Correct coordination of ECA rules by verification and control

Julio Cano\textsuperscript{1}, Gwenael Delaval\textsuperscript{2}, and Eric Rutten\textsuperscript{1}

\textsuperscript{1} INRIA, Grenoble, France, julio-angel.cano-romero@inria.fr, eric.rutten@inria.fr
\textsuperscript{2} LIG / UJF, Grenoble, France, gwenael.delaval@inria.fr

Abstract. Event-Condition-Action (ECA) rules are a widely used language for the high level specification of controllers in adaptive systems, such as Cyber-Physical Systems and smart environments, where devices equipped with sensors and actuators are controlled according to a set of rules. The evaluation and execution of every ECA rule is considered to be independent from the others, but interactions of rule actions can cause the system behaviors to be unpredictable or unsafe. Typical problems are in redundancy of rules, inconsistencies, circularity, or application-dependent safety issues. Hence, there is a need for coordination of ECA rule-based systems in order to ensure safety objectives. We propose a tool-supported method for verifying and controlling the correct interactions of rules, relying on formal models related to reactive systems, and Discrete Controller Synthesis (DCS) to generate correct rule controllers.

1 Coordination problems in ECA rules

Event-Condition-Action (ECA) rules is defined in [12] as a set of rules where each of them 'autonomously reacts to actively or passively detected simple or complex events by evaluating a condition or a set of conditions and by executing a reaction whenever the event happens and the condition is true'. The form of the rule is: \textbf{ON Event IF Condition DO Action}. Some characteristics are that:

- a rule is activated only by events;
- its execution is autonomous and independent of other rules in the system;
- it implements a reaction to the incoming event;
- it contains a guarding condition to execute such actions.

Many research work on ECA rules systems are related to active database management systems (ADBMS) [2,13]. Events represent modifications produced in the database, and ECA rules are used to control it the integrity. But they have also been used in different control environments [7] or adaptation frameworks [9], which means that there are many different implementations of ECA rule-based systems.

The nature of ECA rule-based systems shows several different problems in their execution. As described in [17], the most extended problems are redundancy, inconsistency and circularity.
Redundancy means that there are two (or more) rules in the system whose functionality is replicated. This can happen in large rule systems where rules are written by different persons. An example in a smart home automated system is to have two similar rules: one detects the presence of a person in a room and, if temperature is lower than 15 degrees, then turns on room heaters. The other rule does the same, but also closes the room door. This can be described in ECA syntax as follows (rule numbers are indicated here only for reference, a concrete grammar is described later in Section 3):

rule1: ON presence IF (temperature_get < 15) DO heater_on
rule2: ON presence IF (temperature_get < 15) DO heater_on, door_close

This represents an overload in the rules system in the best of cases, and an undesired repetitive activation of orders on environment devices.

Inconsistency occurs when contradictory actions are sent to devices. This can also occur if multiple rules are activated at the same time, and their execution order may render different final states in the system. An example is: lights are activated by the presence of a person in the room, and TV will also be activated. A third rule will turn off the lights then the TV is turned on.

rule1: ON presence IF true DO lights_on
rule2: ON presence IF true DO TV_on
rule3: ON TV_light IF TV_on DO lights_off

Depending on the order of execution of rules, the final state of the system will be different. If rules 2 and 3 are activated before rule 1 is executed then the final state of lights will be different than executing rule 1 before rule 3. So the result of the execution of these rules is not predictable.

Circularity occurs when rules get activated continuously without reaching a stable system state that makes them finish their execution. Rules can be repeatedly activated without termination condition. Supposing that two lights in a room are programmed with different behaviors in mind, the following rules generate a circularity problem:

rule1: ON light1_change IF light1_on DO light2_off
rule2: ON light1_change IF light1_off DO light2_on
rule3: ON light2_change IF light2_on DO light1_on
rule4: ON light2_change IF light2_off DO light1_off

The first two rules will try to change the second light to a state different from the first light. The third and fourth rules will try to maintain both lights in the same state. This will continuously generate a continuous circular execution if not detected.

Application-specific issues can be considered additionally in an environment. An example is ordering to open a windows and to turn on the room heaters. It can be considered as a contradiction by the user. In order to know which actions are contradictory, specific information must be provided about the environment.
In this paper we will consider that multiple actions sent to the same device are contradictory. Only one action can be requested to every device at every instant.

