

Towards the Coordination and Verification of Heterogeneous Systems with Data and Time

Tim Kräuter 

Adrian Rutle 

Yngve Lamo 

tkra@hvl.no, aru@hvl.no, yla@hvl.no


Western Norway University of Applied Sciences
Bergen, Norway

Harald König 

harald.koenig@fhdw.de

University of Applied Sciences, FHDW
Hanover, Germany

Western Norway University of Applied Sciences
Bergen, Norway

Francisco Durán 

fdm@uma.es

University of Málaga
Málaga, Spain

Abstract—Modern software systems are often realized by coordinating multiple heterogeneous parts, each responsible for specific tasks. These parts must work together seamlessly to satisfy the overall system requirements. To verify such complex systems, we have developed a *non-intrusive* coordination framework capable of performing *formal analysis* of *heterogeneous* parts that *exchange data* and include *real-time* capabilities. The framework utilizes a linguistic extension—which is implemented as a central broker and a domain-specific language—for the integration of heterogeneous languages and coordination of parts. Moreover, abstract rule templates are reified as language adapters for non-intrusive communications with the broker. The framework is implemented using rewriting logic (Maude), and its applicability is demonstrated by verifying certain correctness properties of a heterogeneous road-rail crossing system.

Index Terms—Coordination, Verification, Heterogeneous Systems, Data, Time

I. INTRODUCTION

Software systems are integral to nearly every aspect of modern life. To meet their ever-growing requirements, these systems are often made by coordinating separate parts, which are implemented using the most appropriate tools for each of them. Consequently, modern software systems consist of multiple heterogeneous parts, each responsible for specific tasks that must work together to fulfill the overall system requirements. This rising complexity has made the development of software systems more challenging, while their ubiquitous nature amplifies their need for safety, reliability, and correctness [1].

To verify properties—for example, safety and reliability—of systems consisting of *heterogeneous* parts that *exchange data* and can involve *real-time* capabilities, we have developed a coordination framework designed for *formal analysis*. Here, *heterogeneous* means that each system part may be specified using a different *real-time behavioral* modeling language. We refer to behavioral modeling languages as languages that specify the dynamic aspects of a system, such as statecharts, Petri Nets, and process models. In contrast, structural modeling languages, such as UML class diagrams or entity-relationship models, focus on data representation. Behavioral languages can include *real-time* features, where actions are influenced by the passage of time. This means one can define when an

action can be executed and how long it takes to complete. For instance, an action may occur periodically or after a specific time while in a particular state. In addition, *data exchange* is a unique feature currently missing in other coordination frameworks [2]–[4].

Our coordination framework enables integration while upholding *separation* of the different parts of the system by using a mediator, referred to as *broker*. Embracing separation makes the framework suitable for a wide range of scenarios and facilitates the addition of new modeling languages.

The main idea behind our approach is based on three key ingredients, namely *language integration*, *coordination*, and *verification*, which are depicted in Figure 1 and explained in more detail in section IV:

Language Integration. Integrating a behavioral language into our framework requires implementing a *language adapter*. The adapter mediates between the behavioral language and the common language of the *broker*. Thus, we can use new languages by defining a *behavioral interface* for the given language and then building an adapter that uses it to communicate with the broker. The interface definition remains non-intrusive, leveraging a *linguistic extension* for each modeling language. Each adapter involves aligning the data model of the specific language with the broker’s *canonical data model* by defining data transformation functions.

Coordination. The system model consists of individual models conforming to the previously integrated behavioral languages. These models are then instantiated and coordinated to create a *system configuration*. Since there might be multiple instances of a model, coordination is defined at the instance level. Coordination relies on the *channels* of each instance, i.e., specific entities where data can be read from or written to as identified in the behavioral interface of the corresponding language. In our framework, we provide a domain-specific language (DSL) to define Input/Output (I/O) bindings, i.e., asynchronous data exchange between the channels.

