10-2014

Contract-Based Integration of Cyber-Physical Analyses

Ivan Ruchkin  
Carnegie Mellon University

Dionisio de Niz  
Carnegie Mellon University

Sagar Chaki  
Carnegie Mellon University

David Garlan  
Carnegie Mellon University

Follow this and additional works at: http://repository.cmu.edu/isr

Part of the Software Engineering Commons

Published In
ABSTRACT
Developing cyber-physical systems involves creating systems with properties from multiple domains, e.g., timing, logical correctness, thermal resilience, aerodynamics, and mechanical stress. In today’s industrial practice, multiple analyses are used to obtain and verify such properties. Unfortunately, given that these analyses originate from different scientific domains, they abstract away interactions among themselves, risking the invalidation of their results. Specifically, one challenge is to ensure that an analysis is never applied to a model that violates its assumptions. Since such violation can originate from the updating of the model by another analysis, analyses must be executed in the correct order. Another challenge is to do this soundly and scalably over models of realistic complexity and diverse set of analyses. To address these challenges, we develop an analysis integration approach that uses contracts to specify dependencies between analyses, determine their correct orders of application, and specify and verify applicability conditions across multiple domains. We present an implementation of our approach, and demonstrate its effectiveness, extensibility, and scalability.

General Terms
Verification, Design, Theory

Keywords
Cyber-physical systems, analysis, real-time scheduling, thermal runaway, model checking, battery scheduling, analysis contracts, virtual integration

1. INTRODUCTION
The development of today’s industrial-scale cyber-physical systems (CPS) is heavily driven by models and analyses. This trend is expected to strengthen, since it enables CPSs to be developed, upgraded, integrated, and verified virtually through models before manufacturing starts. Modeling also supports collaborative development by different teams, and fosters early error detection, faster development, and lower costs. In particular, analyses enable model creation and verification at design time to guarantee important quality attributes, such as control stability, schedulability, power consumption, safety, and security.

These analyses emerge from different scientific domains, such as timing, logical correctness, and thermal resilience. Consequently, they focus on different CPS abstractions that interact in subtle ways. This leads to two problems that render analysis results untrustworthy: (i) one analysis modifies a system model in a way that violates the assumptions made by another, e.g., a real-time task-allocation algorithm assigns a set of threads to a processor scheduled via a dynamic priority algorithm, thus violating the fixed priority assumption made by a model checker; (ii) the specification of such assumptions and the detection of their violation are left implicit in the hands of human designers that, more often than not, are unable to cope with their complexity and subtlety due to the inter-domain nature of the assumptions.

As a consequence, these problems are currently discovered very late during system integration, leading to costly fixes. This issue is particularly prevalent in multi-tier industries, such as avionics and automotive, where systems are integrated from independently-developed parts, designs of which are analyzed with a mishmash of tools. It is currently mitigated in an ad-hoc and manual way, which is neither scalable, nor able to provide a high degree of assurance.

In this paper, we present and evaluate an alternative solution that is mathematically rigorous and automated. Our approach consists of two parts: (i) contract specifications for analyses in a language with well-defined syntax and semantics. A contract for an analysis expresses both the assumption under which it produces a sound result, and the guarantee about the resulting modified model. (ii) An algorithm that computes inter-dependencies between analysis contracts, ensures that they are consistent, and executes them in an order guaranteeing soundness of all analysis results. More specifically, we make the following contributions.

First, we present a new language for specifying analysis contracts, and define its syntax and semantics. Our language finds a balance between expressiveness and decidability to support contracts that capture both design-time and runtime system aspects. An example is the frequency scaling analysis, which assumes that the runtime scheduling of threads allocated at design-time to the same CPU is behaviorally equivalent to deadline monotonic. To this end, our contract language combines a many-sorted first-order logic with a variant of linear temporal logic, propositions of which are derived from predicates over the system state. The logical nature of the language also makes it applicable to multiple analysis domains. In addition, validity of contracts expressed in our language is efficiently decidable.

Second, we present a contract verification algorithm that takes a set of analysis contracts and an architectural CPS model as input, computes the dependencies between the contracts, and uses this dependency to execute the analyses over the model in an order guaranteed to produce sound results. During this process, our algorithm checks the validity of each contract as follows: (i) before an analysis is executed, the validity of its assumption is checked over the input model; and (ii) after the analysis completes, the validity of its guarantee is ensured over the output model. Moreover, the validity is checked in a sound and exhaustive manner via co-operative application of an SMT solver (to the design-time aspect) and a model checker (to the runtime aspect) of the contract.

Finally, we implement our approach and demonstrate its effectiveness, extensibility, and scalability with a case study that involves multiple analyses from two domains — real-

Contract-Based Integration of Cyber-Physical Analyses
time thread scheduling and battery cell scheduling. Our implementation is based on OSATE [20], which enables us to handle CPS models described in the Architecture Analysis and Design Language (AADL) [8], an SAE standard. It also uses state-of-the-art tools Z3 [9] and Spin [13] for SMT solving and model checking, respectively. We show how our approach detects subtle bugs in interactions between analyses, and how the use of advanced tools enables it to scale to systems of realistic complexity.

The rest of the paper is organized as follows. Sec. 2 introduces a running example of a system and analyses used in its design. Sec. 3 presents the analysis contract language. Sec. 4 presents our contract verification algorithm. Sec. 5 and Sec. 6 present our implementation and evaluation, respectively. We wrap up by surveying related work in Sec. 7 and concluding in Sec. 8.

2. RUNNING EXAMPLE

Consider a reconnaissance aircraft that must satisfy certain security, power, thermal, timing, and logical requirements. It is controlled by a set of threads (a.k.a. tasks) with different security levels executing on several processors. Each thread executes an infinite sequence of jobs triggered periodically. A job is a finite computation, e.g., a control correction to aircraft stability. The system has dynamic multi-cell batteries with configurable connections between cells so that some cells recharge while others are discharging [12]. Thread scheduling policies, processor frequencies and voltages, battery cell scheduling policies, and allocation of threads to processors are adjustable parameters that different analyses set and use to verify the system’s requirements.

The aircraft system has to satisfy several requirements: (i) from the security viewpoint, parts of the system with sensitive information must be protected from less sensitive parts, therefore threads with different security levels should not execute on the same processor; (ii) from the timing perspective, all jobs must meet deadlines required by the control algorithms (e.g., for flight stability); (iii) from the electrical domain, processors must draw minimal power, switching to the minimal frequency possible, thereby maximizing battery lifetime; (iv) logically, threads must be free of deadlocks and race conditions; (v) and from the thermal domain, even if a battery cell overheats, it should not trigger a chain reaction called thermal runaway [3].

All of these requirements can be satisfied individually with different analysis tools. However, ensuring that they are all satisfied together is challenging, since one tool can select some design parameters that violate the assumptions of another, as discussed before. Similarly, creating a single overarching analysis that takes into account all requirements is intractable. Our approach uses each analysis as is, but complements them with analysis contracts that allow us to model their interdependencies and ensure their sound application. This enables sound and tractable verification of all the system requirements.