Coordinating ECA rules is therefore necessary in order to enforce safety properties. One of the problems of ECA rules is that they are considered to be executed independently or autonomously. This means that possible interactions between rules and their effects are not controlled. In contrast, synchronous reactive languages, used to design and program control systems, provide some characteristics, such as determinism and verifiability [8]. This is useful for the safe execution of control systems. The objective of this work is to provide validation of the ECA rule system before and during the execution of the system, by relating them to synchronous languages. Here, safety is meant for the control system and people in the environment controlled by this control system. The system should not go into undesired states, and controlled devices are considered part this state.

Our approach proposed in this paper consists of a model transformation from an ECA rules description to a synchronous programming language. The characteristics of this programming language will be used to validate the set of rules. ECA rule systems are validated, detecting the described issues. Rules execution is also controlled and coordinated to avoid the described problems at run-time.

We will concentrate on small or home environment as target systems, although our results are generic enough to be applied in any ECA rule-based system. The Heptagon/BZR programming language [1] is used here to model the ECA rule-based system, including different execution policies. This language is used because of its capability to express invariants in the system in the form of contracts, which allows verifying the application by the use of model checking as well as controlling or coordinating the execution of the application according to the described invariants.

The following section describes related work to validate or verify ECA rule systems. Section 3 formalizes the ECA models used in this paper. Section 4 shows how ECA rules are translated into a synchronous programming language to profit of its intrinsic characteristics. Section 5 shows how we perform verification and control on rule systems. Finally, in Section 6, we show some conclusions and future works.

2 State of the art

2.1 ECA rule based control systems and their validation

ECA rule systems are widely used to control the environment as well as to control reconfiguration of software systems. Here are described the closest proposals to our approach and ECA rule-based systems verification and validation. In [9], an adaptation framework is proposed. It detects the state of the system in the form of events. When these events are detected the associated rules can be applied. These rules will perform the required actions according to the detected state, to adapt the behavior of the system to the changes of the environment. In [15,16], a
method is proposed to design applications with reconfiguration capabilities. At design time, invariants can be described for every state and transitions between states. These invariants are used in the design of Petri Nets representing the desired behavior of the application. Designed Petri Nets can be used to check the previously defined invariants and to create prototypes of the system. The system is supposed to be safe by design, if the design is correctly translated to the implementation. No control is performed at run-time about the specified invariants. A mixture of rule based system and utility functions is proposed in [4]. Rules are mainly used to change the priorities for the utility functions when a state change is detected. The number of possible available configurations can grow exponentially, so the calculation of the utility functions at run-time takes time.

The following work cover basic aspects in verification and validation of ECA rule systems. In [14], a way to validate a set of rules in a knowledge based systems is proposed. It defines different types of rules to create a rule net consisting of chained rules, which explicitly invoke other rules. In the rule net, it checks if different paths contain inconsistencies according to the constraints defined in the system or other rules. In [10], an infrastructure is described to detect and solve static (compilation time) and dynamic (execution time) conflicts for a framework of WS-ECA. This framework is based in the use of ECA rules for Web Services. The existence of distributed devices with their own rules may lead to conflicting rules. No implementation is described for this infrastructure.

In [17], a more complete proposal is described to verify an ECA rule based system. It starts formalizing the system to be able to define the problems of redundancy, inconsistency and circularity. Three levels are described regarding the verification and validation of these problems. Level 1 refers only to rule set level, where no information about run-time execution is considered. Level 2 takes into account direct results of the execution of actions on the environment. This means actions that will directly provoke new events activating rules. Level 3 takes into account all the possible responses of the environment, which cannot be previously known because they are completely random or unpredictable. Certain problems can only be verified at some levels because of the required information to perform such verifications. In [3], a method is provided to verify ECA rule systems with formal methods, transforming the ECA rules set into a set of different kinds of automata for every part of the process, and using the automata verification tool Uppaal. This verification is limited to performing model checking of timed automata and their correspondence to the provided ECA rule set.

Every ECA rule-based system implementation imposes different execution semantics. These semantics can vary from parallel synchronized execution of rules to execution in depth first and discard of previously activated rules. So the result of the execution of a rule set differs depending on the execution policy of the implementation. All the proposals described here are centered in one kind of ECA rule system execution policy, or they do not take into account that results depend on the execution policy used by every different implementations. Here
we propose a solution that takes into account the desired execution policy of the target implementation to verify an ECA rules set.