Verification. Once a system configuration is available, global properties of interest, i.e., *system properties*, can be defined and checked. In our framework, the verification takes *real-time features* into account. In this work, we propose using reachability analysis and Linear Temporal Logic (LTL) model

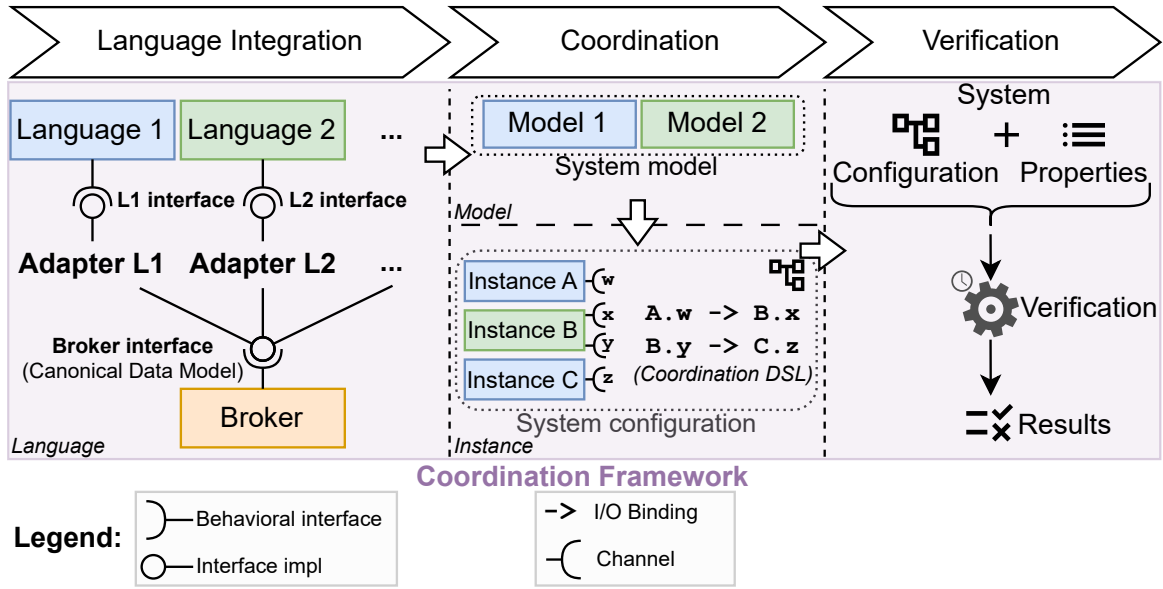


Fig. 1. Overview of the Approach

checking. The result of the analysis is either a confirmation that the property holds or the identification of a counterexample.

The coordination framework provides an architecture built on general concepts like language adapters, I/O bindings, and a canonical data model. To function, this framework must be instantiated with a formalism that can express these concepts and support verification involving data exchange and real-time features. Once instantiated, it allows the analysis of heterogeneous systems by applying the methods of the chosen formalism. As explained in section V, our framework has been developed using rewriting logic and is implemented in Maude [5]. Maude allows us to provide semantics to different modeling languages and to formally check properties using its reachability analysis tool and model checker for real-time systems [6], [7]. Our framework may also be implemented using other formalisms provided that the following requirements are satisfied:

- (1) coping with the (operational) semantics of the modeling languages used to specify the different parts,
- (2) supporting data exchange between the used modeling languages,
- (3) modeling time and its passage affecting the dynamics of the global system, and
- (4) providing analysis capabilities for the global system.

The main contributions are summarized as follows. **(i)** Our coordination framework provides a methodology to define coordination between multiple *heterogeneous* behavioral models in a *non-intrusive* manner, allowing for formal *analysis* of the resulting *global system*. **(ii)** The framework enables *data exchange* between different languages, a capability missing in previous coordination frameworks [2]–[4]. **(iii)** Moreover, the framework supports *real-time functionality* while maintaining

a clear separation between the integrated languages.

The remainder of the paper is structured as follows. First, we provide the necessary background for our contribution in section II. Then, we introduce a use case to motivate our framework in section III. Afterward, we describe the coordination framework in section IV before instantiating it using rewriting logic (Maude) to obtain a concrete implementation, which we apply to the use case in section V. Finally, we conclude in section VI.