As an example for the rest of the paper, we consider the following analyses: (i) thread co-location security: computes permissible thread co-locations based on security classes; (ii) bin packing [27]: assigns threads on processors to ensure schedulability; (iii) frequency scaling: minimizes the processor frequency given the threads assigned to processors; (iv) REK model checking [3]: checks if threads satisfy user-specified safety properties; (v) thermal runaway: determines patterns of battery cell connections that lead to thermal runaway; and (vi) battery scheduling: determines a battery scheduler given the required operation time and battery size.

Arbitrary independent use of these analysis can lead to unsound results. For example, running the bin packing analysis before the co-location security analysis may violate thread co-location constraints set by the latter but not present at the time we run the former. Similarly, using the frequency scaling algorithm that assumes a deadline-monotonic scheduler on a processor that uses the earliest deadline first scheduler may produce unsound results. In this paper we demonstrate how our approach enables systematic integration of these analyses ensuring satisfaction of interdependencies and assumptions of analyses.

3. CONTRACT SPECIFICATION

In this section we present our contract language, and use it to formalize contracts for the analyses from Sec. 2.

3.1 Analysis Domain

We formalize an analysis domain as a “signature” that “externalizes” the domain’s concepts.

**Definition 1.** An analysis domain $\sigma$ is a many-sorted signature $(\mathcal{A}, \mathcal{S}, \mathcal{R}, \mathcal{T}, \{\cdot\}, \cdot)$ where:

- $\mathcal{A}$ is a set of sorts: $\mathcal{A} = \{A_i\}$.

Examples of sorts are Booleans ($B$), integers ($Z$), threads, processors, and scheduling protocols.

- $\mathcal{S}$ is a set of static properties: $\mathcal{S} = \{S_i\}$. Each static property is a typed function $S_i : A_i \times \ldots \times A_j \to A_k$.

Static properties capture system invariants set at design-time, e.g., standard operators like addition ($+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$), conjunction ($\land : \mathcal{B} \times \mathcal{B} \to \mathcal{B}$), and analysis-specific properties, such as thread periods and processor frequencies. Note that relations, like $<$, are functions with a Boolean range.

- $\mathcal{R}$ is a finite set of runtime properties: $\mathcal{R} = \{R_i\}$, $R_i : A_i \times \ldots \times A_j \to A_k$.

Runtime properties capture system aspects that depend on $\mathcal{S}$ but change during execution, such as preemption between threads or connectivity between battery cells. Given a runtime state $q$, $q(R_i)$ means the evaluation of $R_i$ in $q$.

- $\mathcal{T}$ is the execution semantics of the domain.

Informally, $\mathcal{T}$ is a set of infinite sequences of assignments to the runtime properties. The idea is that each sequence corresponds to an execution of the system, and specifically to the values of the runtime properties observed at the successive states of the execution. The executions are infinite since we are interested in analyzing reactive systems which, in general, do not terminate. $\mathcal{T}$ is discussed in detail for specific domains in Sec. 4.2.3 and 4.2.4.

- $\{\cdot\}$ is a partial interpretation of $\mathcal{A}$ and $\mathcal{S}$. It assigns permissible values to some of the sorts in $\mathcal{A}$ and value mappings to some elements of $\mathcal{S}$. 

Intuitively, $\llbracket \cdot \rrbracket_m$ interprets common sorts and operators in the standard way. For example $\llbracket \mathbb{B}\rrbracket = \mathbb{B}$, $\llbracket \mathbb{Z}\rrbracket = \mathbb{Z}$, $\llbracket + \rrbracket$ is integer addition, and $\llbracket \land \rrbracket$ is Boolean conjunction, and so on. In addition, $\llbracket \cdot \rrbracket_m$ interprets domain-specific sorts, e.g., the set of permissible scheduling protocols.

Note that $\sigma$ represents an analytic domain for the purpose of specifying its external contract, but does not limit internal reasoning of the analysis about the domain. Also, $\llbracket \cdot \rrbracket_m$ leaves some elements of $A$ and $S$ (e.g., set of threads), and $T$, uninterpreted. This is completed by the architectural model (or model, for short).

**Definition 2.** An architectural model $M$ is an interpretation $\llbracket \cdot \rrbracket_M$ of some elements of $A$ and $S$, and $T$.

For example, a set of three threads and their periods is specified by a model $M$ as $\llbracket \mathbb{T}\rrbracket_M = \{t_1, t_2, t_3\}$ and $\llbracket \text{Per}\rrbracket_M = \{t_1 \rightarrow 40, t_2 \rightarrow 50, t_3 \rightarrow 60\}$. The value of runtime properties depends on the execution state, as follows. Let $\llbracket \cdot \rrbracket$ denote the combination of $\llbracket \cdot \rrbracket_m$ and $\llbracket \cdot \rrbracket_M$. Formally, state $q$ maps each runtime property $R_i : A_1 \times \cdots \times A_j \rightarrow A_k$ to a function $q(R_i) : [A_1] \times \cdots \times [A_j] \rightarrow [A_k]$. Let $Q$ be the set of all states, and $Q^\omega$ the set of all infinite sequences of states (i.e., executions). Then $\llbracket \mathbb{T}\rrbracket_M \subseteq Q^\omega$. In other words, $\llbracket \mathbb{T}\rrbracket_M$ is set of executions of the system defined by $M$. Note that $R$ is interpreted indirectly and modally via $\llbracket \mathbb{T}\rrbracket_M$. Specifically, each state $q$ in each execution in $\llbracket \mathbb{T}\rrbracket_M$ gives an interpretation $q(R_i)$ to each $R_i \in R$.

We require that $\llbracket \cdot \rrbracket$ interpret $A$, $S$, and $T$ completely and unambiguously. In general, analyses from multiple domains are applied to a single model $M$. Therefore, $M$ must complete the interpretations for $A$, $S$, and $T$ from each such domain.

### 3.2 Contract Language

Our contract language consists of a combination of first-order and temporal logic formulas over the sorts and properties of a target domain. We present it in stages, beginning with the syntax of contract formulas.

#### 3.2.1 Contract Formula Syntax

We first define the static fragment of contract formulas. Consider a domain $\sigma = (A, S, R, T, \llbracket \cdot \rrbracket_m)$. Let $V$ be a denumerable set of typed variables, $V = \{v_1, \ldots, v_j\}$. Then the set of static formulas over $\sigma$, denoted $\phi$, is defined by the following grammar:

$$\phi ::= v_1 \ldots v_j$$

where $v \in V$, $f \in S$ with arity $j$, and $e_1, \ldots, e_j \in \phi$.

**Typing.** Formulas are well-typed. Variables are typed with their sorts. If the type of $f$ is $A_1 \times \cdots \times A_j \rightarrow A_k$, then the type of $f(e_1, \ldots, e_j)$ is $A_k$ and it is well-typed iff the type of each $e_i$ is $A_i$. For simplicity, we write $v_1 + v_2$ instead of $+(v_1, v_2)$, $e_1 \land e_2$ instead of $\land(e_1, e_2)$, etc.

