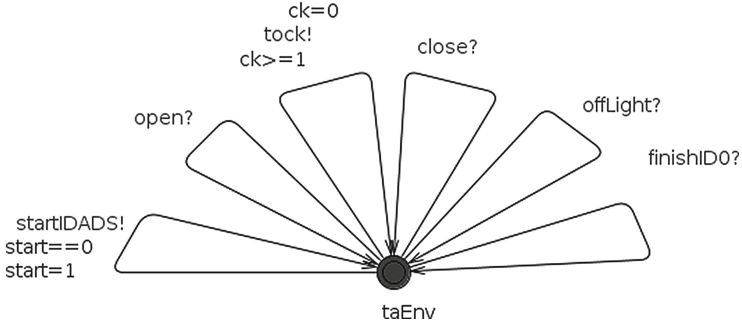
*Example 2.* A translation of the process ADS, from Example 1, produces a network of small TAs in Fig. 1. TA00 captures concurrency by starting the two automata for the processes Controller and Lighting in two possible orders—either Controller then Lighting or vice versa—depending on the operating environment. Here, we use the committed locations ( $s_2$ ,  $s_3$  and  $s_4$ ) to show that starting the concurrent automata is a compound action. Then TA00 waits on state  $s_5$  for the termination actions in the two possible orders, either  $finishID1?$  then  $finishID2?$  or vice versa. However, for the termination, we do not use committed locations because the processes can terminate at different times. TA00 synchronises the processes before terminating the system with the action  $finishID0!$ .

TA01, TA02 and TA03 capture the behaviour of the process Controller. TA01 captures the occurrence of the event `open`. TA02 captures the occurrence of `tock` to synchronise with the environment TA in recording the progress of time. TA03 captures the event `close` to synchronise with the controller TA04.

TA05 and TA06 capture the behaviour of the process Lighting. TA05 captures `close`, which also synchronises with TA04. Then, TA06 captures the event



**Fig. 1.** A list of networked TAs for the translation of the process ADS.



**Fig. 2.** An environment TA for the translated behaviour of the process ADS.

offLight. Finally, Fig. 2 shows the environment TA that has co-actions for all the translated events. The environment TA serves the purpose of ‘closing’ the overall system as required for the model checker. In the environment TA, we use the variable `start` to construct a guard `start==0` that blocks the environment from restarting the system.

The main reason for using a list of small TAs is to capture the compositional structure of *tock-CSP*, which is not available in TA [9]. For instance, it can be argued that a linear process constructed with a series of prefix operators can be translated into a linear TA<sup>2</sup>. However, the compositional structure of *tock-CSP* is not suitable for this straightforward translation. For instance, consider a case where the linear process is composed with an interrupting process<sup>3</sup>: the behaviour is no longer linear because the process can be interrupted at any stable state, as illustrated in Example 4. This problem can be seen in translating a process  $P = (e1 \rightarrow \text{SKIP}) [] ((e2 \rightarrow \text{SKIP}) ||| (e3 \rightarrow \text{SKIP}))$ , which contains both external choice and concurrency. However, a network of small TAs provides enough flexibility for composing TA in various ways to capture the behaviour of the original *tock-CSP* process.

In constructing the networked TAs, we use additional *coordinating actions* to link the list of small TAs to establish the flow of the input *tock-CSP* model. For example, the channel `startIDADS` links the environment TA (Fig. 2) with TA00 (Fig. 1), on performing the action `startIDADS!` and its co-action `startIDADS?`. A precise definition of the coordinating action is as follows.

**Definition 1.** A *Coordinating Action* is an UPPAAL action that does not correspond to a *tock-CSP* event. There are six types of coordinating actions:

<sup>2</sup> A TA with linear transitions only, no branches.

<sup>3</sup> Also, *tock-CSP* inherits the operator *interrupt* ( $/\backslash$ ) from CSP, which allows a process to shut down another and takes over the control. For instance, initially the process  $(P/\backslash Q)$  behaves as  $P$  but at any time before its termination if the process  $Q$  performs a visible action, the process  $P$  hands over the control to the process  $Q$ . Therefore, the process  $P$  terminates and the whole process  $(P/\backslash Q)$  behaves as  $Q$ .

**Flow actions** coordinate a link between two TAs for capturing the flow of their behaviour; **Terminating actions** record termination information, in addition to coordinating a link between two TAs; **Synchronisation actions** coordinate a link between a TA that participates in a synchronisation action and a TA for controlling the synchronisation; **External choice actions** coordinate an external choice, such that choosing one of the TA that is part of the external choice thus blocks the other choices TAs; **Interrupting actions** initiate an interrupting transition that enables a TA to interrupt another; and **Exception actions** coordinate a link between a TA that raises an action for exception and a control TA that handles the action.