II. BACKGROUND

Multiple research fields have investigated the coordination, verification, or simulation of software or even the combination of software and hardware systems. In this section, we provide a brief overview of the three related research areas: *coordination languages*, *architecture description languages*, and *co-simulation*.

Coordination languages can be broadly categorized into two families. The Linda approach enables communication between software programs by providing a global shared memory, commonly called a tuple space, along with operations to read and write to this shared space [8]. The coordination languages of the Linda approach are usually embedded in a general-purpose programming language [9]–[11]. In contrast to *data-driven* coordination in the Linda approach, a family of *control-driven* languages emerged [9] including for example Manifold [12], [13] and REO [14]. These languages define interfaces, i.e., ports for each entity, which can be connected to facilitate communication [15].

The goal of **Architecture Description Languages (ADLs)** is to describe the overall structure of a system by focusing on high-level system components and their connections [16]–[18]. One uses an ADL to define which *components* and *connectors* exist before combining them in a concrete *architectural*

configuration to describe a system's structure [17]. Often, ADLs support verification, such as checking if an architectural configuration is free of deadlocks and starvation, by employing process algebras such as CCS, CSP, and π -calculus [19].

Co-Simulation approaches facilitate the information exchange between multiple simulations running concurrently, ensuring temporal relationships. A simulation is based on a simulation unit with black-box behavior but a predefined simulation interface of inputs and outputs. Typically, an *orchestrator* uses these interfaces to transfer data between simulations and dictate the passage of simulated time [20]. Co-simulation approaches are classified into *Discrete Event* (DE), *Continuous Time* (CT), or *Hybrid* when they combine both DE and CT elements. At present, the two primary standards for co-simulation are the *Functional Mock-up Interface* (FMI) [21] and the *High Level Architecture* (HLA) [22].

The methodology in our approach outlines a **coordination framework**. The unique characteristic of coordination frameworks is that they embrace *model heterogeneity* by operating on the language level [4], i.e., not only providing one formalism or modeling language that must be used exclusively, such as coordination languages and ADLs. ADLs typically verify only predefined properties and lack support for custom states and temporal logic formulas. We do not consider co-simulation approaches as coordination frameworks since they compose executable programs (simulation units) that embrace heterogeneity at the execution level, not the model level. Coordination frameworks described in the literature include Ptolemy [23], BCOoL [3], [4], and [2].

However, because Ptolemy is focused on execution, it relies on a general-purpose programming language, which limits the ability to verify the coordinated system formally. The other coordination frameworks are built on sound formalisms. Still, they lack support for data exchange during coordination, which is essential and a natural form of communication in modern software systems. Both approaches identify data exchange as a key focus for future work [2]–[4]. Our coordination framework enables formal analysis of heterogeneous systems, incorporating *data exchange* and *real-time capabilities* while remaining *non-intrusive* and upholding separation.

Our contribution focuses on software systems that can include real-time characteristics. We exclude CT or hybrid systems, typically involving hardware components modeled by differential equations. By applying the principles of Real-Time Maude, we can model continuous-time software systems that can be “discretized” using time-sampling strategies available in Maude [7].

III. USE CASE

In this section, we present a use case to illustrate the motivation behind our coordination framework. We begin by introducing the use case, followed by explaining its specification. Finally, we discuss several properties that must be verified for the specification.

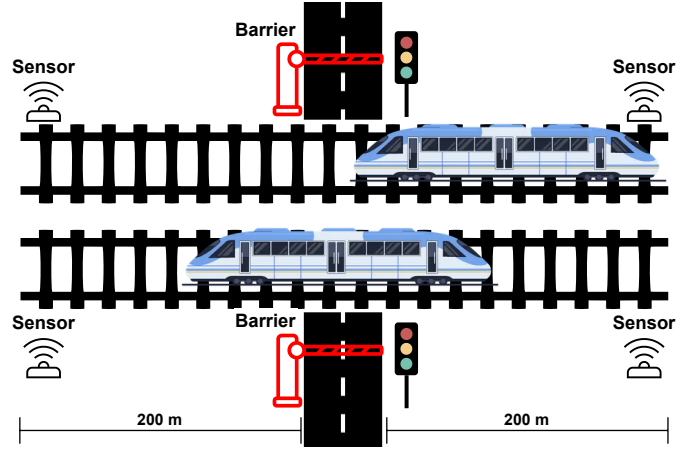


Fig. 2. Use case: Active Level Crossing (two train tracks)

