Requirements Modelling by Synthesis of Deontic Input-Output Automata

Emmanuel Letier and William Heaven
Department of Computer Science
University College London
London, United Kingdom
{e.letier, w.heaven}@cs.ucl.ac.uk

Abstract—Requirements modelling helps software engineers understand a system’s required behaviour and explore alternative system designs. It also generates a formal software specification that can be used for testing, verification, and debugging. However, elaborating such models requires expertise and significant human effort. The paper aims at reducing this effort by automating an essential activity of requirements modelling which consists in deriving a machine specification satisfying a set of goals in a domain. It introduces deontic input-output automata—an extension of input-output automata with permissions and obligations—and an automated synthesis technique over this formalism to support such derivation. This technique helps modellers identifying early when a goal is not realizable in a domain and can guide the exploration of alternative models to make goals realizable. Synthesis techniques for input-output or interface automata are not adequate for requirements modelling.

I. INTRODUCTION

Our objective is to support the incremental elaboration of requirements models where a set Goals of required properties is to be satisfied by a machine specification Spec in the context of domain properties and assumptions Dom [1][2]:

\[ \text{Spec, Dom } \models \text{Goals.} \]

The machine specification must be realizable [3][4]. Intuitively, this means it must correspond to a transition relation between the machine’s monitored and controlled events [5]. The domain model Dom is typically composed of multiple agents (components) corresponding to human agents, hardware devices, and other automated systems. Systematic techniques have been developed to support the elaboration of goals, domain models, and realizable machine specifications satisfying the above condition [2][4][6][7][8]. However, elaborating formal models using these techniques requires significant effort and expertise.

Automatically deriving a realizable specification that satisfies a set of goals for a given domain model is an instance of a controller synthesis problem [9][10]. Such problems have been studied extensively in a wide variety of formal frameworks [11][12][13][14][15][16][17][18]. However, most of these frameworks rely on assumptions that are not valid in a requirements engineering context, such as that of a machine that can observe all events referenced in the goals or of a machine that can always act faster than its environment (even if it is composed of other automated systems). For example, recent techniques for deriving live behaviour models from goals and domain properties assume the machine can observe all domain events [19][20]. Our objective in this paper is to present a formal framework for automated specification synthesis that is suitable in a requirements engineering context where a clear distinction must be made between goals, machine specifications and domain properties, where machine specifications can be derived compositionally from goals and domain properties, and where assumptions about the relative speed of the machine are recorded explicitly as domain assumptions instead of being built into the formalism.

A first contribution is to present a novel event-based formal foundation for requirements modelling. This foundation is motivated by previous work showing that mismatches between the synchronous, state-based foundations for goal modelling [4][7] and the asynchronous, event-based foundations for scenarios and behaviour modelling [21] prevent an efficient derivation of event-based behaviour models from declarative goals [22]. In this paper, we introduce deontic input-output LTS to resolve that problem. A deontic input-output LTS is an extension of input-output labelled transition systems [23] that allows one to distinguish between the permission and obligation to perform an event—a distinction that is essential to requirements modelling [7] but absent in standard event-based behaviour models. We adapt previous definitions of agent responsibility [6] and goal realizability [4] to this context.

The second contribution is an automated specification synthesis technique defined over that formal foundation. The technique derives the weakest (i.e. least constraining) realizable machine specification that satisfies a goal for a particular domain model, or it signals that the goal is not realizable by the machine in the domain. The technique is compositional: partial specifications can be derived from different goals and domain specifications before being combined to form a specification that satisfies the combined set of goals. It can also be used symmetrically to derive weakest domain assumptions to satisfy goals for a given machine specification. Our approach is limited to discrete-time, finite-state models and to goals that correspond to safety properties (including bounded liveness properties [16]). Our algorithm is a version of a controller synthesis algorithm under partial observability, which means that the controller is not assumed to be able to observe all events in its environment [12][13][14][17][18]. It differs from previous work in this area by its clear separation between machine specification and domain assumptions, its distinction between permission and obligation, and the possibility of relying on alternative synchrony assumptions (saying that the machine is infinitely fast compared to its environment) or on no
such assumption at all. We have implemented our technique in the LTSA toolset [21]. This allows our technique to take as input goals and domain models specified as Fluent Linear Temporal Logic (FLTL) assertions [24][25], Finite State Processes (FSP) [21], the subset of the KAOS modelling language that has a LTS semantics [22], and a combination of all the above within the same model. The tool and all models discussed in the paper are available at

http://www.cs.ucl.ac.uk/staff/e.letier/ltsa-

A third contribution is a discussion of the role of specification synthesis during requirements modelling. In practice, goals and domain models are rarely specified completely and without error before deriving the machine specification. Elaborating goals, domain models, and machine specification is an intertwined process during which alternative models corresponding to alternative choices of agents and interfaces are explored. Most works on controller synthesis are presented without explicit attention to such a process. We illustrate through an example how realizability checking and specification synthesis can be used to incrementally elaborate and explore alternative requirements models.

II. EXAMPLE

Modern television systems are built by assembling a large number of hardware and software components [26]. One of the simplest systems is a television consisting of a Tuner, a Screen, and a single TV-Controller software [24]. Fig. 1 shows a context diagram for this small system. In this diagram, a box denotes a system component, and a labelled arrow between two components denotes a set of events that are controlled by the source component and monitored by the target component. The Tuner is a component that accepts channel selections from a user and is responsible for transmitting the signal from the selected channel to the Screen. It also interacts with the TV-

Controller to signal when it starts and ends tuning to a new channel. The Screen can be blanked and unblanked by the TV-Controller and when unblanked it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts and ends tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.