2.2 Synchronous reactive programming and Heptagon/BZR

Reactive systems are interactive systems that constantly communicate with their environment taking into account the timing needs of this environment [8]. These systems will work reacting to received events or by sampling incoming signals. Synchronous programming languages allow programming of reactive systems using automata, where reactions will correspond to the automata transitions. Computations and transitions performed by composed automata are considered to occur in parallel at the same time instant. This intrinsic synchronism makes it easier to preserve the determinism, and allows these programming languages to be based on sound formal semantics. Thus, these languages are provided with tools for the verification (e.g., by automated test or model-checking) or control (e.g., by controller synthesis) of programs.

Heptagon/BZR [1] is a synchronous dataflow programming language with support for equations and automata. This language also provides a contract mechanism allowing the use of discrete controller synthesis (DCS) within the compilation, using the Sigali synthesis tool [11]. The discrete controller synthesis method is based in partitioning input variables into controllable and uncontrollable ones. For a given objective, such as staying in a subset of states, its DCS algorithm will automatically compute, by symbolic exploration of the state space, the constraint on controllable variables, so that the behavior satisfies the objective, whatever be the values of the inputs from the environment. Figure 1(a) represents the control loop. The automata-based program is in charge of controlling the environment. The behavior of the automata is constrained by the synthesized controller, which is in charge of maintaining the system in the desired subset of states. The main elements of a Heptagon/BZR program are:

- Nodes: blocks of equations or automata with input and output signals
- Equations: determining the value of node outputs. A set of equations in parallel are separated by semicolons.
- Automata: mode automata using states, input and output signals.
- Contracts: describing invariants to be enforced by control at execution.

The compiler generates executable code in C or Java. Figure 1(b) shows an example of Heptagon/BZR code. It contains a delay node, with an automaton which makes use of a controlled variable to delay the emission of a received signal. A main node makes use of this automaton. It includes a contract to enforce that both signals are not emitted at the same time. Heptagon/BZR makes use of Sigali at compilation time to synthesize the needed controller that will provide the correct value for every controlled variable (c1 and c2), and hence forcing the delay of one of the signals.

The control variable (c) in Figure 1(b) determines when the signal has to be delayed. When a new_sig is received, depending on the value of the controlled
variable; the new\_sig value is emitted (staying in the Idle state) or delayed (performing a transition to the Waiting state) until the controlled variable indicates that it can be released. The value of the out variable is described in function of new\_sig and the controlled variable. Automata transitions will be effective in the next step of its execution. To avoid delays in the desired automaton output, the value of the out variable is described in function of new\_sig and the controlled variable. This allows emitting the desired value in the same execution step.

Heptagon/BZR has been used by some work in smart home / environment context, to design safe control systems. In [18], Heptagon/BZR is proposed for the autonomic management of small environments. The behavior of devices is represented using automata and control objectives are described as contracts. For instance, it can avoid the request to turn on a device if it can generate an energy consumption higher than the specified. In [6], a similar approach is proposed to provide safe environment for disabled people. However, none of these works featured ECA rules as a high-level description language. In another domain, the coordination of multiple autonomic loops in adaptive computing systems has been approached with a discrete control approach [5].

3 Modeling ECA

Here we describe a formalization of an ECA rule-based system to be able to translate it into a Heptagon/BZR program. The ECA rule-based system is assumed to be connected to the physical world through devices that may work as sensors or actuators. The control system loop is generated providing devices
A rule-based system \( S = (R, E, D) \) is composed of a set of rules \( R \), a set of events \( E \) and a set of devices \( D \). We consider that rules, events, devices and signals are identified by unique names, taken in a name set \( N \). Thus, events are names, i.e., \( E \subseteq N \).

Devices \( d \in D \) are a virtual representation of physical devices in the system as sensors and actuators. A device \( d = (n, I, O) \), named \( n \), is composed of a set of input signals \( I \subseteq N \) and a set of output signals \( O \subseteq N \). In the following, we will denote by \( \text{Expr}(O) \) the set of Boolean expressions defined on the set of output signals \( O \).

The function \( \text{EventExpr} \in E \rightarrow \text{Expr}(O) \) maps events to Boolean expressions based on output signals received from devices. The event \( e \in E \) is activated whenever the expression \( \text{EventExpr}(e) \) is true.