A. Description

The use case is a traffic management system for a *level crossing* (also called road-rail crossing). Level crossings account for over 400 accidents in the European Union every year [24]. The challenge with level crossings is that trains have a much larger mass relative to their braking capability and, thus, a far longer braking distance than road vehicles. As a result, trains typically do not stop at a level crossing and depend on vehicles and pedestrians to clear the tracks beforehand. *Passive* level crossings are only equipped with a traffic sign and are associated with a higher number of accidents compared to *active* crossings [24].

This use case aims to design an *active* level crossing system that warns cars about incoming trains using traffic lights and barriers. Figure 2 provides an overview of the scenario with two train tracks. The case study was kept as simple as possible (trains do not communicate with the system) to illustrate the key concepts of our approach. In this case, the primary objective is to ensure that the proposed specification enables cars and trains to *safely pass* through the crossing.

B. Specification

The case study is realized by coordinating three system parts specified using two different modeling languages, namely Colored Petri Nets (CPN) [25] and statecharts. This corresponds to the model level in the coordination step in Figure 1. We will explain the system parts as sketched in the diagram in Figure 3. By default, all distances will be expressed in meters, time in seconds, and speed in meters per second.

a) *The sensor system*: shown in Figure 2 detects the speed of incoming and outgoing trains. In general, trains can arrive in any order and at different speeds, and there may be level crossings with either one or multiple tracks. To model train behavior flexibly, the model was developed using CPN as shown in Figure 4. It consists of two parts: a train simulation (blue) and the sensor system (green).

In a CPN, places are represented with ellipses and transitions with rectangles. Each token carries a data value that

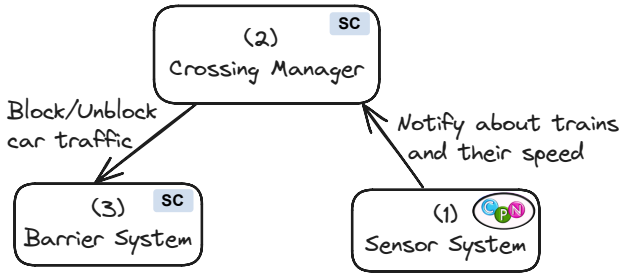


Fig. 3. System parts in the use case

belongs to a given type, indicated at the bottom right of a place (TIMED_REAL means real value and a timestamp). In the state in Figure 4, the place *New train can approach* (upper left corner) has two tokens with values 25 and 40 (train speed). Transitions can have a time inscription displayed at the top right, increasing the timestamp of produced tokens. For example, when a token moves from *New train waiting to approach* to *New train can approach*, its timestamp increases by 10. The arc labels are expressions that reference the values of tokens as they traverse the arcs. In the given use case, they ensure that the measured speed is transmitted correctly. Finally, the places with double lines (the two on the right side of the figure) are *port places*, representing the interface through which the model communicates with its surroundings. The blue tag indicates the place's type; in this case, both are output ports.

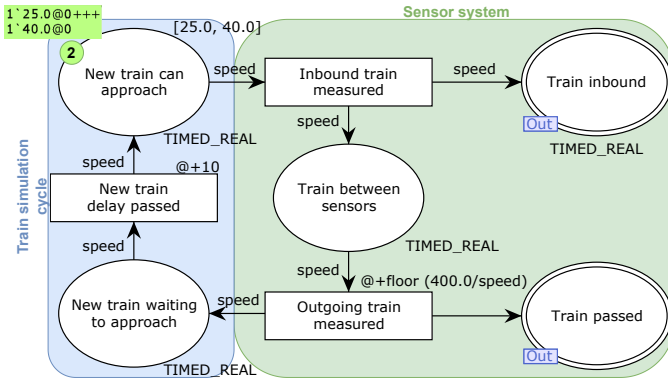


Fig. 4. Train simulation & Sensor system (CPN)