The TV-Controller must ensure these two goals by blanking the screen when the tuner starts tuning and, when not tuned, it will display whatever signal it receives from the Tuner. The system has two goals:

(G1) The screen should never display a static signal, a noisy signal sent by the Tuner while tuning between channels.

(G2) When a channel is selected, it should be displayed on the screen as soon as possible.
tuner is tuning to channel 1. In Fig. 2, when the TV_Controller receives end_tune in state 0, it moves to state 1 where it can perform unblank leading to state 2. In state 2, when it receives tune, it can perform blank leading back to state 0.

LTS models merely specify when events may occur; they do not specify when they must occur. For example, when the TV_Controller is in state 3, blank may occur (it is enabled) but nothing in the LTS itself specifies that it must occur. In this example, this is a problem because while the TV_Controller is in state 3, if it doesn’t perform blank immediately, the Tuner could send a signal.static event which could be followed by the Screen performing display.static which would violate G1.

To force events to occur, behaviour models usually rely on additional fairness and “maximal progress” assumptions. For example, the fair choice assumption in [21] states that every transition that is enabled infinitely often must be executed infinitely often. Maximal progress assumptions consist in giving higher priority to machine-controlled events (in our example to the TV_Controller events blank and unblank) so that when enabled, these events are always performed before all other events. Maximal progress means that the machine always performs its enabled events faster than its environment. In our example, giving higher priority to blank and unblank events in (Tuner || TV_Controller || Screen) ensures that when the TV_Controller is in state 3 of Fig. 2, it will perform blank before the Tuner and Screen send and display a static signal. However, fairness and maximal progress are problematic for requirements modelling. They both are global system properties that prevent compositional reasoning needed for goal-oriented requirements modelling. Their validity is also questionable. In requirements models, fairness assumptions can’t be justified as abstractions of a global process scheduler as they are for concurrent programs. The validity of maximal progress assumptions is also hard to justify when the domain is composed of other automated components that may be as fast if not faster than the machine. In Section IV, we’ll present a different way to specify progress using obligations rather than relying on fairness and maximal progress. In Section VI, we’ll also show how alternative “synchrony assumptions” about the relative speed of the machine with respect to its environment can be included explicitly in the domain model.

B. Interface and Input-Output LTS

An interface labelled transition system (I-LTS) is an LTS \( M = \langle Q, aM, \delta, q0 \rangle \) where the alphabet \( aM \) is partitioned into three sets \( \text{in}, \text{int}, \text{and out} \) denoting the input, internal, and output events of the LTS, respectively [30]. An input-output labelled transition system (IO-LTS) is an interface LTS whose transition relation \( \delta \) is required to satisfy the input-enabling rule according to which every input event must be enabled in every state, i.e. for all \( s \in Q, ev \in \text{in} \), there exists \( s' \in Q \) such that \( \langle s, ev, s' \rangle \in \delta \) [23].

The input-enabling rule is fundamental to requirements modelling: it corresponds to the real-world property that an agent cannot prevent occurrences of events controlled by its environment [1][4][23]. Fig. 2 satisfies this rule for the TV_Controller. Fig. 3 is an alternative LTS model, used as a specification for the TV_Controller in [24], that does not satisfy this rule because the input event tune is not enabled in state 2. As we will see below, this LTS defines the behaviour admitted by the assertion \( \exists(Tuning \rightarrow Blanked) \) requiring the screen to be blanked while the tuner is tuning. It is impossible to implement a TV Controller satisfying this model because in state 2, a state where the Tuner is tuned and Screen unblanked, it requires the TV_Controller to perform blank before tune occurs.

Instead of requiring a component’s LTS to satisfy the input-enabling rule, the formalism of interface automata constrains the environment models that can be composed with an interface automaton: the environment model must be such that it never produces an input event when that event is not enabled in the interface LTS, and it should never block the occurrences of output events performed by the interface LTS. This approach is problematic for requirements modelling because it means that an interface LTS mixes the component’s required behaviour with assumptions on its environment. For example, Fig. 3 models both constraints on the TV_Controller behaviour (not to perform unblank in state 0) and assumptions on the Tuner behaviour (not to perform tune in state 2).

In the paper, we will use the LTS ‘interface’ operator \( M@\alpha \) to denote the projection of an LTS \( M \) on an alphabet \( \alpha \subseteq Act \). This projection is obtained from \( M \) by replacing in the transition relation all events not in \( \alpha \) by \( \tau \). At the trace level, the projection of a trace \( \sigma \) on \( \alpha \subseteq Act \), noted \( \sigma\upharpoonright \alpha \), is obtained by removing from \( \sigma \) all occurrences of events not in \( \alpha \). We will also use the common approach of modelling passage of time by an explicit tick event to which all LTS synchronize [21].

C. Modelling System Properties

System properties are modelled as property LTS. A property LTS is a deterministic LTS \( P \) whose set of traces defines a set of admissible behaviour over the property’s alphabet. A LTS \( M \) satisfies \( P \), noted \( M \models P \), if and only if \( \text{Tr}(M) \supseteq \text{Tr}(P) \). A property \( P \) is weaker (less constraining) than or equivalent to a property \( Q \) if and only if for all \( M \models Q \) then \( M \models P \). Every property LTS \( P \) has an associated error LTS \( P_{err} \) that characterizes all possible violations of \( P \). Such LTS contains a special error state, labelled -1, denoting a state to be avoided. This error LTS is obtained from \( P \) by adding transitions to the error state for each missing transition in \( P \). To verify whether \( M \models P \), LTS computes \( (M \parallel P_{err}) \) and checks whether the error state is reachable in the resulting model. Any trace to the error state is a counter-example to \( M \models P \). If the error state is not reachable, then \( M \models P \) [31].