**Temporal Logic Formulas.** We now turn our attention to the temporal fragment of contract formulas. Since we are interested in expressing properties of infinite executions of reactive systems, we use a variant of next-time-free linear temporal logic (LTL) [21]. The key difference with standard LTL is that propositions in our logic are not atomic, but are formulas constructed from runtime and static properties. The set of all such runtime formulas is defined by the following grammar:

$$RF ::= \phi$$

where $\phi \in V$, $f \in S \cup R$ with arity $j$, and $e_1, \ldots, e_j \in \phi$.

Runtime formulas are also well-typed in the same way as static formulas. Then our LTL formulas, denoted $\psi$, are defined by the following grammar:

$$\psi ::= p \mid \neg \psi \mid \psi \land \psi \mid \psi \lor \psi \mid \exists v_1 \ldots v_j. \phi$$

where $p \in RF$ is a runtime formula with Boolean type. Note that other temporal operators, such as $G$ and $F$, are defined in terms of $\neg$, $\land$, and $\lor$ in the standard manner. Finally, we define contract formulas using $\phi$ and $\psi$.

**Definition 3.** Given a domain $\sigma$, a set of contract formulas $\mathcal{F}_\sigma$ is defined by the following grammar:

$$\mathcal{F}_\sigma ::= \forall v_1 \ldots v_j. \phi \mid \exists v_1 \ldots v_j. \phi$$

where $\phi$ is a static formula of Boolean type, and $\psi$ is a LTL formula – both over variables $v_1, \ldots, v_j$. Thus, a contract formula can be purely first-order (i.e., the first two forms) or a combination of first-order and LTL (i.e., the last two forms). The meaning of the last form is that every assignment of $V$ that satisfies $\phi$ also satisfies $\psi$. The meaning of the last form is that at least one assignment of $V$ satisfies both $\phi$ and $\psi$. Note that formulas without variables are also allowed. We are now ready to define analyses and their contracts.

#### 3.2.2 Analysis Contracts

Functionally, an analysis $An$ takes an architectural model $M_i$ as input and produces a new architectural model $M_O = An(M_i)$ as output. The contract for $An$ specifies restrictions on valid input models and valid output models, as well as the model properties its reads and modifies.

**Definition 4.** A contract $C$ for an analysis $An$ over a domain $\sigma$ is a 4-tuple $C = (I, O, A, G)$, where:

- $I \subseteq A \cup S$ are sorts and properties read by $An$.
- $O \subseteq A \cup S$ are sorts and properties modified by $An$.
- $A \subseteq \mathcal{F}_\sigma$ are assumptions – contract formulas that must be satisfied by every valid input model to $An$.
- $G \subseteq \mathcal{F}_\sigma$ are guarantees – contract formulas over that must be satisfied by every valid output model from $An$.

In order to determine whether $An$ satisfies its contract, we must first define what it means for $An$ to satisfy a contract formula. This is the topic of the next subsection.

#### 3.2.3 Contract Semantics

We start with the evaluation of static formulas and build up to defining satisfaction of a contract. Let the interpretation of sort $A$ be $\llbracket A \rrbracket$ and the interpretation of $f : A_1 \times \cdots \times A_j \rightarrow A_k$ be $\llbracket f \rrbracket : [A_1] \times \cdots \times [A_j] \rightarrow [A_k]$. An assignment $\mu$ maps each variable $v : A$ to an element of $\llbracket A \rrbracket$. Given a static formula $\phi$, and an assignment $\mu$, $\llbracket \phi, \mu \rrbracket$ is the evaluation of $\phi$ under $\mu$ defined as:

$$\llbracket v, \mu \rrbracket = \mu(v)$$

$$\llbracket [f(e_1, \ldots, e_j)], \mu \rrbracket = \llbracket [f([e_1, \mu], \ldots, [e_j, \mu]) \rrbracket$$
Note that if the type of \( \phi \) is \( A \), then \( \langle \phi, \mu \rangle \in [A] \). The evaluation of a runtime formula \( RF \) under an assignment \( \mu \) in a state \( q \), denoted \( [RF, \mu, q] \), is defined as:

\[
[v, \mu, q] = \mu(v)
\]

\[
[f(e_1, \ldots, e_j), \mu, q] = [f][\{e_1, \mu, q\}, \ldots, \{e_j, \mu, q\}]. f \in S
\]

An execution \( \pi = q_0, q_1, \ldots \) satisfies an LTL formula \( \psi \) under assignment \( \mu \), denoted \( \pi, \mu \models \psi \), if:

- If \( \psi \in RF \) then \( \pi, \mu \models \psi \) iff \( [\psi, \mu, q_0] = \top \).
- \( \pi, \mu \models \neg \psi' \) iff \( \pi, \mu \models \psi \).
- \( \pi, \mu \models \psi \) U \( \psi \) iff there exists \( i \geq 0 \) such that for all \( 0 \leq j < i \), \( \pi, \mu \models \psi \) and \( \pi^i, \mu \models \psi_2 \), where \( \pi^i \) is the (infinite) suffix of \( \pi \) starting with state \( q_i \).

Consider a model \( M \). Let \( [\cdot]_M \) be the combination of \( [\cdot]_A \) and \( [\cdot]_M \). A contract formula \( f \in F_\pi \) is satisfied by \( M \), denoted \( M \models f \), based on the form of \( f \) (see Def. \( \ref{def:contract} \)) as follows:

- \( f \) is of the first form and \( \forall \mu \in \mathcal{V}. [f, \mu] = \top \).
- \( f \) is of the second form and \( \exists \mu \in \mathcal{V}. [f, \mu] = \top \).
- \( f \) is of the third form and \( \forall \mu \in \mathcal{V}. \forall \pi \in [T]. [\phi, \mu] = \top \Rightarrow \pi, \mu \models \psi. \)
- \( f \) is of the fourth form and \( \exists \mu \in \mathcal{V}. \forall \pi \in [T]. [\phi, \mu] = \top \land \pi, \mu \models \psi. \)

Thus, first-order quantification over static formulas is interpreted in a natural manner. Universal quantification over a static formula and an LTL formula holds if and only if all assignments that satisfy the static formula also satisfy the LTL formula. Existential quantification over a static formula and an LTL formula holds if and only if there exists an assignment that satisfies both static and LTL formulas.

**Analysis Applicability.** A model to which an analysis is applied should satisfy its assumption, and the resulting model should satisfy its guarantee. Formally:

**Definition 5.** A model \( M \) is applicable to an analysis \( An \) with contract \( An.C = (I, O, A, G) \) – denoted \( M \models C \) – iff

\[
\forall a \in A. M \models a \land \forall g \in G. An(M) \models g.
\]

In Sec. \( \ref{sec:analysis} \) we present an algorithm to decide \( M \models C \). Now, to highlight our approach, we turn to formalizing analysis domains and contracts for the example from Sec. \( \ref{sec:example} \).