The number of initial tokens in the CPN model determines the number of tracks being modeled, assuming that there is only one train at a constant speed on each track at any given time (25 m/s and 40 m/s in Figure 4). The two main transitions are *Inbound train measured* and *Outgoing train measured*, which refer to the sensors detecting a train as it enters or leaves the 400-meter corridor. Sensors are assumed to be placed on the tracks 200 meters on each side of the barriers. These transitions produce tokens in *Train inbound* and *Train passed*, which are the above-mentioned interfaces. After a short cooldown period (see *New train delay passed*), new trains can start approaching the crossing, resulting in an endless cycle of trains passing over time; see

the blue train simulation part on the left of Figure 4. Adjusting either the number of tokens or the train simulation within the CPN model can change the simulated behavior.

b) *The crossing manager*: monitors the information from the sensors to detect whether any trains are within the 400-meter zone. Based on this, it manages car traffic by sending signals to the barrier system. The crossing manager is specified as a statechart in Figure 5. Transitions are defined as usual using three optional components in the following format: *trigger [guard] / effect*. Here, the *trigger* can be either time-based or event-driven, the *guard* is a boolean expression, and the *effect* consists of a series of statements (separated by semicolons) that raise an event or modify the statechart's variables.

The system starts in the state *No Trains* and transitions to the state *Trains inbound* when a *trainInbound* event is received. It also tracks the number of trains in the corridor using the *trains* counter. Additionally, it calculates how many seconds it will take for the trains to reach the level crossing, factoring in a safety margin: $closeIn = 200 / trainSpeed - safetyBuffer$.

In the *Trains inbound* state, the *closeIn* variable decreases every second until it reaches 0. At that point, the system transitions to the *Trains are passing* state, triggering the *blockCarTraffic* event. However, additional trains may arrive while still in the *Trains inbound* state and could reach the level crossing before the previous train. In such cases, the *closeIn* variable must be updated accordingly.

In the *Trains are passing* state, the *trains* variable is either decreased when trains pass or increased when trains approach. When the variable reaches 0, the *unblockCarTraffic* event is triggered, and the system transitions to the *No Trains* state, allowing the process to restart. The events *blockCarTraffic* and *unblockCarTraffic* represent the data flowing from the crossing manager to the barrier system in Figure 3.

c) *The barrier system*: manages car traffic by controlling the barriers and corresponding traffic lights. The system is specified as a statechart in Figure 6. It depends on two *external* events, *openBarrier* and *closeBarrier* (incoming data in Figure 3), which trigger an intermediate state lasting two seconds, representing the time required for the barrier to move.

All three systems—the sensor system, barrier system, and crossing manager—must work together to ensure safe and efficient traffic management at the level crossing. This is more complex than it appears in Figure 3, as CPN models typically do not interact natively with statecharts. Moreover, even the event names in the statecharts do not align, such as *blockCarTraffic* and *closeBarrier*. To address this challenge, the modeling languages must be integrated and proper coordination must be established, as illustrated in Figure 1. In the next section, we describe the intended verification to ensure correct coordination.

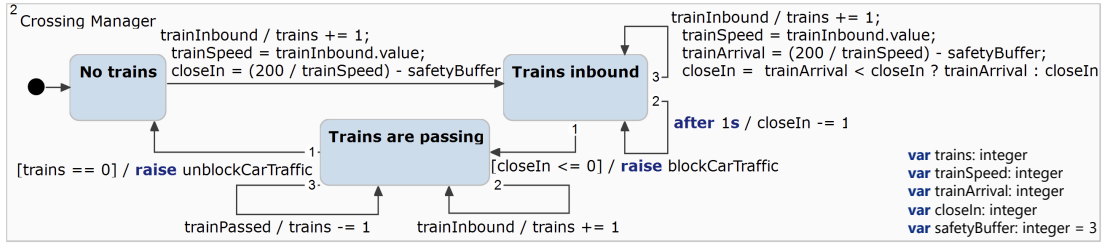


Fig. 5. Crossing Manager (statechart)