Figure 2. IO LTS for the TV_Controller

Figure 3. Interface LTS for the TV_Controller
For example, Fig. 4 shows the error LTS for G1. To verify G1, LTS A checks if the error state is reachable in (Screen || Tuner || TV_Controller || G1_err).

At the syntactic level, properties can be described in FSP [21] or declaratively in FLTL [24]. FLTL assertions are linear temporal logic assertions that can refer to events and to state propositions called fluents. An fluent is defined by a pair of set of events that make the fluent become true and false, respectively and by its initial condition. For example, in our TV system, the fluents Tuning and Blanked are defined as follows:

\[
\text{fluent Tuning} = <\text{tune}, \text{end\_tune}> \text{ initially True}
\]

\[
\text{fluent Blanked} = <\text{blank}, \text{unblank}> \text{ initially True}
\]

FLTL assertions are build from fluents using the usual Boolean operators, linear temporal logic operators such as \([\) (always), \(<\) (eventually), \(\) (waiting for) as well as bounded temporal operators such as \(<\) (eventually within \(\) time units) which can be used to model bounded liveness properties [25].

If an FLTL assertion \(P\) is a safety property, LTSA can generate an error LTS \(P_{\text{err}}\), characterizing all possible violations of \(P\). For example, \(G1\) can be defined by the FLTL assertions \([\![\text{display\_static}\text{ and}\ G2] \text{ by forall } [c:\text{Channel}] [\{\text{request}\[c\] -> \(<\! d\] \text{ display}[c]\}] \text{ where } d \text{ is a constant (e.g. set to 2 time units)}\). Both are safety properties. The error LTS corresponding to \(G1\) is shown in Fig. 4. \(G2\) generates another error LTS (of 8 states for 2 channels and \(d=2\)) characterizing sequences of events that violate this goal.

In any LTS \(P\), transitions to error can be removed using the function \(\text{behaviour}(P)\). This can be used to transform an error LTS generated from an FLTL assertion into a property LTS. For example, as mentioned previously, the behaviour LTS for the FTL assertion \([\![\text{Tuning } \rightarrow \text{Blanked}]\) is shown in Fig. 3.

IV. FOUNDATION

We now introduce our novel event-based foundation for requirements modelling. This foundation adapts the synchronous state-based model of KAOS agents [4] to the asynchronous event-based model of LTS. In our model, an agent is characterized by the following items:

- an interface declaring disjoint sets of events the agent monitors (its input events) and controls (its internal and output events);
- a behaviour model given as an LTS that satisfies the conditions of a deontic IO LTS given below;
- a responsibility relation that maps the agent to the set of goals the agent is responsible for.

Multiple agents run concurrently and synchronize on shared events. A single event can be monitored by several agents, but we require each event to be controlled by at most one agent. A system context diagram, such as the one shown in Fig. 1, provides a graphical view of the agents’ interfaces.

The key differences with the previous KAOS model of agents are that the agent interfaces are composed of events rather than state variables, the agents’ behaviour models are defined as asynchronous deontic IO LTS instead of synchronous state-based transition systems, and the goals and agents’ responsibilities are defined as asynchronous properties instead of synchronous ones (see [22] for an explanation of the difference between synchronous and asynchronous properties).

A. Deontic IO LTS

Deontic IO LTS are extensions of IO LTS that enable the distinction between states in which controlled events are permitted to occur and states in which controlled events are obliged to occur. This distinction relies on the concepts of stable states and transient states: a stable state is a state in which time is allowed to pass, a transient state is one in which time is not allowed to progress. The formalism has no explicit constructs for obligation and permission. The notions of permission and obligation rather come from the (informal) interpretation we give to transitions in the LTS. The permissions of an agent in a given state are represented as usual by the controlled events that are enabled in that state. The obligations of an agent are represented by the sequences of controlled events leading to a stable state. If the agent is already in a stable state, it has no obligation. If it is in a transient state, then it has an obligation to perform one or more controlled events to reach a stable state.

Instead of extending LTS with new language constructs for stable and transient states, we have chosen to rely solely on tick events to mark this distinction. If tick is not in the LTS alphabet, then all its states are stable. If tick is in the LTS alphabet, then stable states are those where tick is enabled and transient states are those where tick is not enabled. This approach has the benefit of being consistent with the standard interpretation of LTS models with respect to time and permissions. By convention, in LTS figures, transient states are marked with a double ring.

For example, Fig. 5 shows a deontic IO LTS for the TV_Controller specifying that this agent may perform unblank in state 1 and it must perform blank in state 3. Fig. 2 is another deontic IO LTS for the TV_Controller. Here, because the model is untimed, all states are stable and the model includes no obligation. This model has the usual LTS meaning of specifying that unblank may occur only in state 1 and blank may occur only in state 3.

For a deontic IO LTS to be well-formed, an agent should not have obligations that it can’t fulfil because it doesn’t have the necessary permissions to do so. This is captured by the independent progress rule. It states that for every transient state, the transition relation must include a sequence of controlled events leading to a stable state. In other words, the agent model must be such that, whatever the behaviour of other agents, the agent is always able to independently reach a stable state where time can progress.