The names of each coordinating action are unique to ensure the correct flow of the translated TAs<sup>4</sup>. In our tool, the names of the flow actions are generated in the form `startIDx`, where `x` is either a natural number or the name of the input *tock-CSP* process. For instance in Fig. 1, `startID00_1` is the flow action that connects TA00 and TA01.

Likewise, the names of the remaining coordinating actions follow similar pattern: `keywordIDx`, where `keyword` is a designated word for each of the coordinating actions; `finish` for a terminating action, `ext` for an external choice action, `intrp` for an interrupting action, and `excp` for an exception action. Similarly, we provide a special name for a synchronising action in the form `eventName__sync`: an event name appended with the keyword `__sync` to differentiate a synchronising action from other actions. This is particularly important for analysis and are in the reserved keywords for the supporting tool.

For each translated *tock-CSP* specification, we provide an environment TA, like the TA in Fig. 2, which has corresponding co-actions for all the translated events of the input *tock-CSP* model, plus three coordinating actions that link the environment TA with the networked TAs. The first flow action links the environment with the first TA in the list of the translated TA (as illustrated in Fig. 2, the action `startIDADS` links the environment TA with TA00 in Fig. 1). This first flow action activates the behaviour of the translated TA. Second, a terminating action links back the terminating TA to the environment TA to capture a successful termination of a process (as shown in Fig. 2 with the action `finishID0`). Third, a flow action `tock` records the progress of time. A precise definition of the structure of the environment TA is as follows.

**Definition 2.** *An environment TA models operating environments for UPPAAL. The environment TA has one state and transitions for each co-action of all the events in the input tock-CSP process, in addition to three transitions: the first starting flow action, the final terminating co-action and the action tock for recording the progress of time.*

In translating multi-synchronisation, we adopt a centralised approach developed in [28] and implemented using Java in [12], which uses a separate cen-

<sup>4</sup> We use terminating actions where a TA needs to communicate a successful termination for another TA to proceed. For instance, in translating sequential composition  $P1; P2$ , the process  $P2$  begins only after successful termination of the process  $P1$ .

tralised controller for handling synchronisation. Here, we use a separate TA with an UPPAAL broadcast channel to communicate synchronising information. In Fig. 1, we illustrate the translation of synchronisation in translating the event `close`, which synchronises TA03 and TA05 using the broadcasting channel `close__sync`.

Each synchronising TA has a guard to ensure synchronisation with the correct number of TAs. The guard requires that the sum of special synchronisation variables from all the TAs that synchronise on the synchronisation action equals the number of such actions. Each TA updates its synchronisation variable from 0 to 1 to show its readiness for the synchronisation and waits for the synchronisation action. For instance, in Fig. 1, the synchronising TA (TA04) has a guard expression  $(g\_close00\_3 + g\_close01\_2) == 2$ , which becomes true only when TA03 and TA05 update their synchronisation variables: `g_close00_3` and `g_close01_2`, from 0 to 1. Then, TA04 notifies the occurrence of the action `close` and broadcasts the synchronising action `close__sync!`. After the synchronisation, each TA resets its variable to zero and performs its remaining behaviour. A precise definition of the synchronisation TA is as follows.

**Definition 3.** *A **synchronisation TA** coordinates synchronisation actions. The synchronisation TA has an initial state, and a committed state for each synchronisation action, such that each committed state is connected to the initial state with two transitions. The first transition from the initial state has a guard and an action. The guard is enabled only when all the processes are ready for synchronisation, which also enables the synchronising TA to perform the associated action that notifies the environment of its occurrence. In the second transition, the TA broadcasts the synchronisation action to all the processes that synchronise, which enables them to synchronise and proceed.*

In translating external choice, we provide additional transitions to capture the behaviour of the chosen process in blocking the behaviour of the other processes. Initially, in the translated TA, all the initials<sup>5</sup> of the translated processes are available such that choosing one process blocks all the other choices.

