Hindawi Publishing Corporation
EURASIP Journal on Embedded Systems
Volume 2008, Article ID 251957, 9 pages
doi:10.1155/2008/251957

Research Article

Using Visual Specifications in Verification of Industrial Automation Controllers

Valeriy Vyatkin[1] and Gustavo Bouzon[2]

[1] *Department of Electrical and Computer Engineering, University of Auckland, Auckland 1142, New Zealand*
[2] *Controle Soluções em Mecatrônica Ltda., Rua Mauro Nerbass, 72, CEP 88024-420 Lages, SC, Brazil*

Correspondence should be addressed to Valeriy Vyatkin, v.vyatkin@auckland.ac.nz

Received 3 February 2007; Accepted 4 November 2007

Recommended by Jose L. Martinez Lastra

This paper deals with further development of a graphical specification language resembling timing-diagrams and allowing specification of partially ordered events in input and output signals. The language specifically aims at application in modular modelling of industrial automation systems and their formal verification via model-checking. The graphical specifications are translated into a model which is connected with the original model under study.

1. INTRODUCTION

Formal verification of industrial automation systems requires three constituent components: a model of the controller, a model of the uncontrolled plant, and a specification of desired or forbidden plant behaviour. Generation of the two first elements can be facilitated by application of modular modelling approaches and from automatic model-generation as described in [1].

However, languages commonly used for specification, such as temporal logic, are still rarely familiar to control engineers. So, the engineers would benefit from having user-friendly means of specifying the desired or forbidden behaviour of a model.

Inspired by the timing diagram specifications explored in the domain of digital systems design (e.g., by Fisler [2], Amla et al. [3], Schlör et al. [4]), a graphical language for describing the dependency of interface signal changes was proposed in [5], and some of its implementation issues were developed in [6].

In this paper, we harmonise the earlier developed specification and implementation techniques aiming at a solution that can be a part of an integrated verification framework. The underlying modelling language of the framework is the modular formalism of net condition/event systems (NCES) described in [7, 8]. The proposed visual language specifies the behaviour of NCES models and the verification technique also relies on the use of NCES. We suggest two procedures for translation and checking of visual specifications: one for verifying the output behaviour, and the other for combined input-output behaviour. The paper is organized as follows. Net condition/event systems are briefly introduced in Section 2. Timing diagrams as a means for specifying desired or forbidden behaviour of NCES models of automation systems are defined in Section 3. The transformation of timing diagrams to NCES modules is subject of Section 4. Section 5 describes the implementation of the method in a software prototype. Some conclusions are presented in Section 6.

2. NET CONDITION/EVENT SYSTEMS

The formalism of net condition/event systems (NCES) was introduced by Rausch and Hanisch [7] as a modular extension of signal/net systems (SNS)—a place-transition formalism for discrete state, discrete time modelling. The idea of signal/net systems is described as follows, following [9].

2.1. Definition of SNS

A signal/net system is a tuple $(P, T, F, V, B, W, S, M, m_0, \text{eft}, \text{lft})$, where P is a nonempty finite set of *places*; T is a nonempty finite set of *transitions* disjoint with P; F is the set of *flow arcs*, where $F \subseteq (P \times T) \cup (T \times P)$; V maps a weight

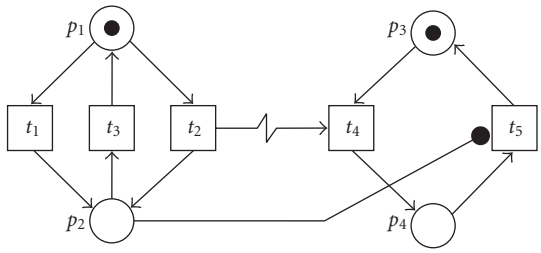

Figure 1: Signal-net system.

to every flow arc and V: $F \to \mathbb{N}$; B is the set of *condition arcs*, which carry condition signals and $B \subseteq P \times T$; W maps a weight to every condition arc and W: $B \to \mathbb{N}$; S is the set of irreflexive *event arcs*, which convey event signals and $S \subseteq T \times T$; M maps an event-processing mode (AND or OR) to every transition, M: $T \to \{\wedge, \vee\}$; m_0: $P \to \mathbb{N}_0$ is the initial marking of SNS, where for each place $p \in P$, there are $n_p \in \mathbb{N}_0$ tokens; eft maps the *earliest firing time* to every pre-arc $[p,t] \in F$, eft: $F \cap (P \times T) \to \mathbb{N}_0$; and lft maps the *latest firing time* to every pre-arc $[p,t] \in F$, lft: $F \cap (P \times T) \to \mathbb{N}_0 \cup \{\omega\}$, where $\omega \in \mathbb{N}$ and $0 \le \text{eft}(p,t) \le \text{lft}(p,t) \le \omega$. The interval $[\text{eft}(p,t), \text{lft}(p,t)]$ is called the *permeability interval*.

An example of SNS is presented in Figure 1. The model consists of four places and five net transitions. Places p_1 and p_3 have tokens at the initial marking. Besides ten token flow arcs, the transition t_2 is connected to t_4 via an event arc, and place p_2 is connected to t_5 via condition arcs.

2.2. State of SNS model

Places bear integer clocks whose values are denoted as u: $P \to \mathbb{N}_0$, where for each place $p \in P$, the clock reading in the place is denoted as $u_p \in \mathbb{N}_0$. All clocks have zero value at the initial state of the model. The clock of a place resets to zero anytime marking of the place changes.