Figure 5 satisfies independent progress because in state 3, the TV_controller can perform blank to reach the stable state 0. Figure 6, however, violates independent progress because in
states 1 and 2, the *TV_Controller* has no sequence of controlled events leading to a stable state.

Formally, deontic IO LTS are defined as follows:

**Definition (deontic IO LTS).** A deontic IO LTS is an IO LTS $M = \langle Q, \alpha M, \delta, q0 \rangle$ that must satisfy the input-enabling rule and an additional independent progress rule requiring that for every transient state $s0 \in Q$, there is a finite sequence of controlled events (i.e. output and internal events) $<c_{i1}, ..., c_{in}>$ that leads to a stable state, i.e. for all $s_{i1}, ..., s_{in}$ such that $<s_{i1}, c_{i1}, s_{i2}> \in \delta, s_{i2}$ is a stable state.

The trace semantics of deontic IO LTS is the standard trace semantics of LTS. Note that stable and transient states should not be confused with accepting and non-accepting states in Buchi automata. Unlike accepting states in Buchi, stable states are not required to be visited infinitely often.

Because deontic IO LTS are LTS, they can be composed, determined, minimized and projected onto alphabets like any other LTS. The behaviour of a system composed of multiple agents is defined by the standard LTS parallel composition of the agents’ deontic IO LTSs. Because in our framework every event is controlled by at most one agent, the input-enabling and independent progress rules ensure the transition relations of different agents do not interfere (an agent model cannot affect permissions and obligations in another agent’s model).

The behaviour model of a single agent can also be defined as the composition of several deontic IO LTSs for the agent. This composition is guaranteed to preserve the satisfaction of the input-enabling rule, but not of the independent progress rule. This will for example happen when one deontic IO LTS imposes an obligation to perform an event in a certain state and the other deontic IO LTS forbids this event to occur in that state. In practice, this means that when we define the behaviour of an agent as the composition of several deontic IO LTSs, as we will do in Section VI and VII, it is necessary to check that the composed model satisfies the independent progress rule. Violations of that rule signal an inconsistency between the agent’s obligations and permissions.

Note that deontic IO LTS allow one to model agents that have multiple simultaneous obligations without introducing an inconsistency. This is a characteristic that caused difficulties in previous deontic formalisms where obligations was defined as the obligation for an event to occur next in the execution trace [32]. When traces are defined as sequences of events (i.e. they have an interleaving semantics), such semantics of obligation introduce inconsistencies as soon as an agent has more than one simultaneous obligation because only one of the obliged events can possibly occur next in the trace. Our approach avoids this problem by defining obligations as the obligation to perform events before the next occurrence of *tick*.

An important difference between deontic IO LTS and other models of concurrency is that it doesn’t rely on fairness to ensure that some of the enabled events are eventually performed. This limits the expressive power of deontic IO LTS to safety properties (it’s impossible to model a liveness property with a deontic IO LTS). This is a deliberate choice justified by the pointlessness of liveness properties in requirements specifications: a liveness property —classically defined as a property for which every finite trace can be extended into a trace satisfying it— is by definition not testable (no violation can be witnessed in the running system) and it imposes no real constraint on the agent behaviour (its satisfaction can always be postponed)[4]. For example, a specification stating that all debtors must repay their debts eventually —without time bound on the repayment— allow debtors to indefinitely postpone repayment without ever violating the specification. Liveness properties are therefore inadequate as statements of requirements. This does not mean that we exclude liveness entirely from requirements models. They are useful abstractions of bounded liveness properties when it’s more convenient to leave the actual bound unspecified [16], but as long as they remain pure liveness properties they are untestable and impose no real constraints on the running system. In our framework, goals and domain properties can be liveness properties, but the controller synthesis technique presented in this paper can’t deal with them.

**B. From LTS to Deontic IO LTS**

When an agent LTS model does not satisfy the input-enabling and independent progress rules, it is possible to automatically transform it into a deontic IO LTS by adding additional transitions to the model. This is useful for transforming standard LTS obtained from the semantics of FSP, FLTL, and KAOS operation models into deontic IO LTS. It shows that it is possible to define the semantics of existing requirements modelling languages in deontic IO LTS.

Alternative extensions of an LTS into a deontic IO LTS are possible. For our synthesis procedure in Section V, we will use the **weakest IO completion** that given an LTS $P$ with alphabet $\alpha P$ and a set of controlled event $\text{Ctrl} \subseteq \alpha P$, generates the weakest deontic IO LTS (i.e. the one with the most the traces) that satisfies $P$. This LTS is generated by adding to $P$ (1) a new “sink” state (i.e. a state with no outgoing transitions) with self-transitions for all events in $\alpha P$, (2) new transitions $(s, e, \text{sink})$ from every state $s$ where some input event $e \in \alpha P\text{Ctrl}$ is not enabled, and (3) new transitions $(s, \text{tick}, \text{sink})$ from every transient state $s$ for which there is no sequence of controlled events to a stable state in $P$. For example, Fig. 8 shows the weakest IO completion for the LTS in Fig 7. The new sink state is state 3. This model an agent that behaves as in P but enters into a sink state where all behaviours are permitted as soon as some unexpected input or tick event occurs. Alternative functions to transform an LTS into a deontic IO LTS are the **strongest IO completion** (where the sink state admits input and tick events only) and the **robust IO completion** (where instead of adding transitions to a sink state, missing input and tick events generate new self-transitions, i.e. these event are just ignored by the agent). The choice of which completion function to use is left to modellers or language designers. Considerations about modelling language design are left out of this paper.