Rules \( r \in R \) are defined by a tuple \( r = (n, e, c, A) \), where \( n \in N \) is the name of the rule, \( e \in E \) the activating event, \( c \in \text{Expr}(O) \) the condition, and \( A \subseteq I \) a set of actions to perform. The condition is a Boolean expression based on the output of devices. If the event occurs and the condition is true, the corresponding actions will be performed.

Figure 2 shows the concrete grammar used by the implemented tool to translate a ECA rule-based system into a Heptagon/BZR program. The descriptions contain lists of events, rules and devices. Events can be internal (generated by rules as an action, indicated by the \( \text{INTERNAL} \) term) or be generated if the described expression becomes true (when the term \( \text{IF} \) is used in its description).

Rules contain the event name that activates them (preceded by term \( \text{ON} \)), a Boolean expression to determine if certain conditions apply (preceded by term \( \text{IF} \)), and the list of actions that have to be performed if event and condition are true (preceded by term \( \text{DO} \)).

The device contains the device name, a specification of the policy to be used in the device when multiple simultaneous actions are sent to this device, a list of inputs and a list of outputs of the device. The term \( \text{SIMULTANEOUS} \) allows specifying the policy used when multiple signals are sent to the same device. \( \text{DISCARD} \) allows discarding all the signals but one. \( \text{DELAY} \) allows delaying all the signals but one. Delayed signals will be emitted later, in following executions of
the controller, in order of priority. The priority in all cases is given by the order in which input and output signals are declared. Inputs and outputs are optional in the description of the device. At least one should be indicated. If the device policy is not specified, the default value is DISCARD.

EVENT presence:BOOL IF presence_get
EVENT TV_lights:BOOL IF TV_on
EVENT light1_change IF light1_on or light1_off
EVENT light2_change IF light2_on or light2_off

ON presence IF (temperature_get < 15) DO heater_on
ON presence IF (temperature_get < 15) DO heater_on, door_close
ON presence IF true DO light1_on
ON presence IF true DO TV_on
ON TV_lights IF TV_on DO light1_off
ON light1_change IF light1_on DO light2_off
ON light1_change IF light1_off DO light2_on
ON light2_change IF light2_on DO light1_on
ON light2_change IF light2_off DO light1_off

DEVICE presence OUTPUTS (get:BOOL)
DEVICE temperature OUTPUTS (get:BOOL)
DEVICE light1 SIMULTANEOUS DISCARD INPUTS (on:BOOL, off:BOOL) OUTPUTS (on:BOOL, off:BOOL)
DEVICE light2 SIMULTANEOUS DISCARD INPUTS (on:BOOL, off:BOOL) OUTPUTS (on:BOOL, off:BOOL)
DEVICE TV SIMULTANEOUS DELAY INPUTS (on:BOOL, off:BOOL) OUTPUTS (on:BOOL, off:BOOL)

Figure 3 shows an example of how a system can be described textually according to the proposed grammar. Rules from the introduction section are included here. Events required to activate the rules are declared. As an example, \textit{light1\_change} will be activated if light1 is turned on or off.

The needed devices for the example are also described. A \textit{presence} and \textit{temperature} sensors are used. They only have outputs.

![Fig. 4. Heptagon/BZR code detailed model](image-url)
4 Transformation to synchronous language

We propose a transformation to Heptagon/BZR code from the described ECA rule-based system. As shown in Figure 4, the generated Heptagon/BZR program will be defined in the body of a main node. This node is structured into three sub-nodes named events, rules and devices. The main node will receive all the sensor signals from the devices. The events node will use them to determine if events occur according to their definition. Events and devices signals are then passed to the rules node, where rules are activated according to their firing event and condition. Actions corresponding to activated rules are then used in the devices node, to be processed before being sent to devices, according to the corresponding device policy. The Rule Engine contains the execution policy to be simulated, determining the behavior of the rule-based system. Its output is the activated internal events, according to the specified policy.

Fig. 5. Program structure in Heptagon/BZR

4.1 Code transformations

Figure 5 shows the skeleton for the code generated from a textual representation of an ECA rule-based system according to the grammar of Figure 2, with terms
that are defined in the following. The order of the program is that nodes are defined before being used as sub-nodes in later nodes. The main node (e) invokes the sub-nodes events (defined in (a)), rules (c) and devices (d) nodes. The rules node (c) invokes the sub-node rule_engine (b), which models the execution policy, as described in 4.2. Event detectors, rules and devices are translated as lists of equations inside of the indicated nodes.