A *state* in timed SNS is defined as a pair $z = [m, u]$, where m is a marking of P and u is the vector of the clock positions, such that $u(p) > 0 \to m(p) > 0$. Evolution of SNS consists of changing its states. A state change (also called *state transition*) can consist in changing net's marking, or changing values of clocks (elapsing of time).

In every state there could be some *enabled* net transitions. If there are no enabled transitions, then the clocks count (increment they value by 1) in all marked places and the SNS net transitions to a new state. Otherwise, that is, if there are some enabled transitions, then it is said that one or several enabled transitions *fire,* that leads to the change of marking as explained by the firing rules. The set of simultaneously firing transitions is called *step.* In a given state, there could be several different steps ready to fire, meaning that a state of SNS can have several successor states.

2.3. Firing rules

Let St denote the set of incoming event arcs of transition t: $St := \{t' \mid [t', t] \in S\}$. If St is empty, which indicates that no incoming event arc is associated with transition t, then t is spontaneous, otherwise it is forced. Firing of a forced transition is caused by firing of some other transition connected to it by an event arc. Both are included in the same step, that is, fire simultaneously. Enabled spontaneous transitions can fire regardless of other transitions. For example, the transition t_4 in Figure 1 is forced and other transitions are spontaneous. Accordingly, the transition set T can be subdivided on two disjoint sets: $T = \text{Spont} \cup \text{Forc}$, where Spont is the set of all spontaneous transitions of the SNS, and Forc denotes the set of all forced transitions of the SNS.

For any transition t, there can be three kinds of markings: the marking on incoming flow arc t^-, the marking on outgoing flow arc t^+, and the marking on incoming condition arc $\hat{t}$, defined as follows:

$$t^-(p) := \begin{cases} V(p,t), & \text{if } [p,t] \in F, \\ 0, & \text{else,} \end{cases}$$
$$t^+(p) := \begin{cases} V(p,t), & \text{if } [t,p] \in F, \\ 0, & \text{else,} \end{cases} \quad (1)$$
$$\hat{t}(p) := \begin{cases} W(p,t), & \text{if } [p,t] \in B, \\ 0, & \text{else.} \end{cases}$$

For any subset $s \subseteq T$, the markings s^- and s^+ denote the sum of markings t^- and t^+, respectively, and $\hat{s}$ represents the union of markings $\hat{t}$ for $t \subseteq s$.

The firing of a spontaneous transition is determined by the three factors listed below.

(1) Token concession

A transition is said to have a *token concession* or is *token-enabled* when all the flow arcs from its preplaces are enabled. More specifically, a flow arc is enabled when the token number in its source place is not less than its weight, that is, $m(p) \ge V(p,t)$. For example, given the marking m, transition t is token-enabled if $t^- \le m$. Transitions which have no preplaces are always marking-enabled.

(2) Permeability interval

The permeability interval defines the time constraints applied to the input flow arcs of transitions. A transition t: $\exists (p,t) \in F$ is *time-enabled* only when clocks of all its preplaces have a time $u\ (p)$ within permeability interval of the corresponding place-transition arc: $\text{eft}(p,t) \le u(p) \le \text{lft}(p,t)$.

(3) Incoming condition signals

A spontaneous transition may have incoming condition arcs. It is considered *condition-enabled* when all the condition signals on its incoming condition arcs are true, that is, $\hat{t} \le m$.

A spontaneous transition is eligible to fire only when it is token-enabled, time-enabled, and condition-enabled.

2.4. Step and state transitions

SNSs are *executed in steps*, meaning that for each state transition there is a unique set of concurrently firing transitions $s \subseteq T$. A state is *dead* if no further step is enabled or will be enabled by elapsing time. For nondead states, the *delay* $D(m,u)$ denotes the minimum amount of elapsed time before a step is enabled.

A step is referred to as *executable at the state* $[m,u]$ if all of its constituent transitions fire after $D(m,u)$. The execution of an executable step s at state $[m,u]$ is accomplished by first elapsing $D(m,u)$ amount of time and then firing s.

The new state $[m',u']$ led by the execution of step s is determined by

$$m' = m - s^- + s^+,$$
$$u'(p) := \begin{cases} u(p) + D(m,u), & \text{if } m(p) > 0 \wedge m'^{(p)} > 0, \\ & \wedge p \notin (Fs \cup sF), \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Subsequent step executions from the initial state construct the *reachability graph* of the SNS model, which illustrates the relationship of all realizable states within the state space. The reachability graph of a timed SNS can be represented as a 3-tuple:

$$\mathrm{RG} = (Z, R, z_0), \tag{3}$$

where Z is a finite set of reachable states, R is a finite set of state transitions, and z_0 is the initial state $[m_0,u_0]$.

For any subsequent states $[m_i,u_i]$ and $[m_{i+1},u_{i+1}] \in Z$, there is a state transition $\tau \in R$, such that $[m_{i+1},u_{i+1}]$ is reachable from $[m_i,u_i]$ via state transition τ. This state transition is also denoted as $[m,u] \xrightarrow{\tau} [m',u']$.

2.4.1. Adding modularity to SNS

A basic net condition/event system [10] is an SNS augmented by interface elements: condition and event inputs and outputs, which can be connected by event and condition arcs to SNS transitions and places. A basic NCES without inputs is SNS. A composite NCES consists of the interface elements and a network of other NCES, interconnected by event and condition arcs with each other and with the interface elements.