**C. Responsibility and Realizability**

In our model, goals define sets of admissible traces. The **responsibility** of an agent is a set of goals the agent must satisfy regardless of the behaviour of other agents in its environment [2][4][6]. This is captured by the following constraint.
Definition (Agent responsibility constraint). If an agent is responsible for a goal \( G \), then its behaviour model \( M \) must satisfy \( G \) for all valid environment \( E \), i.e. \( M \models |E| \models G \).

In this definition, a valid environment is one whose behaviour model is a deontic IO LTS for the agent’s environment: the environment’s input, i.e. the agent’s output events, must be enabled in every state, and the model must ensure independent progress through environment-controlled events. When these conditions are satisfied, we can show that the responsibility constraint is equivalent to the simpler constraint \( M \models G \) requiring that \( M \) satisfies \( G \) without any environment model (which means that all environment events can occur at all time). This property allows us to check agents’ responsibilities independently of their environment models.

The notion of realizability has its usual meaning, adapted to agents characterized by deontic IO LTS behaviour models.

Definition (Realizability). A goal \( G \) is realizable by an agent if there exists a deontic IO LTS \( M \) for that agent such that \( M \models G \).

A goal \( G \) is realizable by an agent for a domain model \( \text{DOM} \) if there exists a deontic IO LTS \( M \) for that agent such that \( M \models \text{DOM} \models G \).

As usual, two goals may be realizable individually, but not together because the behaviour models that realize each goal individually may be inconsistent with one another (their composition admits no trace or it does not satisfy the independent progress property).

V. SPECIFICATION SYNTHESIS

We now describe a technique for checking whether a goal \( G \) is realizable by an agent \( Ag \) in a domain \( \text{DOM} \), and if the goal is realizable for synthesising the weakest realizable specification for \( Ag \) that satisfies \( G \) in \( \text{DOM} \). Our technique takes as input a goal \( G \) given as a property LTS \( G_{\text{err}} \) (derived from an FLTL assertion or FSP property), a domain model \( \text{DOM} \) in the form of a deontic IO LTS (again, derived from FSP, FLTL, or KAOS descriptions), and the agent’s alphabet \( \alpha Ag \) partitioned into its monitored (its input) and controlled events (its output and internal events). The agent’s controlled events are noted \( \text{Ctrl}(Ag) \).

A. Specification Synthesis Algorithm

The algorithm proceeds in two steps. The first step relies on an existing technique [33] to generate the weakest interface LTS that satisfies \( G \) in \( \text{DOM} \) (our presentation and context of use are however different from [33]). The second step adds the constraint that the agent LTS must satisfy the input-enabling and independent progress rules of deontic IO LTS.

Step 1. Deriving the interface controller. The derivation of the weakest interface LTS that satisfies \( G \) in \( \text{DOM} \) has three substeps.

The first substep computes \( C_0 = (\text{DOM} \parallel G_{\text{err}}) \) which gives an LTS whose error traces are all traces in \( \text{DOM} \) that violate \( G \).

Example: To check the realizability of \( G_1 \) by the \( TV_{\text{Controller}} \), we compute \( C_0 = (\text{Screen} \parallel \text{Tuner} \parallel G_1) \). This generates an LTS (with 33 states) characterizing all behaviours of a system composed of a \text{Screen} and a \text{Tuner} (without \( TV_{\text{Controller}} \) yet) and where all behaviours that violate \( G_1 \) lead to the error state.

If \( C_0 \) has no error trace, the domain model satisfies the goal without the need for any constraint on the agent. In this case, the synthesis procedure terminates and the weakest interface and deontic IO LTS for the agent consists of a single state that accepts all events in the agent’s alphabet. If \( C_0 \) contains error traces, the domain model in itself does not satisfy the goal, and the synthesis procedure must continue.

If the agent for which we want to derive a specification was omnipotent, i.e. if it could observe and control all events, then it would be able to avoid error traces in \( C_0 \) (the subscript in \( C_0 \) stands for omnipotent). But the agent is not omnipotent, and \( C_0 \) may contain traces \( \sigma \) and \( \sigma' \) that are indistinguishable to the agent, i.e. such that \( \sigma \upharpoonright \alpha Ag = \sigma' \upharpoonright \alpha Ag \). For example, the traces \( \sigma = \langle \text{select.2, tune, signal.2} \rangle \) and \( \sigma' = \langle \text{select.2, tune, signal.static} \rangle \) are indistinguishable by the TV_{Controller} because their projections on its alphabet are both equal to \( \langle \text{tune} \rangle \). These two traces lead to different states in \( C_0 \); the first leads to a state where the tuner has reached the selected channel and therefore it would be safe for the TV_{Controller} to unblank the screen, the second leads to a state where the tuner is still sending a static signal and therefore it would not be safe to unblank the screen. However, whichever of these two traces is executed, the TV_{Controller} will only observe the occurrence of \( \langle \text{tune} \rangle \) and will therefore not know which of these two states (and possibly others) the system is in.

The second substep takes the agent’s partial observability into account by merging together states in \( C_0 \) that are indistinguishable to the agent. This is achieved by projecting \( C_0 \) on the agent’s alphabet and \( \text{tick} \) event (using the LTSA ‘interface’ operator \( @ \) ) and determinizing the resulting model:

\[ C_1 = \text{deterministic}(C_0 @ \alpha \text{Ag} \,(\text{tick}) \). \]

The determinization function uses the classic powerset construction in which sets of states in the non-deterministic LTS are mapped to single states in the deterministic LTS. In this construction, if a set of states of the non-deterministic LTS includes the error state, then the corresponding state in the deterministic LTS is labelled as error. Intuitively, if a transition can non-deterministically lead to the error state or not, then it should be avoided and therefore in the deterministic LTS it should lead to error.