### 3.3 Scheduling Domain

The scheduling domain \( S_{Sched} \) encodes the semantics of the real-time scheduling of threads along with their allocation to processors. Analyzers in this domain decide valid thread allocations, priority assignments, check schedulability according to a selected scheduling policy, determine processor frequency, etc. The domain is defined as \( S_{Sched} = (A_{Sched}, T_{Sched}, R_{Sched}, T_{Sched}, S_{Sched}) \). In addition to Booleans \( B \) and integers \( Z \), \( A_{Sched} \) has reals \( R \), threads \( T \), CPUs \( C \), thread security classes \( SecCl \), and thread scheduling policies \( SchedPol \). Sorts \( B, Z, R \) are interpreted by \( \{0, 1\} \) in a standard way. There are three security classes – normal, secret, and top-secret – \( [SecCl]_{Sched} = \{normal, secret, topsecret\} \) and three scheduling policies – rate monotonic scheduling (RMS), earliest deadline first (EDF) \( \gamma \), and deadline monotonic scheduling (DMS) \( \varphi \) – \( [SchedPol]_{Sched} \). Sorts \( T \) and \( C \) are interpreted by \( \{0, 1\} \).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per</td>
<td>( T \rightarrow Z )</td>
<td>Thread’s period.</td>
</tr>
<tr>
<td>Dline</td>
<td>( T \rightarrow Z )</td>
<td>Thread’s deadline.</td>
</tr>
<tr>
<td>WCET</td>
<td>( T \rightarrow Z )</td>
<td>Thread’s worst case execution time.</td>
</tr>
<tr>
<td>ThSecCl</td>
<td>( T \rightarrow SecCl )</td>
<td>Thread’s security class.</td>
</tr>
<tr>
<td>CPUSchedPol</td>
<td>( C \rightarrow SchedPol )</td>
<td>CPU’s scheduling policy.</td>
</tr>
<tr>
<td>CPUFreq</td>
<td>( C \rightarrow R )</td>
<td>CPU’s normalized frequency.</td>
</tr>
<tr>
<td>NetColor</td>
<td>( T \rightarrow 2^Z )</td>
<td>Thread mapped to a set of threads that should not share the same CPU as ( t ).</td>
</tr>
<tr>
<td>CPUBind</td>
<td>( T \rightarrow C )</td>
<td>Thread-to-CPU binding.</td>
</tr>
<tr>
<td>ThSafe</td>
<td>( C \rightarrow B )</td>
<td>Flag whether CPU’s threads are thread-safe.</td>
</tr>
<tr>
<td>Voltage</td>
<td>( () \rightarrow R )</td>
<td>Required system voltage. (^2)</td>
</tr>
</tbody>
</table>

\(^1\)A real number between 0 and 1.

\(^2\)Voltage is a nullary function, or a Boolean constant. We consider a simplified example where the system voltage is far apart physically they are.

### 3.4 Battery Domain

The domain of battery design and usage \( \sigma_{Batt} = (A_{Batt}, S_{Batt}, R_{Batt}, T_{Batt}, [\cdot]_{Batt}) \) is defined as follows. Sorts \( B, Z, R \in A_{Batt} \) and their interpretations are identical to \( S_{Sched} \). The set of batteries is \( B \in A_{Batt} \), and \( ConnSchedPol \in A_{Batt} \) is the set of three battery scheduling policies \( \{\text{unweighed round robin with fixed cell group}(\text{URwRR}), \text{weighed round robin with fixed cell group}(\text{WRwRR})\} \). The domain of battery design and usage \( \sigma_{Batt} \) contains the properties \( S_{Batt} \) that are specified in Tab. 2.

Informally, the battery execution consists of continuous charging, discharging, and rest of cells. The precise semantics \( [\cdot]_{Batt} \) is model-dependent and defined in Sec. 3.

There is one runtime property \( R_{Batt} = (\text{TN}: Z \rightarrow Z) \). Informally, when the system is in state \( q \), \( q(\text{TN}(i)) \) denotes the number of cells with \( i \) thermal neighbors – cells that exchange heat conductively through a connector. This is motivated by results \( \gamma \); there is a close connection between thermal neighbors and thermal runaway. Specifically, there exist constants \( K(i) : i \in Z \) such that a state \( q \) triggers a thermal runaway if it violates the condition:

\[
\sum K(i) \times q(\text{TN}(i)) \geq 0
\]
Table 2: Static properties of \( \sigma_{\text{Batt}} \).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage</td>
<td>( B \to K )</td>
<td>Required system voltage.</td>
</tr>
<tr>
<td>BattRows</td>
<td>( B \to Z )</td>
<td>Battery's cell rows.</td>
</tr>
<tr>
<td>BattCols</td>
<td>( B \to Z )</td>
<td>Battery's cell columns.</td>
</tr>
<tr>
<td>BattCommSchedPol</td>
<td>( B \to Z )</td>
<td>Battery’s cell scheduling policy.</td>
</tr>
<tr>
<td>SerialReq</td>
<td>( B \to Z )</td>
<td>Number of cells required to connect in series.</td>
</tr>
<tr>
<td>ParalReq</td>
<td>( B \to Z )</td>
<td>Number of cells required to connect in parallel.</td>
</tr>
<tr>
<td>HasReqdLifetime</td>
<td>( B \to B )</td>
<td>Flag whether a battery has the lifetime required.</td>
</tr>
</tbody>
</table>

needed to estimate \( K \). 

3.5 Analysis Contracts for Running Example

Using the domains signatures \( \sigma_{\text{Sched}} \) and \( \sigma_{\text{Batt}} \) we define the contracts for analyses \( \mathcal{A} \mathcal{V} \) from Sec. 2.

Secure thread allocation (\( \sigma_{\text{Sched}} \)) has contract \( \mathcal{C}_{\text{SecAlloc}} : I = \{ T, \text{ThsCl} \}, O = \{ \text{NotColoc} \}, A = \varnothing \), and \( G = \{ g \} \) where \( g \) is:

\[
\forall t_1, t_2, \text{ThsCl}(t_1) \neq \text{ThsCl}(t_2) \Rightarrow t_1 \notin \text{NotColoc}(t_2)
\]

Thus, \( \sigma_{\text{Sched}} \) makes no assumptions, but guarantees that threads with different security classes are never co-located.

We omit sorts, e.g., \( t_1 : T \) and \( t_2 : T \), since they are implied by typing rules.

Bin packing (\( \sigma_{\text{BinPack}} \)) has contract \( \mathcal{C}_{\text{BinPack}} : I = \{ T, C, \text{NotColoc, Per, WCET, Dline} \}, O = \{ \text{CPUBind} \}, A = \varnothing \), and \( G = \{ g \} \) where \( g \) is:

\[
\forall t_1, t_2, t_1 \notin \text{NotColoc}(t_2) \Rightarrow \text{CPUBind}(t_1) \neq \text{CPUBind}(t_2)
\]

Thus, \( \sigma_{\text{BinPack}} \) makes no assumptions but guarantees that threads that should not be co-located are never scheduled on the same CPU.