The NCES concept provides a basis for a compositional approach to build larger models from smaller components. According to the rules presented in [11], the composition is performed by connecting inputs of one module with outputs of another module as depicted in Figure 2. The modularity, introduced in NCES, does not bring any semantic consequences—the model analysis is applied to the SNS resulting from the composition of several NCES modules.

The result of the composition of two NCES, N_1 and N_2, is an NCES N_{1+2} obtained as a union of the components. The result of the composition again can be represented as a new module. Inputs and outputs of the "composition" are unions of the components' inputs and outputs, except for those which are interconnected to each other, and hereby "glued," that is, substituted by the corresponding condition and event arcs. If the resulting NCES from Figure 2 is considered stand alone, its condition input can be neglected making it semantically equivalent to the SNS from Figure 1.

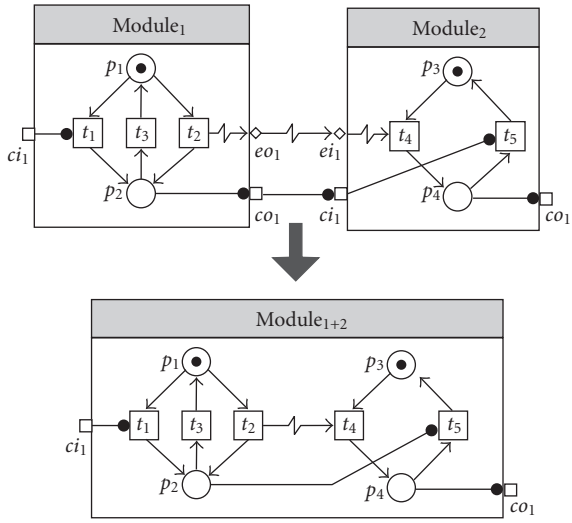

Figure 2: An example of a modular composition.

The reachability graph of the model from Figure 2 is shown in Figure 3, assuming that the input ci_1 of the Module1 is not assigned, thus neglecting the condition arc (ci_1, t_1). The transitions are shown as arcs of the graph, and are marked by names of NCES transitions simultaneously occurred. Observing values of model parameters along a certain path in the reachability graph, one can draw a timing diagram, like the one shown in the right part of Figure 3 for some outputs of the NCES modules from Figure 2 (some of which are inputs to another module).

NCES attempts to enhance the structured model development of place-transition nets. NCES models can precisely follow the structure of popular block diagram modelling and implementation languages, such as stateflow of MATLAB/Simulink and the function blocks of the IEC61499 standard—new reference architecture [12] used for modelling and implementation of distributed automation systems.

NCES were successfully used for modelling of traditional automation systems built using programmable logic controllers (PLCs), as presented, for example, in [1, 13], and of distributed embedded control systems following IEC61499 systems, as explained in [14].

The trend to improve structuring and composition potential of formal languages based on Petri net is seen in other dialects of Petri nets, as reported in [15, 16].

2.5. Integrated tools for model creation, editing, and analysis

The timing diagram specification technique explained in this paper is a part of the tool chain for integrated modelling and

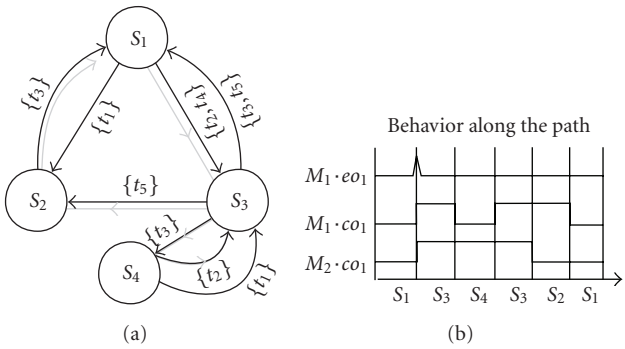

Figure 3: Reachability graph describing the complete behaviour of the model from Figure 2 and timing diagram in one of possible traces.

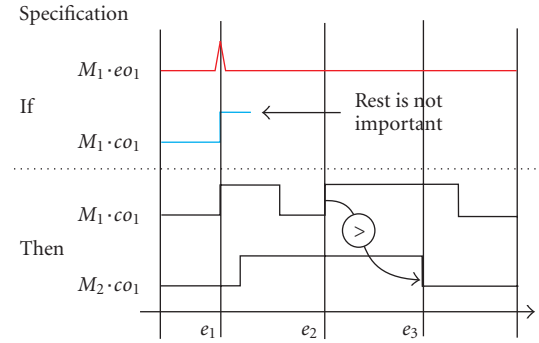

Figure 4: Timing diagram specification.

verification of automation systems. The tool chain, described in more details in [17], consists of

(1) a graphical editor of NCES models;
(2) the integrated environment for model assembly and checking (VisualVerifier) that inputs model-type files and is capable of assembling a composite, hierarchically organized model from modules contained in different libraries and translating the model into a "flat" NCES with the through numbering of places and transitions.

Thus, module boundaries are removed and the model-checking tools can be applied. In particular, the translator generates files in the input format of SESA model-checker [9].

Model-checkers like SESA prove properties of desired or prohibited behaviour of NCES models in their reachability space. A reachability graph like the one in Figure 3 is generated, and the properties are checked in its states or trajectories. Properties of single states can be captured in form of predicates, and properties of trajectories are usually defined in temporal logic languages, such as computational tree logic (CTL).