Example: In our running example, \( C_1 = \text{deterministic}(C_0 @ \{\text{tune, end_tune, blank, unblank, tick}\}) \). This generates the LTS shown in Fig. 7.

In step 2, the derivation of the weakest deontic IO LTS realizing \( G \) will continue from \( C_1 \). The third substep of step 1 is needed only if one wants to derive the property LTS \( \text{Spec}_1 \) characterizing the weakest interface LTS satisfying \( G \) in \( \text{DOM} \). This LTS is obtained by generating the weakest IO completion of \( C_1 \) then removing its transitions to error.

Example: The weakest IO completion of the LTS in Fig. 7 is shown in Fig. 8. To obtain the weakest interface property LTS, we then remove the transitions from state 0 and 2 to error. It is interesting to observe that the LTS in Fig. 3 corresponding to the property \((\text{Tuning} \rightarrow \text{Blanked})\) is a refinement of the synthesised model (all traces of Fig. 3 are traces of \( \text{Spec}_1 \)).

The correctness of this last substep relies on the fact that transitions to the sink state added during the weakest IO completion correspond to transitions that are not enabled in \( \text{DOM} \) and therefore will never be exercised when \( \text{Spec}_1 \) is combined with \( \text{DOM} \). A proof of correctness is given in [33].
Step 2. Deriving the deontic IO LTS controller. If the agent could control its input events and all occurrences of tick, then it would be possible to implement an agent that prevents error traces in C. But in our framework, an agent can’t prevent occurrences of its input events and it can’t prevent tick transitions to error unless it can perform a sequence of controlled events to a stable state.

For example, in Fig. 7, the tune transition to error cannot be prevented by the TV_Controller because it corresponds to an input event. As another example, in Fig. 9, the TV_Controller can’t prevent the tick transitions to error because it doesn’t have a sequence of controlled events to a stable state. To avoid the error state, the agent must avoid reaching states that have such uncontrollable transitions to error. For example, the TV_Controller should avoid state 2 in Fig. 7 and it should avoid states 1 and 2 in Fig. 9. The second step of the synthesis procedure consists in transforming such states into an error state by backward propagation of the error state through such uncontrollable transitions. We have extended LTSA with a new “Controllable” function that performs this step:

\[ C_D = \text{Controllable}(C)@\langle \text{Ctrl}(ag) \rangle. \]

Our syntax overloads the @ symbol in LTSA; here it is used to declare the set of controlled events for the backward error propagation (rather than the alphabet on which to project an LTS). Our implementation assumes that the LTS model on which this function is performed is deterministic, which is always the case when performed after step 1.

**Examples:**
1. Applying this function to Fig. 7 with \( \text{Ctrl}(\text{TV_Controller}) = \{\text{blank, unblank}\} \) turns state 2 into error resulting in the LTS in Fig. 10. This LTS specifies that to achieve G1 the TV_Controller must never unblank the screen. This makes G1 realizable but prevents G2 from being satisfied.
2. Applying this function to Fig. 9 first transforms states 1 and 2 into error, then it also transforms state 0 into error because its end_tune transition to state 1 (which is now assimilated to error) can’t be prevented.

(3) Not every tick transition to error results in merging its source state with error. For example, state 3 of the TV_Controller model in Fig. 11 is not merged with error because an occurrence of blank leads the system to a stable state. In this model, when the TV_Controller is in state 3, it can avoid an error by blanking the screen before the next tick. □

If, as a result of this step, the initial state becomes the error state, there is no deontic IO LTS for the agent that satisfies G in DOM: G is therefore not realizable by the agent in DOM. Otherwise, the agent’s weakest realizable specification SpecD can be constructed by generating the weakest IO completion of \( C_D \) and removing the remaining transitions to error in the same way we transformed \( C_i \) into SpecC at the end of step 1.

The following proposition establishes that SpecD is the weakest deontic IO LTS for the agent that satisfies G in DOM.

**Proposition.** For all deontic IO LTS model M for Ag, \( M \models \text{SpecD} \) if and only if \( (\text{DOM} \parallel M) \models G \).

Its formal proof is omitted due to space limitation. It follows the same structure as the proof of correctness for step 1 in [33].

B. Compositionality

Because we’re dealing with safety properties only, our approach is compositional. We can show that if I1 is the weakest specification satisfying G1 in DOM and S2 the weakest specification satisfying G2 in DOM, then \( (I1 \parallel S2) \) is the weakest specification satisfying G1 \( \land \) G2 in DOM, provided that \( (I1 \parallel S2) \) satisfies the independent progress rule. If it doesn’t satisfy this rule, then G1 \( \land \) G2 is not realizable by the agent in DOM.

This argument assumes the same domain model DOM has been used to derive I1 and S2 from G1 and G2. In practice, we will often use one set of assumptions Dom1 for G1 and another set of assumptions Dom2 for G2. When this is the case, the model \( (I1 \parallel S2) \) satisfies G1 \( \land \) G2 in (Dom1 \parallel Dom2) but it is not guaranteed to be the weakest specification. This has no serious consequences in practice. It only means that if \( (I1 \parallel S2) \) doesn’t satisfy the independent progress rule (and is therefore not a valid specification for the agent), by rederiving I1 and S2 from DOM = (Dom1 \parallel Dom2), it might be possible to find a weakest specification that satisfies independent progress. If not, then G1 and G2 are not realizable together in DOM.