The developed tool implements several transformation schemes to translate events, rules and devices descriptions into Heptagon/BZR code, which are described for every element. We consider an ECA system $S = (R, E, D)$. The function name is used to define Heptagon/BZR variable names from the set $N$ of rules, events and devices names. We consider for the sake of clarity and simplicity that Boolean expressions in the ECA language corresponds to the Heptagon/BZR ones, and thus they can be used as they are.

\begin{align*}
\text{<devices_outputs>} &= \{ \text{name}(n), \text{name}(o) \mid (n, I, O) \in D, o \in O \} \\
\text{<event_names>} &= \{ \text{name}(e) \mid e \in E \} \\
\text{<event_detection>} &= \{ \text{name}(e) = \text{EventExpr}(e) \mid e \in E \} \\
\text{<rule_names>} &= \{ \text{name}(n) \mid (n, e, c, A) \in R \} \\
\text{<rules_activation>} &= \{ \text{name}(n) = \text{final}_\text{name}(e) \& c \mid (n, e, c, A) \in R \} \\
\text{<signals_activation>} &= \{ \text{name}(a) \lor \bigvee_{(n,e,c,A) \in R, a \in A} \text{name}(n) \mid \exists(n, I, O) \in D, a \in I \}
\end{align*}

Fig. 6. Transformations for various sets

Figure 6 gives transformations to Heptagon/BZR for several terms. The <device_outputs> list is generated over all the devices and their corresponding outputs. Similarly, we can generate <device_inputs>. The <final_event_names> list is build similarly to <event_names>, but adding the “final_” prefix, to differentiate inputs and outputs of the rule_engine node. Other lists are created similarly, <request_devices_inputs> and <temp_event_names>, but adding “req_” or “temp_” prefixes respectively to the names in their counterpart lists.

The <rules_activation> defines the Boolean corresponding to activation of a rule if the corresponding event and its condition are true at the same time. Then, <signals_activation> allows activating every device input if it has been requested by any of the rules. Given that multiple rules could activate the same signal, a disjunction is used to fuse them.

Transformation for devices differs depending on the specified execution policy to apply on signals sent to the device. Actions from rules correspond to devices inputs. The two specified strategies are discarding or delaying contradictory signals sent to a device. Equations are used in the first case, shown in Figure 7, to discard contradictory signals: the total order $\prec$ is used to give priorities. Once a signal with higher priority has already been activated, the rest are discarded. The <device_policy> equations are composed for every device in the system. In the second case, shown in Figures 8, a contract is used to delay signals. Only
\[<\text{device\_policy\_contracts}> = \text{true}\]
\[<\text{device\_policy\_control\_labels}> = \emptyset\]
\[<\text{device\_policy}> = \{\text{final\_name}(n)\_\text{name}(o) = \text{req\_name}(n)\_\text{name}(o)\]
\[\quad \text{and not } \bigvee_{o' \in O, o \prec o'} \text{final\_name}(n)\_\text{name}(o') \mid (n, I, O) \in D, o \in O\}\]

Fig. 7. Transformation for devices (discarding policy)

\[<\text{device\_policy\_contracts}> = \bigwedge_{(n, I, O) \in D, o_1, o_2 \in O, o_1 \neq o_2} \text{not (final\_name}(n)\_\text{name}(o_1) \& \text{final\_name}(n)\_\text{name}(o_2))\]
\[<\text{device\_policy\_control\_labels}> = \{\text{name}(n)\_\text{name}(o)\_c \mid (n, I, O) \in D, o \in O\}\]
\[<\text{device\_policy}> = \{\text{final}_m = \text{delay}(\text{req}_m, m\_c) \mid (n, I, O) \in D, o \in O, m = \text{name}(n)\_\text{name}(o)\}\]

Fig. 8. Transformation for devices (delaying policy)

one of them is sent to the device. The delay automaton from Figure 1 will store the input signal until it can be released and sent to the device. The generated controller will be in charge of selecting the right values for the controlled variables to send only one signal at a time and delay the others.

4.2 Execution models

As described before, the transformation has been designed to support different execution policy models in ECA rule-based systems. Execution models currently accepted by the transformation tool are parallel and delayed execution. The code generation for the rule_engine node will differ for every case.

For the delay of events, as shown in Figure 9, the delay automaton is used as for the device node code generation. Only one event will be sent to the rules node for every execution of the controller.