3. TIMING DIAGRAMS

3.1. Idea of use for specification

Capturing trajectory relevant properties in some formal language like CTL is quite difficult for control engineers. The idea of using timing diagrams for specification is to draw a specification graphically and then ask the model checker: if inputs behave as shown in the input diagram, will outputs behave like in the output diagram? However, a single timing diagram describes only a single scenario. Sometimes it is desirable to define a class of input scenarios with certain properties and then check if certain output patters are observed among all or any trajectories in the reachability graph. The idea is illustrated in Figure 4. The diagram consists of two parts: the upper (if) part presents the "input" part of guaranteed signals and the lower part is the "conjecture" to prove. In this example, there is conditional restriction added between the rising edge of $M_1 \cdot co_1$ (event e_2) and the falling edge of $M_2 \cdot co_1$ (event e_3)—the restriction says that e_3 occurs after e_2. Note that the signal $M_1 \cdot co_1$ belongs to both parts. In the "input" part, it is specified by a single wavefront change that is simultaneous with the event $M_1 \cdot eo_1$. The waveform of the same signal in the "output" diagram is more complicated. Comparing the "then" part of the specification with the timing diagram of real behaviour in Figure 3, one sees that the specification holds in the given path. The idea of this paper is to enable such a check automatically using model checkers.

3.2. Definitions

The use of timing diagrams (TDs) as a method of formal specification requires the definition of a graphical specification and its semantics.

In a diagram, sequences of changes in signal specification values are assigned to condition and event signals. Given the subsets $E \subseteq E^{\text{in}} \cup E^{\text{out}}$ and $C \subseteq C^{\text{in}} \cup C^{\text{out}}$, a specification for a signal set $A = E \cup C$ is described as a tuple $S = (A, f, g)$, where $f = f_e \cup f_c$ defines sequences of specification values: f_e: $E \to {\Sigma_e}^*$ with $\Sigma_e = \{\text{noevent, maybe, always}\}$ specifies sequences for event inputs and outputs, while f_c: $C \to {\Sigma_c}^*$ with $\Sigma_c = \{\text{zero, any, stable, one}\}$ defines values for condition signals.

The partial function g: $f(A) \times N \times f(A) \times N \to (>, =, \neq)$ assigns an ordering operator (precedence, simultaneity, or nonsimultaneity) between signal changes from different signals, in such a way that $g(a_i, m, a_j, n)$ indicates an ordering restriction between the mth signal change of a_i and the nth signal change of a_j.

A graphical description of a specification is illustrated in Figure 5 (for a model with outputs "FAILURE", "RESUME," and "SENS"). Signal changes at the beginning or ending of the diagram are implicitly simultaneous. Nevertheless, no further ordering is determined by the horizontal position of signal changes; therefore, a timing diagram usually specifies a partial ordering among signal changes.

The semantics associated to the diagram is as follows: when the set of levels specified at the beginning of the diagram is achieved, it is required that the sequence of changes of the signals does not violate the partial ordering specified in the diagram, until a final state is reached.

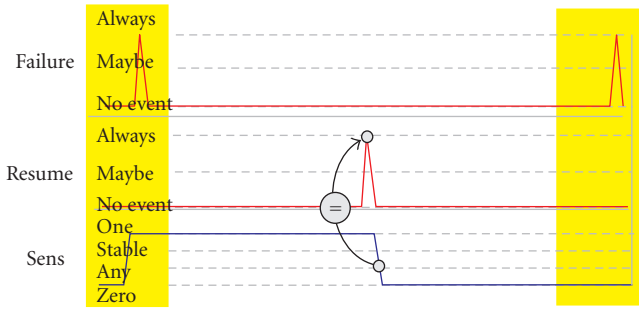

FIGURE 5: Specification including two event inputs, one condition output and a simultaneity operator.

3.3. Specified signals

In order to describe specifications of NCES models, TDs must provide different representations for event and condition signals. Thus, we define the following possibilities of specification:

(i) in the case of a condition signal, the specification may have one of four possible levels: *zero*, corresponding to a logical zero; *any*, representing the situation where the signal might assume any logical value which can change at any state transition; *stable*, which also means undefined value, however assuming that the signal remains at a single level; or *one*, corresponding to the logical one;

(ii) event signals are specified in two possible levels: *no event*, in the case where the occurrence of the event is forbidden, and *maybe*, meaning that the event might occur, it is also possible to specify an obligatory occurrence of the event *signal (always)*, but in this case only as a single pulse, because of the instantaneous nature of an event signal.

We define a *diagram event* as any level change specified at a condition signal; a level change from *no event* to *maybe* or vice versa, at an event-signal; or a specification of an obligatory occurrence of an event (*always* peak at an event signal).

3.4. Event ordering at different signals

If a *partial ordering semantics is* assumed, no prior ordering of events on different signals is implicit. In other words, although each signal presents an ordering of its events, two events of different signals may occur at any sequence, except when special operators explicitly define their sequence. On the other hand, it is also possible to assume that the ordering of all events is defined through their position at the visual description. In this case, we are talking about a *strict* or *sequential ordering*.

Although more intuitive, adopting a sequential ordering would limit the representational capabilities of a diagram. Therefore, we adopt a partial ordering semantics for the TD language. In this case, the same TD represents a set of possible behaviours of the system, each one represented by a different event chain on the modelled system. Each chain is called *scenario*, and the set of scenarios defined by the diagram is named *diagram language*.