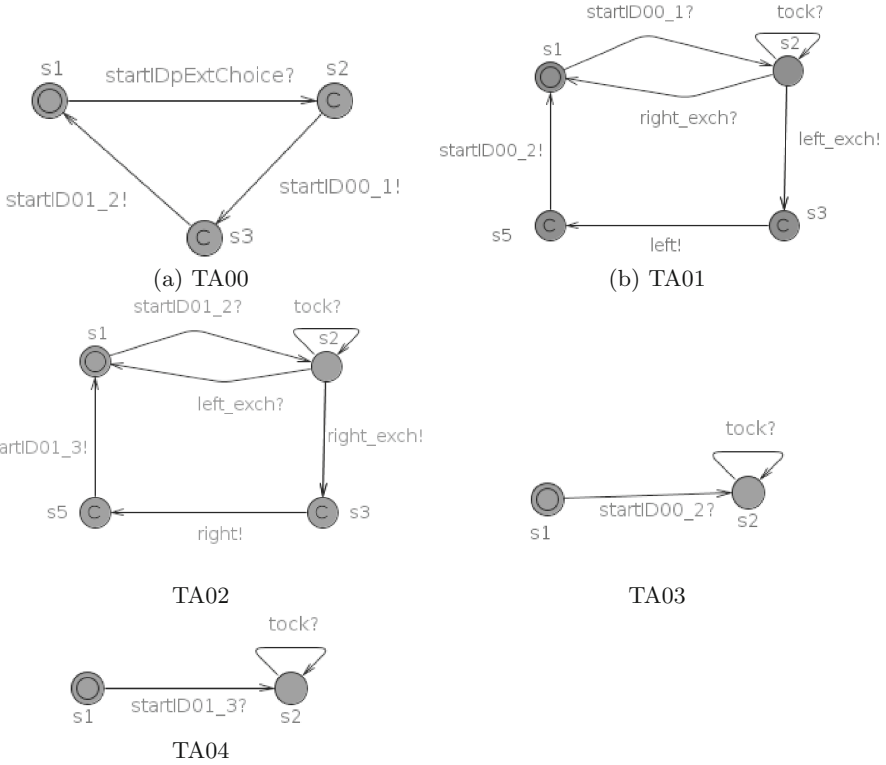
*Example 3.* A translation of external choice is illustrated in Fig. 3 for the process  $P_e = (\text{left} \rightarrow \text{STOP}) [] (\text{right} \rightarrow \text{STOP})$ , which composes two processes `left`  $\rightarrow$  `STOP` and `right`  $\rightarrow$  `STOP` using the external choice operator  $([])$ .

In Fig. 3, TA00 captures the operator external choice. TA01 and TA03 capture the LHS process (`left`  $\rightarrow$  `STOP`). TA02 and TA04 capture the RHS process (`right`  $\rightarrow$  `STOP`). TA00 has three transitions labelled with the actions: `startIDpExtChoice?`, `startID00_1!` and `startID01_2!`. TA00 begins with the first flow action `startIDpExtChoice?` and then starts both TA01 and TA02, using the actions `startID00_1!` and `startID01_2!`, available for choice.

Initially, TA01 synchronises on `startID00_1` and moves to location `s2` that has three transitions labelled: `left_exch?`, `right_exch!` and `tock?`.

<sup>5</sup> The term initials describe the first visible events of a process.





**Fig. 3.** A list of TAs for the translated behaviour of the process  $P_e$

With the co-action  $tock?$ , the TA records the progress of time and remains on the same location  $s_2$ . With the co-action  $right\_exch?$ , the TA performs an external choice co-action for blocking the LHS process when the environment chooses the RHS process, and TA01 returns to initial location  $s_1$ .

Alternatively, TA01 performs the action  $left\_exch!$  when the environment chooses the LHS process, and TA01 proceeds to location  $s_3$  to perform the chosen action  $left!$  that leads to location  $s_5$  and performs the flow action  $startID00_2!$ , which activates TA03 for the subsequent process  $STOP$ . For the RHS process, TA02 captures the similar translation of the event  $right$ . The omitted environment TA is similar to that in Fig. 2.

In  $tock$ -CSP, a process can be interrupted by another process when composed using an operator  $interrupt (/ \setminus)$ . Thus, we provide additional transitions to capture the interrupting behaviour.

*Example 4.* An example of translating interrupt is in Fig. 4, for the translation of the process  $P_i = (open \rightarrow STOP) / (fire \rightarrow close \rightarrow STOP)$ .