Note that we’ve been able to maintain compositionality even though our technique deals with agent’s progress (through obligations). This is a consequence of modelling obligations as safety properties instead of relying on fairness for progress.
VI. A REALIZABILITY-DRIVEN MODELLING PROCESS

We now consider how checking goal realizability and synthesising specifications from goals support the requirements modelling process. Finding that a goal is not realizable by an agent or that the weakest specification that realizes the goal is not adequate (as was the case for Fig. 10 in our running example) prompt modellers to modify the goal definition, to modify domain assumptions, or to add new agents and agent interfaces to fix the problem. In previous work, we have defined a library of model transformations to resolve realizability problems [4]. In this section, we illustrate on our running example how identifying and resolving realizability problems help modellers exploring alternative requirements models relying on different synchrony assumptions about the relative speed of the machine with respect to its environment.

A. Alternative Models Satisfying G1

We have seen in the previous section that the weakest deontic IO LTS satisfying G1 is one where the TV_Controller never unblanks the screen. This is not a good model as it prevents G2 from being satisfied.

To understand the cause of a realizability problem, it is useful to look at the error traces in the intermediate models C₀ and C₁ characterizing the error traces for an omnipotent and interface automata, respectively. In this example, looking at Fig. 7 shows that the problem is caused by the occurrence of tune in state 2. To prevent such tune transition to error, we would like the TV_Controller to perform blank before tune occurs, thereby leading the system to the safe state 1. We explore four options to achieve this.

A first option is to add a domain assumption on the Tuner stating that after a tune event, it will not send signal.static before the next tick, modelled by the following FLTL assertion:

\[ \text{StaticTimeLag} = \square \text{tune} \rightarrow \neg \square \text{signal statically} \text{ W tick}. \]

This gives the TV_Controller time to blank the screen before signal.static occurs. The controllable error LTS C₀ generated with the modified domain model is shown in Fig. 11. It states that the TV_Controller cannot perform blank in state 0 and it must perform blank when it is in state 3.

Note that even though G0 is an untimed safety property, its satisfaction imposes an obligation on the TV_Controller to blank the screen after a tune event. Such immediate obligation can’t be modelled with untimed interface or input-output automata. In our deontic IO LTS, it is represented by the blank transition from transient state 3.

A second set of options is to use generic synchrony assumptions about the relative speed of the machine with respect to its environment. Different modelling frameworks rely on different built-in synchrony assumptions. For example, SCR models rely on the one-input and synchrony assumption stating that the machine will receive one input at a time and will always be able to process it before the arrival of its next input [5]. In our framework, such assumption can be included explicitly in DOM by instantiating the generic LTS in Fig. 12. Checking G1 realizability on the revised model reveals that the only way to satisfy the goal under this assumption is again to keep the screen always blanked. Kupferman and Vardi’s controller synthesis under partial observability [12] relies on a stronger built-in synchrony assumption stating that the environment can perform at most one unobservable event followed by at most one input event before giving turn to the machine to perform its controlled events. In our approach, this can again be modelled explicitly in DOM rather than being built into the formalism. Checking G1 realizability under this alternative assumption gives an acceptable specification in which the screen may be unblanked after an end_tune event and must be blanked again after a tune event. The generated weakest deontic IO LTS is weaker (and more complex in terms of number of states and transitions) than the one in Fig. 11 because it exploits the synchrony assumption to identify all possible states in which the TV_Controller could unblank the screen and still have time to blank it to prevent a goal violation.

The fourth option does not rely on any timing assumption but instead consists in adding to the context diagram of Fig. 1 a new event tune.return controlled by the TV_Controller and monitored by the Tuner, together with a domain assumption stating that after tune, the Tuner will not start tuning before it receives tune.return from the TV_Controller:

\[ \text{No Static Before Tune Return} = \square \text{tune} \rightarrow \neg \square \text{signal statically} \text{ W tune.return}. \]

The synthesized controllable LTS is equivalent to the one in Fig. 11 except that all occurrences of tick are now replaced by tune.return. It states that when the screen is blanked, the TV_Controller may not perform unblank before receiving end_tune, and when the screen is unblanked, it may not perform tune.return before blank.

B. Synthesis for the Bounded Achieve Goal G2

Synthesis for goal G2 also revealed interesting realizability problems that led to transforming the initial model. To satisfy G2, the domain model was first extended with assumptions specifying obligations on the Tuner and Screen, such as the assumption that when a user selects a new channel, the tuner will immediately send tune which will be followed by end_tune within at most one tick, and the assumption that when the screen is unblanked, it always displays the signals it receives immediately (before the next tick). Checking G2 realizability with these assumptions reveals the goal to be unrealizable. The cause of the problem was that after selecting a channel, the user could select another channel...
before the first one had been displayed making the goal impossible to satisfy. The resolution in this case was to weaken the goal by requiring that the selected channel should be displayed within d time units (d=2), except if some other channel has been selected in the meantime.

VII. DISCUSSION

We have applied our technique to a number of systems including the classic turnstile [34] and mine pump [35] as well as a more complex, real-world proton therapy control system [36]. All models are available online. From our experience, we make the following observations:

- Our automated realizability checking and specification synthesis technique shortcuts the previous manual process of iteratively writing, model-checking, and “debugging” requirements models until the machine specification satisfies the goals in the domain. This process is hard and time-consuming. Writing a machine specification satisfying the goal in the domain and conforming to the input-enabling and independent progress rules is particularly hard without tool support.