Frequency scaling (\( \sigma_{\text{FreqSc}} \)) has contract \( \mathcal{C}_{\text{FreqSc}} : I = \{ T, C, \text{CPUBind, Dline} \}, O = \{ \text{CPUFreq} \}, A = \varnothing \), and

\[
A \triangleq \{ \forall t_1, t_2, \text{CPUBind}(t_1) = \text{CPUBind}(t_2) \} \quad \text{and} \quad
G \triangleq \{ \text{CanPrmppt}(t_1, t_2) \Rightarrow \text{Dline}(t_1) < \text{Dline}(t_2) \}
\]

Thus, \( \sigma_{\text{FreqSc}} \) makes no guarantees but assumes that the scheduling used is semantically equivalent to a deadline-monotonic scheduling policy. Note that a scheduling policy can be DMS for a specific model, e.g., rate-monotonic scheduling (RMS) for a harmonic model, even thought it is not deadline monotonic in general.

Model checking with REK (\( \sigma_{\text{REK}} \)) has contract \( \mathcal{C}_{\text{REK}} : I = \{ T, C, \text{Per, Dline, WCET, CPUBind} \}, O = \{ \text{ThSafe} \}, G = \varnothing \), and \( A = \{ a_1, a_2 \} \) where:

\[
a_1 \triangleq \forall t, \text{Per}(t) = \text{Dline}(t), \\
a_2 \triangleq \forall t_1, t_2, G \triangleq \text{CanPrmppt}(t_1, t_2) \Rightarrow G \neg \text{CanPrmppt}(t_2, t_1).
\]

REK \( \square \) takes threads and their marked source code files (which we didn’t include into the formal example) as input and verifies whether the system is safe, where safety is expressed as assertions embedded in the source code. \( \sigma_{\text{REK}} \) assumes implicit deadlines and fixed-priority scheduling. Prior to this work, the only way to apply REK was to use RMS. However, our contract mechanism allows for a broader scope of applicability. Note that \( a_1 \) expresses implicit deadlines, while \( a_2 \) expresses fixed priority scheduling, i.e., if \( t_1 \) preempts \( t_2 \), then \( t_2 \) should never be able to preempt \( t_1 \).

Thermal runaway (\( \sigma_{\text{ThRun}} \)) has contract \( \mathcal{C}_{\text{ThRun}} : I = \{ B, \text{BattRows, BattCols, Voltage} \}, O = \{ K \}, A = \varnothing \), and \( G = \varnothing \). Note that \( \sigma_{\text{ThRun}} \) has no assumptions or guarantees, but has dependency with defined below battery scheduling via \( I \) and \( O \). It determines the patterns, which, given concrete battery characteristics, would result into a thermal runaway. In our example, we encode these patterns as \( K(i) \) for \( i : Z \in [0, 3] \). \( \sigma_{\text{ThRun}} \) determines \( K \) through experimentation, adjusting \( K \) so that acceptable heat propagation patterns satisfy \( [1] \), and unacceptable ones violate it.

Battery scheduling (\( \sigma_{\text{BattSched}} \)) has contract \( \mathcal{C}_{\text{BattSched}} : I = \{ B, \text{BattRows, BattCols, Voltage} \}, O = \{ \text{BattCommSchedPol}, \text{HasReqdLifetime}, \text{SerialReq}, \text{ParalReq} \}, A = \varnothing \), and \( G = \{ g \} \) where \( g \) is:

\[
G \triangleq \{ \text{K}(0) \times \text{TN}(0) + \text{K}(1) \times \text{TN}(1) + \\
\text{K}(2) \times \text{TN}(2) + \text{K}(3) \times \text{TN}(3) \geq 0 \}
\]

\( \sigma_{\text{BattSched}} \) computes a battery cell connectivity scheduler that maximizes the battery lifetime given the battery characteristics and output requirements. It sets a flag indicating whether the battery with the selected scheduler meets the lifetime requirement. Since the scheduling is not aware of the thermal runaway, the determined scheduler needs to be verified against the thermal runaway pattern, hence the guarantee. \( \sigma_{\text{BattSched}} \) also sets cell group characteristics \( \text{SerialReq} \) and \( \text{ParalReq} \) that are used to verify its guarantee.

4. CONTRACT VERIFICATION

This section presents our contract verification algorithm, which takes a model \( M \) and a set of analyses \( \mathcal{A} \mathcal{V} \) and produces a correct execution of \( \mathcal{A} \mathcal{V} \) on \( M \), or aborts. The algorithm consists of the following steps: (i) determine an ordering \( \mathcal{O} \) of \( \mathcal{A} \mathcal{V} \) that respects all inter-analysis dependencies; (ii) process each analysis \( An \in \mathcal{A} \mathcal{V} \) with contract \( C = (I, O, A, G) \) in the order \( \mathcal{O} \) by: (iia) verifying \( \forall a \in A \land M = a \), (iib) updating \( M \) by executing \( An \), i.e., setting \( M \) to \( An(M) \), and verifying verifying \( \forall g \in G \land M = g \); and (iii) output the final \( M \) as the result. The algorithm aborts if either an appropriate ordering \( \mathcal{O} \) cannot be computed, if any of the verifications in Steps (iia) and (iic) fail, or the execution of \( An \) or \( M \) fails. Note that the algorithm ensures that all analyses produce valid results since: (a) an analysis \( An \) executes successfully on \( M \) only if \( M \equiv An.C \) (see Def. \( \Box \)) and (b) the ordering \( \mathcal{O} \) ensures that once an analysis has been executed, future values of \( M \) do not violate its assumptions.

4.1 Analysis Ordering

We begin with Step (i), which uses contracts to determine a correct ordering of analyses execution. The contract of analysis \( An \) is denoted \( C(An) \). For a contract \( C = (I, O, A, G) \), \( C.I \) means \( I, C.O \) means \( O \), etc.

Definition 6. Analysis contract \( C \) is dependent on
4.2 Analysis Applicability

We now focus on Steps (iia) and (iic) of our algorithm. Recall that the core problem here is to decide $M \models f$ where $f$ is a contract formula. In Step (iia) $f$ is one of the contract’s assumptions, while the Step (iic) it is one of the contract’s guarantees. The algorithm for verifying $M \models f$ depends on the form of $f$ (see Def. 2), and we consider each separately.

4.2.1 Verifying Purely First Order Formulas

If $f$ is a quantified first-order formula (i.e., the first two forms of Def. 2) we check $M \models f$ via Satisfiability Modulo Theories (SMT) solving. We first describe how to construct a SMT formula $\varphi(M, \phi)$ using SMT v2 syntax — given a model $M$ and a first-order formula $\phi$. The first step in constructing $\varphi(M, \phi)$ is defining the basic types. These are obtained directly from the sorts (A) of the analysis domain. Basic sorts like Boolean, integer, and float are already primitive types in SMT. Domain-specific sorts, such as threads and processors, are declared as integers using the define-sort SMT command. Subsequently, the IDs of the actual threads and processors are used as concrete values for their corresponding types. For example, if $M$ has five threads with IDs $[0, 4]$ and three processors with IDs $[0, 2]$, then $\varphi(M, \phi)$ has two types — thread and processor — defined as follows:

```
(define-sort thread () (Int))
(define-sort processor () (Int))
```

Subsequently, all variables of type $T$ have five legal values $[0, 4]$ — and all variables of type $C$ have three legal values $[0, 2]$ — and all variables of type $\theta$ have three legal values $\{true, false, unknown\}$.