In  $P_i$ , the RHS process  $fire \rightarrow close \rightarrow STOP$  can interrupt the LHS process  $open \rightarrow STOP$  at any stable state. So, in the translated behaviour of the LHS

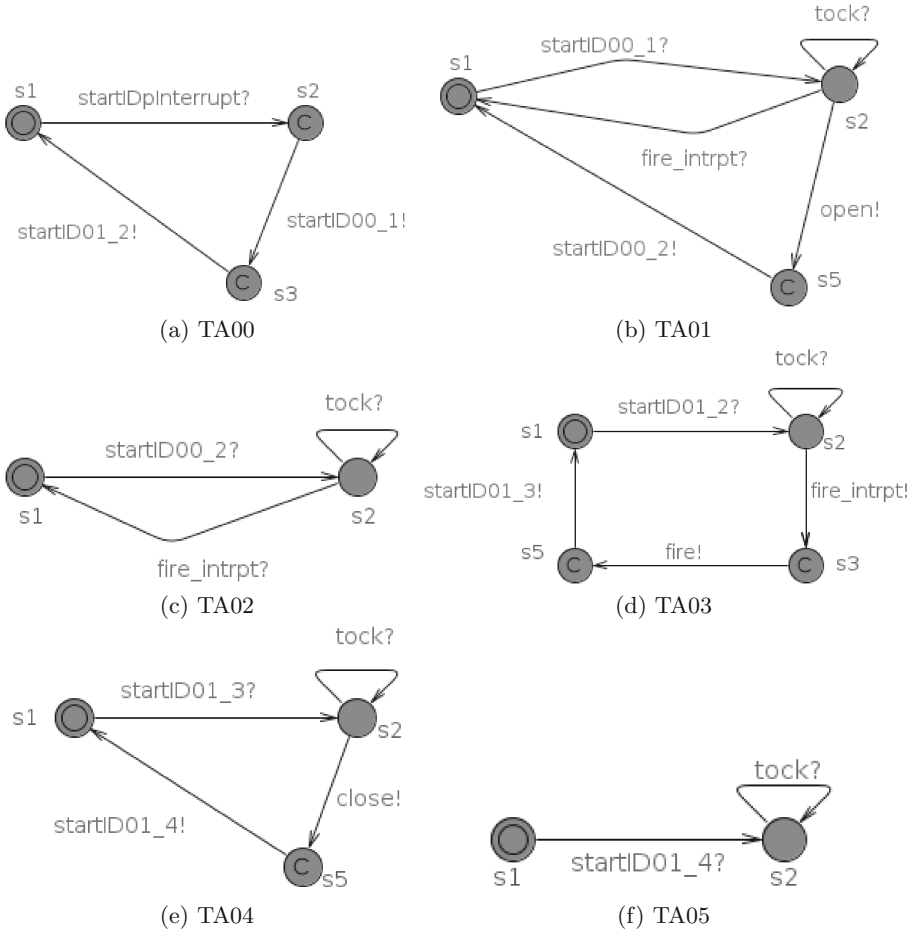


Fig. 4. A list of TAs for the translated behaviour of the process Pi.

process, we provide interrupting actions (like `fire_intrpt`) that enable the translated behaviour of the RHS process to interrupt that of the LHS process. The corresponding co-action of the interrupting actions are provided only for the initials of the RHS process (`fire`) because it can only interrupt with its initials.

In Fig. 4, TA00 is a translation of the operator interrupt. TA01 and TA02 capture the translation of the LHS process `open`->`STOP`, while TA03, TA04 and TA05 capture the translation of the RHS process `fire`->`close`->`STOP`. The environment TA is again similar to the TA in Fig. 2.

First, TA00 performs the actions `startID00_1!` and `startID01_2!` to activate TA01 and TA03. TA01 synchronises on `startID00_1` and moves to location `s2` where there are three possible transitions for the actions:

`tock?`, `open!` and `fire_intrpt?`. With the co-action `fire_intrpt?`, the TA is interrupted by the RHS, and returns to its initial location `s1`. With `tock?`, the TA records the progress of time and remains on the same location `s2`. With `open`, the TA proceeds to location `s5` to perform the flow action `startID00_2!` to activate TA02 for the subsequent process `STOP`. TA02 synchronises on `startID00_2?` and moves to location `s2`, where it either performs `tock?` to record the progress of time or is interrupted through the co-action `fire_intrpt?`, and returns to its initial location `s1`.

For the RHS, TA03 captures the translation of the event `fire`. TA03 begins with synchronising on `startID01_2?`, which progresses by interrupting the LHS process using the interruptive flow action `fire_intrpt!`, then `fire!`, and performs `startID01_3!` for activating TA04 which synchronises on the flow action and moves to location `s2`, where it either performs the action `tock?` for the progress of time and remains in the same location or performs the action `close!` and proceeds to location `s5`, then performs the flow action `startID01_4!` for starting TA05 for the translation of `STOP` (deadlock).