- Without deontic IO LTS, other specification synthesis techniques could be used to generate interface or input-output LTS satisfying the goals in the domain, but the synthesised models would not be guaranteed to satisfy the input-enabling and independent progress rules. This is in practice a serious problem because it may give a false sense that the synthesised specification is correct (it does satisfy the goal in the domain) when in fact it is inadequate because it includes implicit constraints on the environment.

- In most of our case studies, the machine specification satisfying the goals in the domain includes immediate obligations. Such obligations can’t be modelled with untimed IO or interface automata. Deontic IO automata are thus essential for requirements modelling.

- During our case studies, checking our domain models against the input-enabling and independent progress rules helped us identify early critical errors in our domain models. Invalid domain assumptions are in practice one of the main causes of requirements errors [2][8], and there is a high risk that without these checks one would synthesise a machine specification relying on an invalid domain model.

- Understanding the causes of unrealizability is essential to identify how to fix the problem. However, identifying these causes by examining the behaviours in our intermediate models $C_0$ and $C_I$ is extremely difficult and would benefit from automated support.

- Even on our small examples, we sometimes struggled to find how to modify a domain model to make the goals realizable. We sometimes believed we knew what the machine specification should be, and that it would be easier to write this specification first and apply the synthesis technique to derive the weakest domain assumption needed to satisfy the goal. This never worked: the synthesised domain assumptions were either invalid or too complex to check their validity.

- For all our examples, performance was always almost instantaneous (a couple of seconds at most). The most computationally expensive steps of our approach are the generation of LTS from FLTL and the determinization step.

In practice, this becomes an issue only if an FLTL assertion involves a large number of fluents (6 or more) or the deterministic LTS becomes too large. Most goal-oriented models will avoid these cases because they describe partial views related to specific goals. If needed, performance might be improved with symbolic techniques [15].

Much work remains to be done before automated specification synthesis becomes more widely applicable and cost-effective. The research priorities are (1) to provide explanations about why a goal is unrealistic and how to fix it, and (2) to facilitate the modeller’s understanding of the synthesised models, for example by inferring declarative required pre- and trigger conditions from deontic IO LTS.

VIII. RELATED WORK

Our formal foundation is based the KAOS semantics of agents that defined realizability in a requirements context but without automating realizability checking [4]. It also solves previous limitations for relating declarative requirements and even-based behaviour models [25]. Unlike interactive techniques for synthesising behaviour models from goals and scenarios [37][38], our approach does not rely on modellers to guide the synthesis. Furthermore, these works do not consider the question of realizability of the synthesised models.

Modal Transition System (MTS) is another formalism extending LTS with a distinction between may and must transitions [39]. May and must transitions in MTS are designtime concepts used to model uncertainties about which events should be enabled in which state. In MTS, a may transition is one that may be enabled, a must transition is one that must be enabled. In contrast, permissions and obligations in deontic IO LTS are run-time concepts. An agent’s obligation denotes transitions that must be performed before the next tick. Such obligations can’t be modelled in MTS. Both formalisms are intended to support incremental model elaboration. Whether and how the two approaches should be combined is a topic for further study.

Our approach addresses a problem of controller synthesis under partial observability for discrete-time models. Previous solutions rely on assumptions about the interactions between the controller (the machine) and its environment that are too restrictive for requirements modelling. Notably, Lin and Wonham rely on a distinction between prohibitive and forcible events that is irrelevant for requirements modelling [13]. Kupferman and Vardi assume that the environment and machine act in turn [12]. Our approach is more general and allows such assumption to be modelled explicitly as domain assumptions. Our work also differs from those in its ability to take as input goals and domain models specified in a variety of formalisms such as FSP, FLTL, and KAOS. Our algorithm extends standard synthesis algorithms using determinisation and backward error propagation (notably [33]) by its handling of tick events in the context of deontic IO LTS.

Recent work in the area of controller synthesis have focussed on increasing expressive power (e.g. to restricted forms of liveness properties but not under partial observability [16][19][20]), on improving performance by using symbolic techniques [15] and on developing sound theories for compositional synthesis under partial observability for dense time models [17][18]. The independence progress constraint of
deontic IO LTS is the discrete-time equivalent of the corresponding constraint recently introduced for dense timed I/O automata [18]. Our work differs from those by its focus on requirements modelling. Our primary objective is to define agent’s permission and obligation, not to model timed-systems; our use of tick to distinguish stable from transient states is a convenient way to model obligations with minimal extensions to standard LTS. This has the advantage of facilitating integration with existing requirements modelling techniques using LTS for analysis and as semantic domain.

IX. CONCLUSION

Specification synthesis from goals may eventually help resolving the lack of formal specification that hinders software testing and verification. However, such technique must be grounded on a formalism that is adequate for requirements modelling and compatible with a compositional goal-oriented elaboration process. Previous formalisms such as input-output and interface automata do not satisfy these criteria. We have introduced deontic IO LTS and a novel specification synthesis technique to serve these purposes. We have shown how our approach helps constructing and analyzing alternative requirements models relying on different synchrony assumptions or on no synchrony assumption at all. In the future, we intend to develop techniques to explain the causes of unrealizability and to translate back and forth between deontic IO LTS and requirements modelling languages.

REFERENCES