Variables are also declared with appropriate types, e.g., variable $t_1: T$ is declared as: (declare-fun $t_1 () (thread)). Finally, the constraints in $\varphi(M, \phi)$ are obtained from:

- The interpretation of static properties of the domain. For example, if thread 0 has a period 20, then we add the constraint (assert (= (period 0) 20)).
- The model $\phi$ itself. For example if $\phi \equiv \text{Per}(t_1) < \text{Per}(t_2)$ we add the constraint (assert (< (period t1) (period t2))).

Given an SMT formula $\varphi$ as input, an SMT solver returns SAT if $\varphi$ is satisfiable, and UNSAT otherwise. Now checking $M \models f$ reduces to two cases:

- $f = \forall v_3 \cdot \cdots \cdot v_i \cdot \phi$ (form 1 of Def. 2): In this case we return YES if the SMT solver returns UNSAT for input $\varphi(M, \neg \phi)$ and NO otherwise.
- $f = \exists v_3 \cdot \cdots \cdot v_i \cdot \phi$ (form 2 of Def. 2): In this case we return YES if the SMT solver returns SAT for input $\varphi(M, \phi)$ and NO otherwise.

The correctness of our algorithm follows from our semantics and the construction of $\varphi(M, \phi)$. An example of $\varphi(M, \phi)$ constructed for $C_{BinPack}.G$ is shown in Fig. 2. The guarantee states that non-colocated threads should be bound to different processors, and has the first form of Def. 2. The SMT solver returns UNSAT, hence $M \models C_{BinPack}.G$.

4.2.2 Verifying First Order+LTL Formulas

We now show how to verify $f$ if it combines both first-order logic and LTL (i.e., the last two forms of Def. 2). This again has two cases:

- $f = \forall v_3 \cdot \cdots \cdot v_i \cdot \phi : \psi$ (form 3 of Def. 2): We first construct $\varphi(M, \phi)$. Next, we use the SMT solver iteratively to compute all satisfying solutions of $\varphi(M, \phi)$. To obtain all solutions, we use “blocking clauses”, i.e., once we obtain a solution, we add its negation to the formula before re-solving it. From each solution we construct the corresponding assignment $\mu$ to $\{v_3 \cdot \cdots \cdot v_i\}$. For each such assignment $\mu$, we check $\forall \pi \in [T]: \pi, \mu \models \psi$ using a model checker. The model
checking step is domain-specific and described in
the following subsections. We return YES if the model
checker finds no \( \psi \) violations for every \( \mu \), and NO oth-
erwise.

\[ f = \exists v_1 \cdots v_j : \phi : \psi \text{ (form of Def. 3)} \]

We first construct \( \varphi(M, \phi) \). Next, we use the SMT solver iter-
eatively to compute all assignments \( \mu \) to \( \{v_1 \cdots v_j\} \) as
in the previous case. For each assignment \( \mu \), we check
\( \forall \pi \in [T_2] \cdot \pi, \mu \models \psi \) using a model checker. We return
YES if the model checker find no \( \psi \) violations for at
least one \( \mu \), and NO otherwise.

The correctness of our algorithm follows from our semantics
and the construction of \( \varphi(M, \phi) \). Note that our algorithm
always terminates if the sort of each quantified variable \( v_i \)
interpreted to a finite domain (e.g., threads and batteries,
but not integers), since this means that there are only a
finite set of assignments to \( \{v_1 \cdots v_j\} \). This is indeed the
case for all analyses in our example. We now describe the model
checking step for the scheduling and battery domains.

### 4.2.3 Model Checking for Scheduling

The execution semantics \( [T_{Sched}] \) of the scheduling do-
main is defined as follows. Recall that each thread consists
of an infinite and periodic sequence of jobs. A state \( q \) of
the system corresponds to a point in time when a new job
arrives or a currently executing job terminates. An execution
consists of an infinite sequence of such states observed
at runtime. Note that multiple executions are possible due
due to the non-determinism in the time required by each job
to complete. Then \( [T_{Sched}] \) consists of all such executions.

We model \( [T_{Sched}] \) as a Kripke structure \( K([T_{Sched}]) \)
composed of a “task” process for each thread. Task pro-
cesses are periodic and their numeric characteristics –
(Per, Dline, WCET) – are specified by the model \( M \). There
are \( \lceil C \rceil_{\mu} \) processors, and each running task is allocated to a
processor dynamically. For each task process \( t \), \( K([T_{Sched}]) \)
has the following propositions:

- **Prior** \((t) : Z \) – the priority of \( t \).
- **Run** \((t) : B \) – whether a job of \( t \) is dispatched on a
  processor.
- **InQ** \((t) : B \) – whether a job of \( t \) has arrived but hasn’t
  been completed yet.
- **Prior** \((t) \) is set by the scheduling policy and decides which
tasks are executed. The last two propositions encode every
possible state of \( t \): idle if \( \neg \text{InQ}(t) \land \neg \text{Run}(t) \), waiting for
processor if \( \text{InQ}(t) \land \neg \text{Run}(t) \), and executing if \( \text{InQ}(t) \land \text{Run}(t) \).
Also, for any state \( q \) of \( K([T_{Sched}]) \), and threads \( t_1, t_2, q(\text{CanPrompt})(t_1, t_2) \) is \( T \) iff the following holds in \( q \):

\[
\text{Run}(t_1) \land \neg \text{Run}(t_2) \land \text{InQ}(t_2)
\]

Recall that our model checking problem is \( \forall \pi \in [T_{Sched}] \cdot
\pi, \mu \models \psi \), where \( \mu \) is a variable assignment. We solve this by:
(i) instantiating the LTL formula \( \psi \) to a propositional
LTL formula \( \psi_{prop} \) using \( \mu \); and (ii) using a model checker
to verify \( K([T_{Sched}]) \models \psi_{prop} \). For example, \( C_{\text{PrvqSt}, A} \)
is expressed as the following propositional LTL formula:

\[
\left( G \left( \text{Run}(\mu(t_1)) \land \neg \text{Run}(\mu(t_2)) \land \text{InQ}(\mu(t_2)) \right) \Rightarrow \text{Dline}(\mu(t_1)) \right)
\]

The correctness of our algorithm follows from the seman-
tics of our LTL formulas, the semantics of propositional LTL,
and the correctness of model checking.

#### 4.2.4 Model Checking For Battery

Let us now define the execution semantics of the battery do-
main \( [T_{Batt}] \). A battery consists of a matrix of cells \( \chi \) be-
ing continuously charged, discharged, connected and discon-
ected with each other. A state \( q \) of the system corresponds
to a point in time when either the charge or the connectivity
status of a cell changes. An execution consists of an infinite
sequence of such states observed at runtime. Note that many
such executions are possible due to the non-determinism in
the time required by cells to charge and discharge. Then
\( [T_{Batt}] \) consists of all such executions.