We translate the event `tock` into a corresponding action `tock` using a broadcast channel for the environment TA to broadcast the progress of time for all the TAs to synchronise. For instance, in Fig. 1, the environment TA has a transition labelled `tock` guarded with the clock expression  $ck \geq 1$ , so that `tock` happens every 1 time unit, and resets the clock  $ck = 0$  to zero on following the transition.

Also, we translate non-deterministic choice into silent transitions, such that the translated TA follows one of the silent transitions non-deterministically. This completes an overview of the strategy we follow in developing the translation technique. A precise description of all the translation rules in Haskell is in [1, 2].

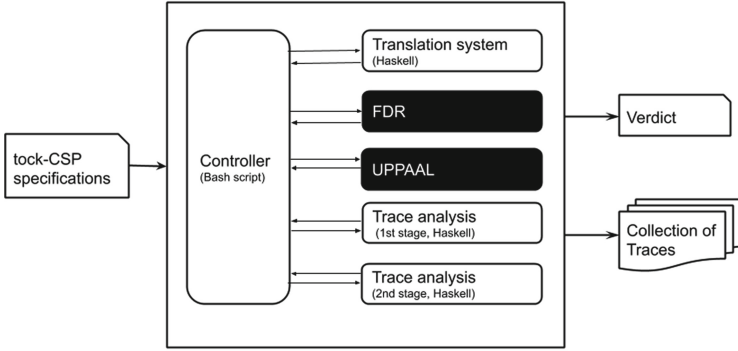
## 4 Evaluation

A sound translation ensures that the properties of the source model are preserved in the translated model. This is determined by comparing their behaviours [4, 20, 24, 26]. We compare the behaviour of the input *tock-CSP* and the output TA in two phases: experimental evaluation and mathematical proof.

### 4.1 Experimental Evaluation

We use trace semantics to evaluate the equivalence of the traces. In carrying out the experiment, we have developed an evaluation tool, which uses our translation tool and both FDR and UPPAAL as black boxes for generating finite traces, as shown in Fig. 5, which shows the structure of the evaluation tool, available at [1].

In generating traces, like most model checkers, FDR produces only one trace (counterexample) at a time. So, based on the testing technique in [27], we have developed a trace-generation technique that repeatedly invokes FDR until we get all the required trace sets of the input process. Similarly, based on another



**Fig. 5.** Structure of the trace analysis system

testing technique with temporal logic [22], we have developed a trace-generation technique that uses UPPAAL to generate traces of the translated TA models.

These two trace-generation techniques form components of our evaluation tool (Fig. 5), which has two stages. In the first stage, we generate traces of the input *tock-CSP* and its corresponding translated TA, using both FDR and UPPAAL. Then, we compare the generated traces; if they do not match, it may be because FDR distinguishes different permutations of events (traces). In contrast, UPPAAL uses a logical formula to generate traces [5, 22] which do not distinguish traces with different permutations. So, we move to a second stage, where we use FDR to complement UPPAAL in generating traces.

Essentially, UPPAAL checks if a system satisfies its requirement specifications (logical formula), irrespective of the behaviour of the system. For example, UPPAAL does not distinguish between the two traces  $\langle e1, e2, e3 \rangle$  and  $\langle e1, e3 \rangle$ , if both traces satisfy the requirement specification formula, such as a system performs the event  $e3$ , either through  $e2$  or before  $e2$ . However, FDR is capable of generating both traces. Thus, in the second stage, we use UPPAAL to check if all the traces of FDR are acceptable traces of the translated TA.

For evaluation, we have used a list of systematically formulated *tock-CSP* processes that pair the constructs of *tock-CSP*. The list contains 111 processes. Archives of the processes and their traces are available in a repository [1].

In addition, we test the translation technique with larger examples from the literature, such as an automated barrier to a car park [33], a thermostat machine for monitoring ambient temperature [33], an Automated Teller Machine (ATM) [32], a bookshop payment system [33], and a railway crossing system [31]. An overview of these case studies is in Table 1, while the details, including the traces, are also available in the repository of this work [1].

Considering that the experimental approach with trace analysis is an approximation for establishing correctness with a finite set of traces, covering infinite sets of traces in proving correctness has to use mathematical proof.