For the parallel execution model, as shown in Figure 10, all the events are allowed to be activated in the same execution step without restrictions. Other execution policies can be added in this node to simulate any ECA execution model.

node rule_engine(<event\_names>) returns (<final\_event\_names>)
contract
  enforce \[\land_{e_1, e_2 \in E, e_1 \neq e_2} \text{not (final\_name}(e_1) \& \text{final\_name}(e_2))\]
  with \{\text{name}(e)\_c \mid e \in E\}\nlet
  \{\text{final\_name}(e) = \text{delay}(\text{name}(e), \text{name}(e)\_c) \mid e \in E\}\ntel

Fig. 9. Delayed execution model
node rule_engine(<event_names>) returns (<final_event_names>)
let
  { final_name(e) = name(e) | e ∈ E }

tel

Fig. 10. Parallel execution model

5 ECA rule set verification and control

Due to the transformation into a Heptagon/BZR program, the ECA problems described in Section 1 can be verified or controlled. We describe how the generated code is used to validate, verify or control the execution of the ECA rule set. Run-time situations can not be verified at compilation time, but the behavior of the rule set can be controlled to obtain safe results.

Different kinds of verifications can be performed on the ECA rule based system, depending on the available information, as described in [17]. Verifications can be static (performed at compilation time) or dynamic (performed at run-time). They can also be classified as generic ECA rule verifications or domain specific issues that can verified. Here are described the verifications that can be performed due to the described transformation of the ECA model into a synchronous programming model.

5.1 Verifications at compilation time

The first verification to be performed is the detection of syntax errors. The use of undeclared events or unavailable device actions are examples of such errors in the declaration of rules. Syntax errors are easily detected by any compiler or interpreter when recognizing the ECA rules source code.

Redundancy Redundancy of rules is detected when the condition and actions of one rule represent a subset of conditions and actions of the other rule. This means that having two rules \( r_1 = (n_1, e_1, c_1, A_1) \) and \( r_2 = (n_2, e_2, c_2, A_2) \) where \( e_1 = e_2, c_1 ⇒ c_2 \) and \( A_1 ⊆ A_2 \).

Redundant rules are not directly detected by Heptagon/BZR. Duplicated rules will be compiled and executed at run-time without problems. Rule actions will be activated using the or operator, so the results will not result in redundancy. Here is a simple example of redundancy:

```plaintext
ON presence IF true DO Tv_on
ON presence IF true DO Tv_on
```

This example generates the following Heptagon/BZR code:

```plaintext
rule6 = (presence) & (true);
rule7 = (presence) & (true);
req_tv_on = rule6 or rule7;
```
The Sigali tool is used to solve this problem. The redundancy can be better checked using this tool. The capability of working with equations \([11]\) in Sigali is used to detect the situation where the condition of one rule is included in the condition of another rule, thus making them redundant. For Sigali this means that the solutions for the equation \(c_1 = \text{true}\) is a subset of the solutions of \(c_2 = \text{true}\). Sigali code performing this check is generated for every couple of rules that fulfill the following conditions:

- Rules are activated by the same event
- The set of actions of one rule is a subset of actions of the other one.
- The set of variables used in the conditions of both rules are not disjoint.

This filtering also helps reducing the quantity of operations in Sigali.

**Inconsistency** Inconsistency is also detected at compilation time. It can be defined as the result of contradictory actions, provided as result of activation of different rules. It can be formalized as having two rules \(r_1 = (n_1, e_1, c_1, A_1)\) and \(r_2 = (n_2, e_2, c_2, A_2)\) where \(e_1 = e_2\) and \(c_1 = c_2\), but \(A_1\) and \(A_2\) are contradictory. As previously defined in the introduction section, we consider as contradictory actions sending more than one signal to the same device at the same time. Due to having the same event and condition to be activated, they will always be activated at the same instant, generating contradictory actions. This verification is performed by compiling the corresponding Heptagon/BZR contracts on the device node, but not discarding or delaying signals. The Sigali tool will detect inconsistencies failing to generate the controller, indicating that the program is not executable regarding the contracts.