We model \( [T_{Batt}] \) as a Kripke structure \( K([T_{Batt}]) \)
with the following propositions for each cell \( c = (x, y) \in \chi \),
which is characterized by its physical coordinates \( x \in [0..\text{BatRows} – 1] \)
and \( y \in [0..\text{BatCols} – 1] \):

- **CellCharge** \((c) \) is the charge of \( c \). To simplify model
  checking we chose a Boolean abstraction for the cell
  charge, but other abstractions are possible too.
- **CellSt** \((c) \) is the status of \( c \) with possible values
  discharging, charging, and idle.
- **Gr** \((c) \) is the number of group of cells electrically con-
  nected in serial within which \( c \) is located. Groups are
treated as electrically connected in parallel with each
other. Every cell belongs to a group, but not every
group or cell is discharging.

\( TN \) is encoded as follows. Cells \( c_1 \) and \( c_2 \)
are thermal neighbors, denoted \( \text{istnbr}(c_1, c_2) \), if:
(i) \( c_1 \neq c_2 \); (ii) \( \text{Gr}(c_1) \neq \text{Gr}(c_2) \); (iii) \( |c_1 - c_2| +
|c_1 - x - c_2, x| \leq TNDIST \); (iv) \( \text{CellCharge}(c_1) =
\text{CellCharge}(c_2) = \text{discharging} \). The number of thermal neighbors of cell \( c \)
is \( \text{ntnbr}(c) = |\{c' \in \chi : \text{istnbr}(c, c')\}| \). Finally, \( TN(t) \)
\( = |\{c' \in \chi : \text{ntnbr}(c) = i\}| \).

### 5. IMPLEMENTATION

In this section we present the implementation of our anal-
ysis contracts tool in OSATE – an open source environment
for AADL modeling \( \S \). In the following we describe how
our tool implements the concepts of this paper, and how
Spin/Promela is used for model checking.

#### 5.1 Contracts Framework

Let us start by describing how the different elements of our
analysis contracts are represented. First, the architectural
model \( M \) is described in an AADL model. Secondly, the
domain sorts, like SecCl and ConnSchedPol, are defined as
AADL property types. Thirdly, thread \( T \) processor \( C \) sorts
are derived from the corresponding threads and processors
from the AADL model, and the device sort \( B \) is also derived
from the corresponding AADL devices in the model. \( S_{Sched} \)
and \( S_{Batt} \) are described using properties of the components.
Finally, we specify the contracts as a sub-language annex
in AADL to capture \( I, O, A, \) and \( G \) of analyses.

Fig. \( \S \) depicts the architecture of our tool. Analysis con-
tracts \( C \) are associated with AADL component types, while
\footnote{For our calculations we use \( TNDIST = 2 \).}
M is derived from the AADL main system instance. Initially, our tool converts M from AADL into a database representation using the OSATE-database converter. All subsequent steps will be performed using this database (model DB). The analysis execution controller constructs the analysis graph γ, as described in Sec. 5.1 and delegates the verification of A and G to an appropriate verification engine, which is determined by the form in Def. 2 along with A, T, and R in the contract. A selected verification engine populates an SMT problem and a Promela model with values from the model DB, executes the verification via Z3 and Spin, and interprets the outputs. To verify forms 3 and 2, as well as new analysis tools (e.g., a higher-fidelity method of γ)

5.2 Scheduling Domain Implementation

We encode $K([T_{Sched}])$ as a single-process Promela program. The program maintains the state CellCharge, CellSt, Gr discussed in Sec. 4.4. The program execution works in two steps: scheduling cells for discharge and charge (i.e., changing Gr and CellSt), and advancing the charge state (i.e., changing CellCharge).

The first step is deterministic: it imitates the logic of a selected scheduler. FGURR does not change Gr and rotates through groups, setting ParalReq groups to discharge at a time, and setting the rest to idle. FGWRR does not change Gr either, but instead of rotating the groups it sorts them in non-increasing order of charge (which, for us, is the number of cells with CellCharge(c) = T) and selects the top ParalReq groups. GPWRR tries to assemble groups by packing as many charged cells into each group as possible. Then it selects the top ParalReq most charged groups to discharge. Within each group, all schedulers select SerialReq number of charged cells.

The other step is non-deterministic: every discharging cell non-deterministically becomes discharged, every charging cell non-deterministically becomes charged; idle cells, however, do not change their charges. The program terminates when there is not enough charge to supply the output requirements.

This program is an overapproximation of high-fidelity battery models with precise measurements of the cell charge. This measurement is then use in these models to schedule the cells. Thanks to the non-determinism in the second step, our implementation accounts for possible cell failures (i.e., cell gets immediately discharged) and any high-fidelity model of charge. On the other hand, the program represents cell schedulers’ logic precisely.

6. EVALUATION

In this section we evaluate two aspects of our approach: (i) the effective integration of analyses – detection of integration errors or demonstration of their absence – and (ii) the scalability of our tool for models of practical size.

Analysis Integration. Consider a concrete configuration for the sample aircraft: threads t1, t2, t3 have $[Per]_M = \{t_1 \rightarrow 100, t_2 \rightarrow 150, t_3 \rightarrow 200\}$, $[Dline]_M = \{t_1 \rightarrow 100, t_2 \rightarrow 90, t_3 \rightarrow 200\}$, $[WCET]_M = \{t_1 \rightarrow 10, t_2 \rightarrow 15, t_3 \rightarrow 20\}$ are allocated to a single processor. Before analysis $An_{Freq\_Sc}$ is applied to determine processor frequencies, its assumption $C_{Freq\_Sc}$ is verified. Recall that $C_{Freq\_Sc}$ states that the scheduling policy must be semantically equivalent to DMS. Suppose first that the system uses RMS scheduling, i.e., Prior(t1) > Prior(t2) > Prior(t3). In this case, our tool detects a violation of $C_{Freq\_Sc}$ via model checking because in this case DMS would assign Prior(t2) > Prior(t3). Next suppose that the system uses EDF. As our Spin program indicates, it satisfies $C_{Freq\_Sc}$. Thus, our approach not only prevents incorrect usage of $An_{Freq\_Sc}$, but also extends its applicability to the case of EDF.

Next, suppose our system has a battery with BatRows = BatCols = 4, and a voltage requirement ParalReq =
SerialReq = 3. It has been observed [10] that heat-dissipating cells (i.e., those with many thermal neighbors) and heat-isolated cells (i.e., those with no thermal neighbors) tend to prevent thermal runaway, while cells with one thermal neighbor tend to accumulate heat and lead to runaway. An assignment of weights \( K(0) = K(1) = K(2) = 2, K(1) = -1 \) in (1) captures this intuition. After executing analysis \( \text{AnBatSched} \), which picks a battery scheduler, our tool verifies its guarantee \( \mathcal{G}_{\text{BatSched}} \). Since \( \text{AnBatSched} \) is not aware of thermal runaway, not every scheduler meets the guarantee. As our Spin verification indicates, FGWRR and FGURR satisfy it, but GPWRR fails because it causes the system to reach a configuration that violates (1) with \( \text{TN}(0) = \text{TN}(3) = 0, \text{TN}(1) = 8, \text{TN}(2) = 1 \). Thus, our approach detects possibility of thermal runaway even though the existing analysis \( \text{AnBatSched} \) does not.