**Table 1.** An overview of the case studies

No.	System	States	Transitions	Events
1	Thermostat machine	7	16	5
2	Bookshop payment system	7	32	9
3	Simple ATM	15	33	15
4	AutoBarrier system	35	84	10
5	Rail crossing system	80	361	12

## 4.2 Mathematical Proof

Here, we illustrate part of the proof using one of the base cases of the structural induction. A more detailed account of our proof can be found in [1, 2]. A TA is defined as the tuple<sup>6</sup> (Sect. 2). Consider TA1 as the translation of the process STOP (TA05 from Fig. 4), then mathematically TA1 is expressed as follows.

$$TA1 = (\{s1, s2\}, s1, \{ck\}, \{startID01\_4, tock\}, \\ \{(s1, startID01\_4, \emptyset, \emptyset, s2), (s2, tock, ck \leq 1, ck, s2)\}, \{\}) \quad (1)$$

In the language of TA, a path [3, 7] is a sequence of consecutive transitions that begins from the initial state. A trace [3, 7] (or word): is a sequence of actions in each path. In TA1, there is only one infinite path, the first transition from location  $s1$  to location  $s2$  and the second transition from location  $s2$  back to location  $s2$ , repeated infinitely. The traces on the path are as follows.

$$traces'_{TA}(TA1) = \{\langle \rangle\} \cup \{\langle startID01\_4 \rangle \wedge \langle tock \rangle^n \mid n \in \mathbb{N}\} \quad (2)$$

The function  $trace'_{TA}(TA)$  computes the traces of the translated TAs generated by our translation technique. It takes a list of networked TAs and returns a set of traces. For instance, in Eq. 2, the first empty trace is for the initial state of the TA, before the first transition; the action  $startID01\_4$  happens on the first transition; the action  $tock$  happens on the second transition, which is repeated infinitely for the infinite traces  $\langle tock \rangle^n$ .

Another function  $trace_{TA}(TA)$  is similar to  $traces'_{TA}(TA)$  but removes all the coordinating actions (Definition 1) from the traces.

$$traces_{TA}(TA) = \{t \setminus CoordinatingActions \mid t \in traces'_{TA}(TA)\} \quad (3)$$

Therefore, without coordinating actions, the traces of TA1 become:

$$traces_{TA}(TA1) = \{\langle tock \rangle^n \mid n \in \mathbb{N}\} \quad (4)$$

<sup>6</sup> TA =  $(L, l_0, C, A, E, I)$  where  $L$  is a set of locations,  $l_0$  is the initial location,  $C$  is a set of clocks,  $A$  is a set of actions,  $E$  is a set of edges and  $I$  is an invariant.

Our goal is to establish that the traces of *tock-CSP* models are the same as those of the translated TA models. Here,  $\text{tranSTA}$  is the translation function we have formalised for translating *tock-CSP* models into TA models. Thus, for each valid *tock-CSP* process  $P$ , within the scope of this work, we need to establish the following theorem.

**Theorem 1.**

$$\text{traces}_{\text{tock-CSP}}(P) = \text{traces}_{\text{TA}}(\text{transTA}(P)) \quad (5)$$

*Proof.* For each translation rule, we have to prove that the translated TAs capture the behaviour of the corresponding input *tock-CSP* model  $P$ .

Starting with the basic process  $\text{STOP}$ , Eq. 5 becomes

$$\text{traces}_{\text{tock-CSP}}(\text{STOP}) = \text{traces}_{\text{TA}}(\text{transTA}(\text{STOP})) \quad (6)$$

Using structural induction in Haskell, we show that:

```

1 (traces_tockCSP n STOP = traces_TA n (transTA STOP))
2 => (traces_tockCSP (n+1) STOP = traces_TA (n+1) (transTA
      STOP))

```

Each step is evaluated automatically. The detailed steps of the proof are available in the extended reports [1, 2].

## 5 Related Work and Conclusions

Timed-CSP [33] is another popular extension of CSP for capturing temporal specifications. Unlike *tock-CSP*, Timed-CSP records the progress of time with a series of positive real numbers. However, the approach of Timed-CSP cannot specify deadline nor urgency. Also, traces of Timed-CSP are infinite, which is problematic for automatic analysis and verification [31]. Thus, there is no proper tool support for verifying Timed-CSP models. Therefore, researchers have explored various approaches, such as model transformations in translating Timed-CSP into *tock-CSP* for using FDR in automatic verification [29]; translation of Timed-CSP into UPPAAL, initially reported in [9] and then subsequently improved in [14]; and translation of Timed-CSP into Constraint Logic Programming (CLP) for reasoning with the constraint solver CLP(R) [10]. Additionally, using PAT for verifying Stateful Timed CSP (a variation of Timed-CSP) [34] and using FDR for verifying a variation of Timed-CSP [30].

However, there is less focus on applying the same transformation techniques for *tock-CSP*. Although, an attempt to transform TA into *tock-CSP* was proposed in [21], in this work, we consider the opposite direction.