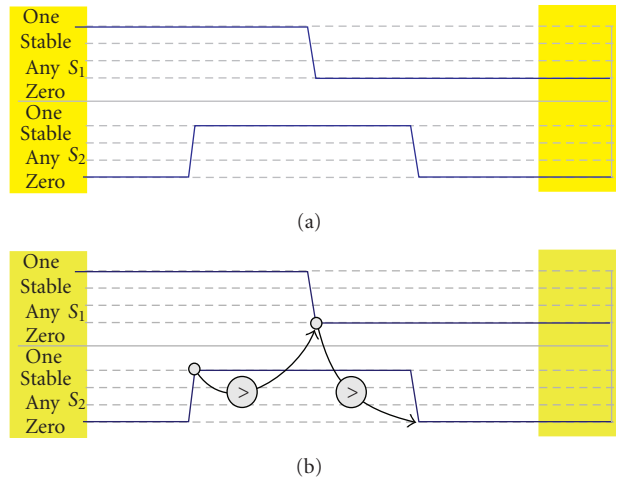

FIGURE 6: Temporally independent signals (a) and event ordering (b).

In Figure 6(a), we observe the specification of two signals: $\mathbf{s_1}$ and $\mathbf{s_2}$. Had we adopted a sequential ordering semantics, only one scenario would compose the diagram language: $\mathbf{s_2}^+\mathbf{s_1}^-\mathbf{s_2}^-$. As the temporal dependence among events from different signals is not predefined (assumed partial ordering semantics), the same figure represents a TD with the following scenarios: $(\mathbf{s_2}^+, \mathbf{s_1}^-)\mathbf{s_2}^-$; $\mathbf{s_2}^+(\mathbf{s_1}^-, \mathbf{s_2}^-)$; $\mathbf{s_1}^-\mathbf{s_2}^+\mathbf{s_2}^-$ and $\mathbf{s_2}^+\mathbf{s_2}^-\mathbf{s_1}^-$. Figure 6(b) indicates the timing diagram that, based on the adopted semantics, accepts as its only scenario $\mathbf{s_2}^+\mathbf{s_1}^-\mathbf{s_2}^-$, by introducing operators that indicate the obligatory ordering among events from different signals. The meaning of these operators will be stated in the next section.

In order to constrain the ordering of two events from different signals, we define the following precedence operators:

$\neq$: events are not allowed to occur simultaneously;
$=$: events must be simultaneous;
$>$: event from the first signal must occur prior to the event from the second signal.

3.5. Specification of finite behaviour

The TD represents a finite behaviour that must be satisfied by the model. The satisfaction of a TD is evaluated from the moment when all specified signals are in their initial levels and some of them execute an initial transition, as indicated at the beginning of the diagram. The verification process ends when all signals achieve their final state, indicated in the end of the diagram. The initial part of the diagram, denominated *precondition*, corresponds to a condition, whose satisfaction by the model indicates that we must start comparing the model's behaviour with the remaining part of the TD. The comparison ends up when the final part of the diagram, called *postcondition*, is reached. Both pre- and postcondition are highlighted at the diagram (Figure 7).

When a TD specifies a finite behaviour, different interpretations are possible.

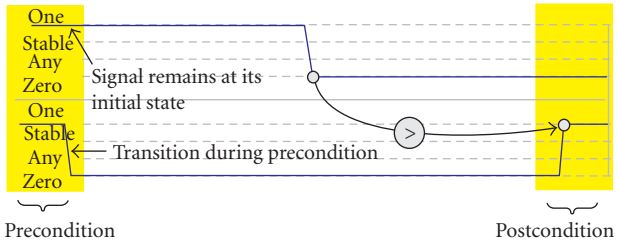

Figure 7: Pre- and postcondition.

Existence of a scenario (from the diagram language): here we require that at least one of the specified scenarios will occur at the model. In other words, there is a path at the state tree of the model, where the precondition is satisfied and the behaviour of the model does not contradict the specification.

Existence of all scenarios: the existence of each scenario must be tested inside the state space of the model.

Generality of a single scenario: here a single scenario, from the set of scenarios specified at the diagram, must be recognized in every path, indicating a situation that has to occur in the future, regardless of which path is taken by the model.

Generality of the diagram's language: the behaviour specified at the diagram will eventually occur, no matter which scenario is in each path from the state tree of the model. Notice that, in this case, the existence of a path with no occurrence of the precondition would already be a counterexample.

Satisfaction of a single scenario: every satisfaction of the precondition must be followed by the satisfaction of the same scenario, among those that are possible according to the specification. This corresponds to an assume-guarantee clause, where the precondition plays the role of an assumption that, when fulfilled, guarantees the occurrence of a given sequence of events.

Satisfaction of the diagram: the specified behavior must not be contradicted, which means that every occurrence of the precondition at the model leads to a behaviour that is accepted by the diagram language. As a particular case, a model that presents no occurrence of a given precondition satisfies every specification starting with this precondition. The following topics will be based on this interpretation of the TD.

3.6. Specification of infinite behaviour

The timing diagram could also correspond to a specification to be satisfied from the time when the precondition occurs, without the need to specify a postcondition. In this case, the final state specified at the diagram would correspond to a restriction that must not be violated.

The absence of a specification for the precondition could indicate that the initial state of the model should comply with the levels specified at the beginning of the diagram. Although these two approaches also present a practical appeal, the absence of postcondition or precondition will not be issued in the work, as a matter of simplicity.