**Scalability of Contract Verification.** We evaluate the scalability of our approach by comparing it to an alternative based on a unified semantic model. We focus on model checking since it is by far the most expensive component of our algorithm. The execution semantics of a unified model would, at the very least, consist of the interleaving of the two Kripke structures – \( \mathcal{K}([T_{\text{Sched}}]) \) and \( \mathcal{K}([T_{\text{Term}}]) \). Model checking this interleaving would be intractable due to statespace explosion. On the other hand, our approach is compositional and always verifies \( \mathcal{K}([T_{\text{Sched}}]) \) and \( \mathcal{K}([T_{\text{Term}}]) \) in isolation.

We evaluated our Promela programs using a general-purpose Amazon EC2 virtual machine with 8 cores and 30 Gb memory. The worst-case exploration times by scheduler for the full statespace \( \mathcal{K}([T_{\text{Sched}}]) \) and \( \mathcal{K}([T_{\text{Term}}]) \) are shown in Tab. 3 and Tab. 4 respectively. For the former we use threads with implicit harmonic periods, and for the latter we grow the battery size, fixing the output voltage requirement to \( \text{SerialReq} = \text{ParalReq} = 3 \). Although the complexity growth is exponential, \( \mathcal{K}([T_{\text{Sched}}]) \) is verifiable up to 6-10 threads (per CPU), and \( \mathcal{K}([T_{\text{Term}}]) \) is verifiable up to batteries with 25 cells. We believe that this enables verification of realistic CPSs. We expect that other techniques, such as abstraction and symbolic model-checking, will help us to push these limits even further.

### 7. RELATED WORK

Contracts and assume-guarantee reasoning have been used extensively to enable modular verification. In particular, in the development and verification of CPS, contracts provide an important alternative to a unified semantic model. For instance, Torngren et al. [20] use architectural viewpoints contracts as a coordination tool for designers from different domains when designing a mechatronic system where multiple tools are used for hardware, software, control, and mechanical design.

Sangiovanni-Vincentelli et al. [21] use contracts between components and platform-based design to combine the semantics of multiple domains. A similar approach is used in the SPEEDS project [2] to enable speculative design to support teams of distributed designers. Specifically, the authors propose the use of “rich” components where functional and non-functional aspects of the system are combined. We do not require a model that semantically unifies multiple domains, and our focus is not on the interaction between components. Instead we use contracts to capture the semantics of, and interaction between, the analyses themselves.

Rajhans et al. [22] present an architectural multi-view approach where different modeling notations are capture in different views of an architectural model, using structural and semantic mappings to ensure consistency. In contrast, while we capture similar semantics on the analysis contracts, we only capture the interactions between analyses. Assume-Guarantee reasoning for control theory has been widely explored. Frehse et al. [9] develop assume-guarantee reasoning for hybrid systems based on over-approximation by simulation to enable compositional reasoning. A similar approach is taken by Girard and Pappas [11] using bisimulation, simulation, and language inclusion to develop approximate system relationships. These approaches are focused on the intersection of control theory and computer science. In contrast, our work aims at capturing a larger set of domains with extensible representations of domains.

Cofer et al. [5] present an approach to add architectural contracts to AADL components to enable compositional verification. While we share the AADL platform, we use the AADL annexes to specify contracts on the analysis and within these contracts we specify the components accessed by these analyses. The FUSED [15] project defines a meta-language approach to merge notations from multiple analysis domains to enable a syntactic integration of multiple tools. It is limited to what the syntax can express and unable to reason semantically. For instance, it would not be able to reason about when different scheduling algorithms are equivalent depending on different parameters of the taskset. In our approach we model the semantics in the analyses algorithms and are able to reason about these behavioral differences that are hidden at the syntactic level.

The work closest to ours is by Nam et al. [19]. However, we go beyond them in a number of aspects. Their contracts are restricted to a single domain (resource allocation), the contract verification is unsound and incomplete (since it explores the system statespace only up to a finite depth), and their implementation is tied to a specific tool (Alloy) which cannot do model checking or SMT solving. In contrast, our contract language supports multiple domains, our algorithm is sound and exhaustive, and our implementation relies on

### Table 3: Scalability of the \( \mathcal{K}([T_{\text{Sched}}]) \) program.

<table>
<thead>
<tr>
<th>Threads</th>
<th>DMS/RMS Time(^{10})</th>
<th>EDF Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>4</td>
<td>0.01</td>
<td>0.52</td>
</tr>
<tr>
<td>5</td>
<td>0.07</td>
<td>33.4</td>
</tr>
<tr>
<td>6</td>
<td>0.37</td>
<td>2290.0</td>
</tr>
<tr>
<td>7</td>
<td>2.18</td>
<td>MEMLIM</td>
</tr>
<tr>
<td>8</td>
<td>12.4</td>
<td>MEMLIM</td>
</tr>
<tr>
<td>9</td>
<td>71.2</td>
<td>MEMLIM</td>
</tr>
<tr>
<td>10</td>
<td>421</td>
<td>MEMLIM</td>
</tr>
<tr>
<td>11</td>
<td>MEMLIM</td>
<td>MEMLIM</td>
</tr>
</tbody>
</table>

### Table 4: Scalability of the \( \mathcal{K}([T_{\text{Bat}}]) \) program.

<table>
<thead>
<tr>
<th>Cells</th>
<th>FGURR Time(^{10})</th>
<th>FGWRR Time</th>
<th>GPWRR Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>0.13</td>
<td>0.15</td>
<td>0.15</td>
</tr>
<tr>
<td>12</td>
<td>0.61</td>
<td>2.34</td>
<td>3.94</td>
</tr>
<tr>
<td>16</td>
<td>44.0</td>
<td>31.4</td>
<td>127</td>
</tr>
<tr>
<td>20</td>
<td>10690</td>
<td>619</td>
<td>MEMLIM</td>
</tr>
<tr>
<td>25</td>
<td>MEMLIM</td>
<td>MEMLIM</td>
<td>MEMLIM</td>
</tr>
</tbody>
</table>

\(^{9}\)http://aws.amazon.com/ec2

\(^{10}\)All times are in seconds. MEMLIM indicates that the verification exceeded the limit of 30Gb.
extensible co-operative use of SMT solvers and model checkers.

8. CONCLUSION AND FUTURE WORK

In this paper we presented an analysis integration approach for the development of cyber-physical systems. Our approach uses novel “analysis contracts” to formally specify analyses for the development of cyber-physical systems. Our framework to realistic models. As future work we plan to explore more scalable contract verification tools and define contracts for the contract verification tools themselves.

9. REFERENCES