**Circularity** Circularity generated by internal events can be detected by Heptagon/BZR, for the case of the parallel execution model, as a causality error at compilation time. The following code generates a circularity problem:

```plaintext
ON internal1 IF true DO internal2
ON internal2 IF true DO internal3
ON internal3 IF true DO internal1
```

A dependency cycle occurs in the definition of rules in a way that these rules are always activating themselves. The circularity is detected independently of the number of involved events. The generated code is as follows:

```plaintext
rule0 = (internal3) & (true);
rule1 = (internal2) & (true);
rule2 = (internal1) & (true);
internal2 = rule2;
internal1 = rule0;
internal3 = rule1;
```

The dependency cycle will be detected by Heptagon/BZR as a causality error. Even if it is not completely precise, as conditions in rules may avoid this dependency, it is still a safe detection of dependencies that avoids any possible dependency cycle.
5.2 Control at run-time

It can not be foreseen at compilation time if two different rules with different events and contradictory actions will be activated at the same time instant at run-time. Coordination or control techniques have to applied in that case. Hep-tagon/BZR is designed to provide this kind of run-time control.

**Inconsistency** Inconsistency at run-time is controlled with the already described code generated for the devices. Contradictory signals can be discarded or delayed depending on the chosen policy. This provides more control on the execution of rules than avoiding the rules. In case that one rule has more than one action, only the inconsistent actions will be discarded or delayed, allowing the rest of actions to be performed. In this case, inconsistency is not only detected, as in the compilation time, but solved using the order priority to discard or delay signals.

**Application-specific issues** Additionally to the above generic ECA rule-based system issues, there exist specific scenarios with specific requirements. These requirements can also be expressed in Heptagon/BZR, to provide more control on the ECA rule set execution. These requirements are also difficult to express in ECA rules, because of the lack of language support to describe them, but their violation would cause inconsistencies during the execution.

```
node device(on, off: bool; c:bool) returns (st_on, st_off: bool; power:int)
let
  automaton
  state Off do st_off = true; st_on = false; power = 0;
  until on & c then On
  state On do st_on = true; st_off = false; power = CONSUMPTION;
  until off & c then Off
end
tel

node devices(req_d1_on, req_d1_off: bool; req_d2_on, req_d2_off: bool) returns (st1_on, st1_off: bool; ... ; power:int)
contract
  enforce (power ≤ LIMIT)
  with (dev1_c, dev2_c:bool)
var power1, power2:bool
let
  power = power1 + power2;
  (st1_on, st1_off, power1) = device1(req_d1_on, req_d1_off, dev1_c);
  (st2_on, st2_off, power2) = device1(req_d2_on, req_d2_off, dev2_c);
... 
tel
```

**Fig. 11.** Application-specific scenario behavior control

Additional information is required about the environment to be able to perform the specific control actions on the environment, following the approach in
An example of such application-specific scenario requirements would be to forbid an energy power consumption higher than a given threshold LIMIT. A model should be provided in the form of automata representing the devices behaviors. Figure 11 shows an automaton called device1, representing the behavior of one device type, with states On and Off, associated with consumption levels, here valued for the example at 0 and CONSUMPTION. A node called devices, shown here only partially, describes a composite system with two such devices, each represented by an instantiation of the former node. The overall power consumption is defined as the sum of local power consumptions. A contract is then declaratively specified, as defined in Section 2.2, such that the global power is lower than the given limit. DCS is applied during the compilation of this program, to automatically solve the control problem. The generated controller will avoid entering the On state of a device if it makes the total power consumption to overcome the threshold. An ECA rule would be able to detect the situation when it is already occurring, whereas DCS performs an analysis predicting possible problems, and the controller generated by Heptagon/BZR will directly avoid reaching the undesired state.

6 Conclusions

We propose a novel method for coordination in ECA rule-based systems, by verification and control based on behavioral models, in order to avoid problems of redundancy, inconsistency, and circularity, as well as application-specific issues. This method is based on the use of model checking and a control technique (DCS) which provides safe control during the execution of the system. Verifications are performed at compilation time with simple transformations and model checking, ensuring that the desired system defined invariants apply. So, for the execution of the ECA rule set, the generated controller ensures that the desired properties will always apply.

Our method also takes into account different possible execution models for the ECA rule-based system. These execution models can be modeled, ensuring that the final implementation of the system is correctly verified.

We are presently working on the integration of the generated controller, using the executable code in C or Java, in an experimental embedded platform for small or home environments where users could introduce ECA rules in the system to control home sensors and actuators using the automatically generated safe controller. We are also working on the possibility to automatically provide device models representing their behavior. This allows specifying, at the same level as ECA rules rather than in Heptagon/BZR, safety properties for application-specific scenarios as the one described in last section. Other perspectives involve modular compilation and DCS, which can improve scalability of the approach, as well as distribution of the executable code, to design distributed controllers.
References