In order to allow the translation of the timing diagram into a formal model, some requirements have to be done in respect to the events presented in each signal. Diagrams satisfying the requirements are said to be *feasible*.

4. NCES MODEL OF TIMING DIAGRAMS

When verifying autonomous NCES models without inputs, each signal specification is translated into an NCES supervisor module comprising two basic submodules: an *event generator* creates sequences of transitions, one for each change of level specified for the signal. Each transition stimulates, through an event arc, the corresponding event input of a *signal generator*, which causes the output of the signal generator to recreate the signal according to the input stimulated. Ordering operators are translated into special places and transitions that create interdependency of event generators.

The verified module is then connected through event arcs to the event generators of the corresponding signals, in such a way that every change of signal in the first is reported to the latter. Along with the translation of the specification into NCES modules, a set of automatically generated temporal-logic statements is created. The composite module is then model-checked against these statements to verify if each transition at the supervisor always fires whenever the corresponding transition at the verified module is fired.

The graphical specification also provides automatic test possibilities for input/output behaviour or nonautonomous NCES modules. In this case, the NCES supervisor modules that describe input signals are used for generating the specified sequences of input signal changes, while the output signals are again verified as described before. The components of the NCES model of the timing diagram are detailed in the following subsections.

4.1. Event generator

The main part of the NCES model for the specification is called *event generator* and consists of a set of parallel *processes* (sequences of transitions and places), started simultaneously by the firing of a transition denoted $\mathbf{t}_{\text{start}}$. Each process is responsible for reproducing the behavior specified for one signal. Events on the signals are translated into transitions at the processes.

For each signal **i**, there is a place $\mathbf{p}_{\text{notstart,i}}$ which is a preplace of $\mathbf{t}_{\text{start}}$ and postplace of the last transition of the corresponding process. The transition $\mathbf{t}_{\text{start}}$ indicates the beginning of the timing diagram. The situation where the diagram language is not being executed corresponds to the marking $\mathbf{p}_{\text{notstart,i}} = 1$ for every signal **i**.

In the case that at least a signal **j** has the marking $\mathbf{p}_{\text{notstart,j}} = 0$, the marking $\mathbf{p}_{\text{notstart,i}} = 1$ for a signal **i** indicates that this signal has already achieved the last level specified at the diagram.

The precedence relationships among events of different signals are mapped to special interconnections among the corresponding processes, as will be detailed in the following section.

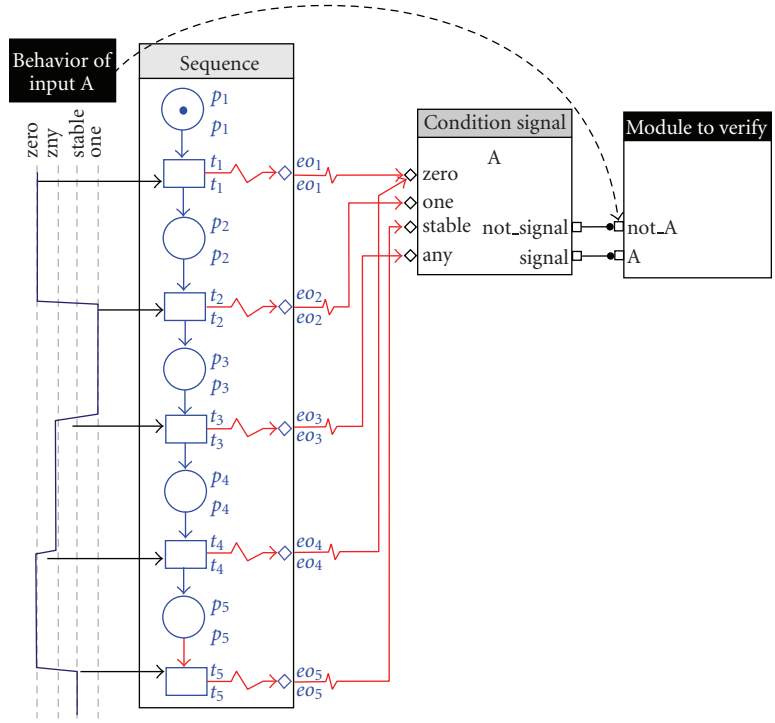

FIGURE 8: Translation of a single specification for a condition output, and linking to the verified model.

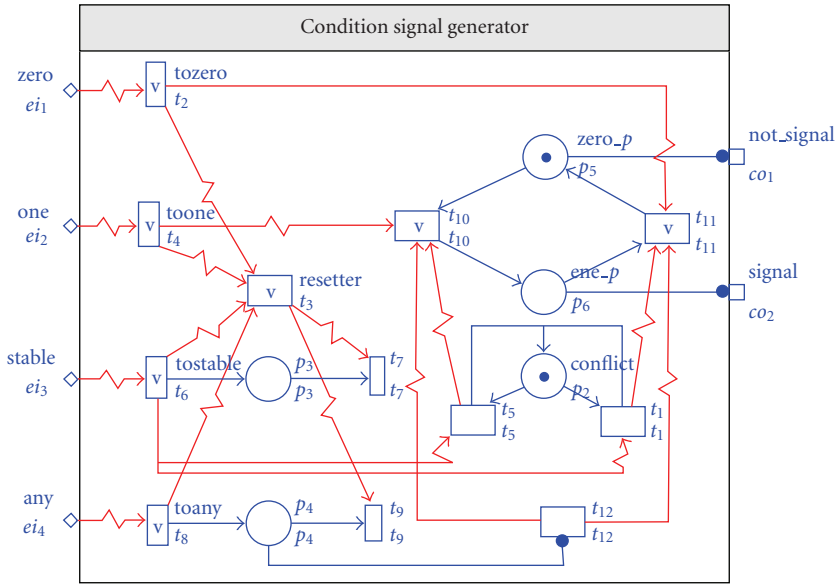

FIGURE 9: Generator of condition signals.