Apart from CSP and TA, model transformations have been used for improving various formal modelling notations. For instance, Circus has been translated into CSP || B for using the tool ProB for automatic verification [36]. Additionally, the language B has been translated into TLA+ for automatic validation with

TLC [16]. Also, translating TLA+ to B has been investigated for automated validation of TLA+ with ProB [15], such that both B and TLA+ benefit from the resources of each other, and their supporting tools ProB and TLC, respectively.

In conclusion, we have presented a technique for translating *tock-CSP* into TA for UPPAAL to facilitate using temporal logic and facilities of UPPAAL in verifying *tock-CSP* models. This work contributes an alternative way of using TCTL to specify liveness requirements and other related requirements that are difficult to verify in *tock-CSP* with refinement. Also, our work sheds light into the complex relationship between *tock-CSP* and TA (temporal logic model).

Currently, we have used trace analysis to justify the correctness of the translation work. Also, we translate the event `tock` into an action that is controlled by a timed clock in UPPAAL. A next step is to relate the notion of `tock` to the notion of time in TA and get rid of `tock` as an action. This additional extension will help us to explore additional interesting facilities of UPPAAL to verify temporal specifications. Also, in future work, a better understanding of relating *tock-CSP* to TA will help us to explore using a single TA instead of network TAs for more efficient verification.

**Acknowledgements.** Abba gratefully acknowledges the financial support of Petroleum Technology Development Fund (PTDF). Cavalcanti is funded by the Royal Academy of Engineering grant CiET1718/45 and the UK EPSRC grants EP/M025756/1 and EP/R025479/1.

## References

1. A repository of this work. <https://github.com/ahagmj/TemporalReasoning.git>
2. Abba, A.: Temporal reasoning about robotics applications: refinement and temporal logic. Ph.D. thesis, The University of York (2021)
3. Alur, R., Dill, D.: A theory of timed automata. *Theor. Comput. Sci.* **126**, 183–235 (1994)
4. Back, R.: On correct refinement of programs. *J. Comput. Syst. Sci.* **23**(1), 49–68 (1981)
5. Behrmann, G., David, A., Larsen, K.G., Håkansson, J., Petterson, P., Wang, Y., Hendriks, M.: UPPAAL 4.0. *Third Int. Conf. Quant. Eval. Syst. QEST 2006* pp. 125–126 (2006). <https://doi.org/10.1109/QEST.2006.59>
6. Bouyer, P.: Model-checking timed temporal logics. *Electr. Notes Theor. Comput. Sci.* **231**, 323–341 (2009)
7. Bouyer, P.: An introduction to timed automata. In: Seatzu, C., Silva M., van Schuppen J. (eds) *Control of Discrete-Event Systems. Lecture Notes in Control and Information Sciences*, vol. 433, pp. 79–94. Springer, London (2011). [https://doi.org/10.1007/978-1-4471-4276-8\\_9](https://doi.org/10.1007/978-1-4471-4276-8_9)
8. Clarke, E.M., Emerson, E.A., Sistla, A.P.: Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Trans. Program. Lang. Syst. (TOPLAS)* **8**(2), 244–263 (1986)
9. Dong, J.S., Hao, P., Qin, S., Sun, J., Yi, W.: Timed automata patterns. *IEEE Trans. Softw. Eng.* **34**(6), 844–859 (2008)

10. Dong, J.S., Hao, P., Sun, J., Zhang, X.: A Reasoning method for timed CSP based on constraint solving. In: Liu, Z., He, J. (eds.) ICFEM 2006. LNCS, vol. 4260, pp. 342–359. Springer, Heidelberg (2006). [https://doi.org/10.1007/11901433\\_19](https://doi.org/10.1007/11901433_19)
11. Evans, N., Schneider, S.: Analysing time dependent security properties in CSP using PVS. In: European Symposium on Research in Computer Security. pp. 222–237. Springer (2000)
12. de Freitas, A.F.: From Circus to Java: Implementation and verification of a translation strategy. Master’s thesis, University of York (2005)
13. Gibson-Robinson, T., Armstrong, P., Boulgakov, A., Roscoe, A.W.: FDR3: a parallel refinement checker for CSP. *Int. J. Softw. Tools Technol. Transf.* **18**, 149–167 (2016)
14. Göthel, T., Glesner, S.: Automatic validation of infinite real-time systems. In: 2013 1st FME Workshop on Formal Methods in Software Engineering (FormaliSE), pp. 57–63. IEEE (2013)
15. Hansen, D., Leuschel, M.: Translating TLA+ to B for validation with ProB. In: International Conference on Integrated Formal Methods, pp. 24–38. Springer (2012)
16. Hansen, D., Leuschel, M.: Translating B to TLA+ for validation with TLC. In: International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z, pp. 40–55. Springer (2014)
17. Hoare, C.A.R.: Communicating sequential processes. *Commun. ACM* **21**(8), 666–677 (1978)
18. Hutton, G.: Programming in Haskell. Cambridge University Press, Cambridge (2016)
19. Isobe, Y., Moller, F., Nguyen, H.N., Roggenbach, M.: Safety and line capacity in railways – an approach in timed CSP. In: Derrick, J., Gnesi, S., Latella, D., Treharne, H. (eds.) IFM 2012. LNCS, vol. 7321, pp. 54–68. Springer, Heidelberg (2012). [https://doi.org/10.1007/978-3-642-30729-4\\_5](https://doi.org/10.1007/978-3-642-30729-4_5)
20. Kahani, N., Bagherzadeh, M., Cordy, J.R., Dingel, J., Varró, D.: Survey and classification of model transformation tools. *Softw. Syst. Model.* **18**(4), 2361–2397 (2018). <https://doi.org/10.1007/s10270-018-0665-6>
21. Khattri, M.: Translating timed automata to tock-CSP. In: Proceedings of the 10th IASTED International Conference on Software Engineering, SE 2011 (2011)
22. Lindstrom, B., Pettersson, P., Offutt, J.: Generating trace-sets for model-based testing. In: The 18th IEEE International Symposium on Software Reliability (ISSRE’07), pp. 171–180. IEEE (2007)
23. Lowe, G.: Specification of communicating processes: temporal logic versus refusals-based refinement. *Form Aspect. Comput.* **20**(3), 277–294 (2008)
24. Mens, T., Van Gorp, P.: A taxonomy of model transformation. *Electr. Notes Theoret. Comput. Sci.* **152**, 125–142 (2006)
25. Miyazawa, A., Ribeiro, P., Li, W., Cavalcanti, A., Timmis, J., Woodcock, J.: RoboChart: a State-Machine Notation for Modelling and Verification of Mobile and Autonomous Robots. *Tech. Rep.* pp. 1–18 (2016)
26. Nielson, H.R., Nielson, F.: Semantics with Applications: an Appetizer. Springer Science & Business Media, London (2007)
27. Nogueira, S., Sampaio, A., Mota, A.: Guided test generation from CSP models. In: International Colloquium on Theoretical Aspects of Computing. pp. 258–273. Springer, Cham (2008). <https://doi.org/10.1007/978-3-030-85315-0>
28. Oliveira, M.V.M.: Formal derivation of state-rich reactive programs using Circus. Ph.D. thesis, University of York (2005)



29. Ouaknine, J.: Discrete analysis of continuous behaviour in real-time concurrent systems. Ph.D. thesis, University of Oxford (2000)
30. Ouaknine, J., Worrell, J.: Timed-CSP = closed timed  $\varepsilon$ -automata. *Nordic J. Comput.* **10**(2), 99–133 (2003)
31. Roscoe, A.W.: *Understanding Concurrent Systems*. Springer Science & Business Media, London (2010)
32. Roscoe, A., Hoare, C., Bird, R.: *The theory and practice of concurrency*. 2005. Revised edition. Only available online (2005)
33. Schneider, S.: Concurrent and real time systems: the CSP approach. In: *World Scientific Proceedings Series on Computer Engineering and Information Science* (2010)
34. Sun, J., Liu, Y., Dong, J.S., Liu, Y., Shi, L., André, E.: Modeling and verifying hierarchical real-time systems using stateful Timed-CSP. *ACM Trans. Softw. Eng. Methodol.* **22**(1) (2013). <https://doi.org/10.1145/2430536.2430537>, <https://doi.org/10.1145/2430536.2430537>
35. Sun, J., Liu, Y., Dong, J.S., Pang, J.: PAT: towards flexible verification under fairness. In: Bouajjani, A., Maler, O. (eds.) *CAV 2009*. LNCS, vol. 5643, pp. 709–714. Springer, Heidelberg (2009). [https://doi.org/10.1007/978-3-642-02658-4\\_59](https://doi.org/10.1007/978-3-642-02658-4_59)
36. Ye, K., Woodcock, J.: Model checking of state-rich formalism by linking to *CSP* || *B. Int. J. Softw. Tools Technol. Transf.* **19**(1), 73–96 (2017)