4.2. *Signal generation module*

For each specified signal, we create a signal generator module which reproduces, at its output, the possible values for the signal, according to the level specification stimulated at its input. Each event on the timing diagram (modelled by the firing of a transition at the event generator) stimulates, by an event arc, the corresponding change at the signal generator, which guarantees that the NCES module, resulting from the combination of the event generator with the signal generators, will reproduce at its output the diagram language. The idea is illustrated in Figure 8. To each condition signal included at the specification is assigned a signal generator module with four event inputs, corresponding to the

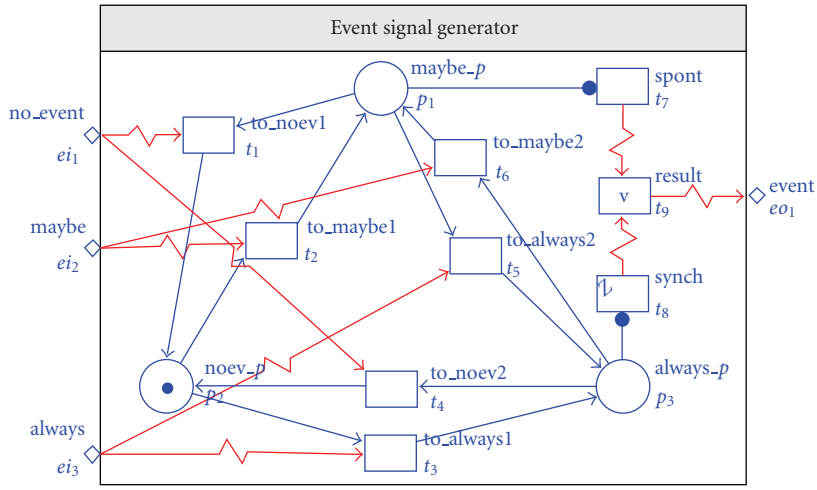

Figure 10: Generator of event signals.

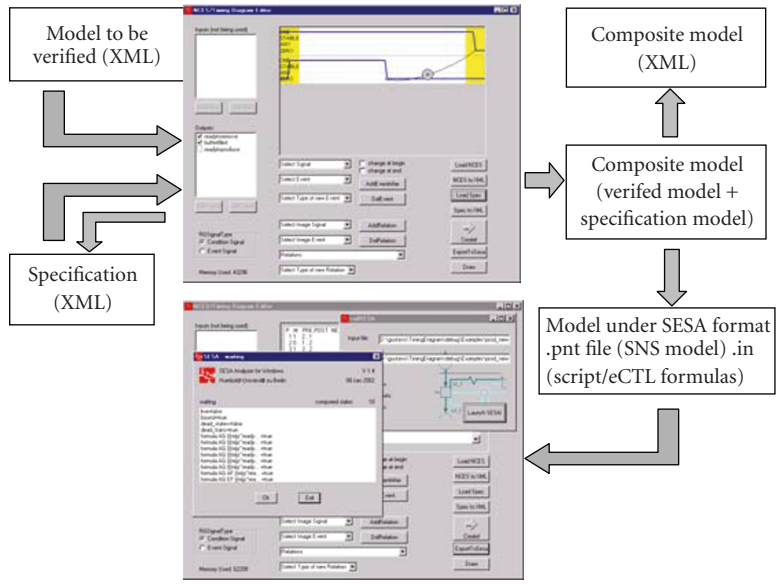

Figure 11: User interface of the TDE tool and file formats adopted for data storage.

four possible specification levels, and two condition outputs, indicating the two possible values assumed by the condition signal (*zero* or *one*).

Figure 9 shows the structure of a signal generator for a condition signal.

The transitions tozero, toone, tostable, and toany receive event arcs, respectively, from the zero, one, stable, and any event inputs.

Firing one of these transitions means that the corresponding signal has changed its specification level to, respectively, *zero*, *any*, *stable*, or *one*—in other words, a diagram event has occurred. The condition outputs not_signal and signal are linked to the internal places zero_p and one_p. The remaining transitions and places implement the desired nondeterministic behaviour, after the firing of tostable and toany, the marking of places zero_p and one_p should be nondeterministic, and may change randomly in the latter case, until another input event is stimulated. The place p_2 always has a conflict with respect to transitions t_5 and t_1 leading to nondeterministic choice in case of the signal "to stable" (i.e., the stable value can be assigned either to 0 or to 1).

Figure 10 presents the internal structure of a signal generator for an event signal.

Event signals are represented by modules with three event inputs, corresponding to the three possible specification values, and an event output, whose firing corresponds to the generation of the event. Internally, this generation corresponds to the firing of the result transition.

The transitions to_noev# (1 and 2), to_maybe# (1 and 2), and to_always# (1 and 2) are fired by stimulating the no_event, maybe, and always inputs, respectively. Every diagram event leads to the firing of at least one of these transitions—actually, an *always* peak at the specification, followed by the specification of a new level, implies that both

the result and the transition that leads to the new level specification (to_noev# or to_maybe#) will be enforced to fire.

5. PROGRAM IMPLEMENTATION

The timing diagram editor (TDE) is an application developed with the aims of providing the following functionalities.

(i) Create, edit, save, and load specifications of function blocks whose internal logic is specified by means of an NCES. These specifications are generated and visualized graphically as timing diagrams, while each signal at the timing diagram may be of one of the following types: event signals and condition signals; the signal levels allowed for each type of signals that were presented above.

(ii) Translate the combination of a function block and the behaviour specified for it into a composite finite state model (NCES) and temporal propositions written in the eCTL [18] format, in such a way that the composite model, and consequently the original function block, can be verified formally with the aid of the SESA tool [19]. If all the generated eCTL propositions evaluate to true with regard to the composite model, we conclude that the behaviour of the original model satisfies the specification.

The TDE tool uses XML as a storage format for both timing diagrams and NCES models and converts them to the input formats of the SESA model checker as illustrated in Figure 11.

6. CONCLUSION

The paper presented the idea of visual specification language to be used with modular discrete models, in particular of plant-controllers systems. Future work will include integration of this language to the visual verification framework [17].

ACKNOWLEDGMENTS

The authors express their gratitude to Professor Hans-Michael Hanisch, who supervised this work and significantly contributed to its success. The work was supported in part by the Deutsche Forschungsgemeinschaft under the reference Ha 1886/10-2 and Ha 1886/12-2 and by the University of Auckland (Grants UARC 3607207 and 3607893).

REFERENCES

[1] H.-M. Hanisch, J. Thieme, A. Lüder, and O. Wienhold, "Modeling of PLC behaviour by means of timed net condition/event systems," in *Proceedings of the 6th IEEE Conference on Emerging Technologies and Factory Automation (ETFA '97)*, pp. 391–396, Los Angeles, Calif, USA, September 1997.

[2] K. Fisler, "Timing diagrams: formalization and algorithmic verification," *Journal of Logic, Language, and Information*, vol. 8, no. 3, pp. 323–361, 1999.

[3] N. Amla, E. Emerson, R. Kurshan, and K. Namjoshi, "Model checking of synchronous timing diagram," in *Proceedings of the Formal Methods in Computer Aided Design (FMCAD '00)*, Austin, Tex, USA, November 2000.

[4] R. Schlör, A. Allara, and S. Comai, "System Verification using User-Friendly Interfaces," in *Design, Automation and Test in Europe*, pp. 167–172, IEEE Computer Society Press, 1999.

[5] V. Vyatkin and H.-M. Hanisch, "Application of visual specifications for verification of distributed controllers," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 646–651, Tucson, Ariz, USA, October 2001.

[6] G. Bouzon, V. Vyatkin, and H.-M. Hanisch, "Timing diagram specifications in modular modelling of industrial automation systems," in *IFAC World Congress*, Prague, July 2005.

[7] M. Rausch and H.-M. Hanisch, "Net condition/event systems with multiple condition outputs," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation*, vol. 1, pp. 592–600, Paris, France, October 1995.

[8] H.-M. Hanisch and A. Lüder, "Modular modelling of closed-loop systems," in *Proceedings of the Colloquium on Petri Net Technologies for Modelling Communication Based Systems*, pp. 103–126, Berlin, Germany, October 1999.

[9] P. Starke, S. Roch, K. Schmidt, H.-M. Hanisch, and A. Lüder, "Analysing Signal-Event Systems, Humbold," http://www.ece.auckland.ac.nz/~vyatkin/tools/modelchekers.html.

[10] V. Vyatkin and H.M. Hanisch, "Re-use in Formal Modeling and Verification of Distributed Control Systems," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA'05)*, Catania, Italy, September 2005.

[11] J. Thieme, "Symbolische Erreichbarskeitanalyse und automatische Implementierung struktuirter," Dissertation zur Erlagung des Grades Dr.-Ing, zeitbewerter Steuerungsmodelle, Berlin: Logos Verl, 2002.

[12] Function Blocks for Industrial Process Measurement & Control Systems, "International Electrotechnical Commission," Part 1: Architecture, 2005.

[13] H.-M. Hanisch, A. Lobov, J. L. Martinez Lastra, R. Tuokko, and V. Vyatkin, "Formal validation of intelligent-automated production systems: towards industrial applications," *International Journal of Manufacturing Technology and Management*, vol. 8, no. 1–3, pp. 75–106, 2006.

[14] V. Vyatkin and H.-M. Hanisch, "Verification of distributed control systems in intelligent manufacturing," *Journal of Intelligent Manufacturing*, vol. 14, no. 1, pp. 123–136, 2003, special issue on Internet Based Modelling in Intelligent Manufacturing.

[15] L. Gomes and J. P. Barros, "Structuring and composability issues in petri nets modeling," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 112–123, 2005.

[16] N. Hagge and B. Wagner, "A new function block modeling language based on petri nets for automatic code generation," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 4, pp. 226–237, 2005.

[17] "Visual Verification Framework," http://www.fb61499.com/valid.html.

[18] S. Roch, "Extended computation tree logic," in *Proceedings of the Workshop on Concurrency, Specification and Programming*, Berlin, Germany, 2000.

[19] "SESA—Signal/Net System Analyzer," http://www.ece.auckland.ac.nz/~vyatkin/tools/modelchekers.html.