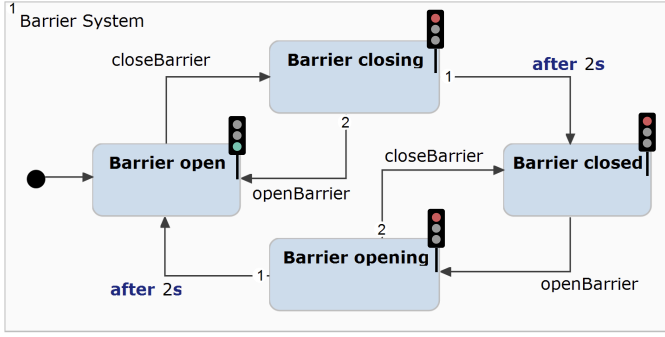


Fig. 6. Barrier System (statechart)

C. Verification

We aim to analyze the proposed specification from the previous section to identify potential issues early on. To ensure the system behaves as intended, we focus on verifying *two key properties*. These properties are expressed using Linear Temporal Logic (LTL), employing state-based model checking as our primary verification method. Nonetheless, in general, other analysis approaches may also be worth exploring.

First, we must ensure that the system does not create unsafe situations, such as allowing trains to pass while the barriers remain open. This safety property can be expressed in LTL with Property (1), which expresses that a train never passes when the barriers are open.

$$\square \neg (\text{Barriers-open} \wedge \text{Train-passing}) \quad (1)$$

Second, we must ensure that when the barrier closes, it will eventually reopen so that car traffic is not indefinitely halted and Property (1) is trivially upheld. This requirement is captured by Property (2), which represents a specific case of the *response* pattern [26]. This pattern dictates that once the system enters the first state (*Barriers-closed*), it must eventually transition to the second state (*Barriers-open*).

$$\square (\text{Barriers-closed} \rightarrow \Diamond \text{Barriers-open}) \quad (2)$$

Verifying these system properties is challenging for several reasons, and as a result, none of the approaches, even coordination frameworks discussed in section II, currently support this. First, the system consists of three parts which are designed using *heterogeneous modeling languages* (statecharts and CPN in our case study). Second, *data is exchanged* between these

parts (train speed in our example), which affects how the system behaves (waiting times). Third, the system's behavior is influenced by *global time*, which needs to remain consistent across the different modeling languages. Finally, we do *not* want to be *intrusive*, meaning imposing model changes or requiring a specific modeling language.

IV. COORDINATION FRAMEWORK

The driving design goals for our coordination framework are *non-intrusiveness* and upholding the *separation* of participating models and instances. Furthermore, we want the integration of additional languages to require minimal effort, for which separation across multiple key aspects is needed. Separation, or loose coupling, is essential in software architecture because it simplifies making changes to the system by minimizing interdependencies [27], [28].

We focus on the separation of the following key aspects: *languages*, *models*, *time*, and *data*. Firstly, each system part should be flexible in choosing the most suitable modeling language, provided the underlying formalism can support the language. Secondly, every part of the system, i.e., each model, must be able to evolve independently. Thirdly, each model should be able to use its native real-time features while time progresses uniformly during execution for all model instances, never skipping real-time events. Finally, each model should be able to use its own data model yet still be able to exchange data with other system parts. In the following sections, we detail our approach by explaining the key aspects highlighted in Figure 1 and explain how it meets the design goals of non-intrusiveness and separation.

Language integration, coordination, and verification are distinct tasks, each typically handled by different roles. For instance, a language engineer is responsible for language integration, a system architect manages coordination, and the quality assurance team oversees the verification process.

A. Language Integration

To facilitate coordination while upholding separation, we introduce a central *broker*, which acts as a mediator. We define the metamodel for the broker on the left in Figure 7. As shown in its metamodel, the broker is just a collection of bindings, which, as we will see below, are handled independently, without interactions between them. To integrate heterogeneous languages, we use a *linguistic extension* [29], [30]. The purple part of the broker metamodel defines the linguistic

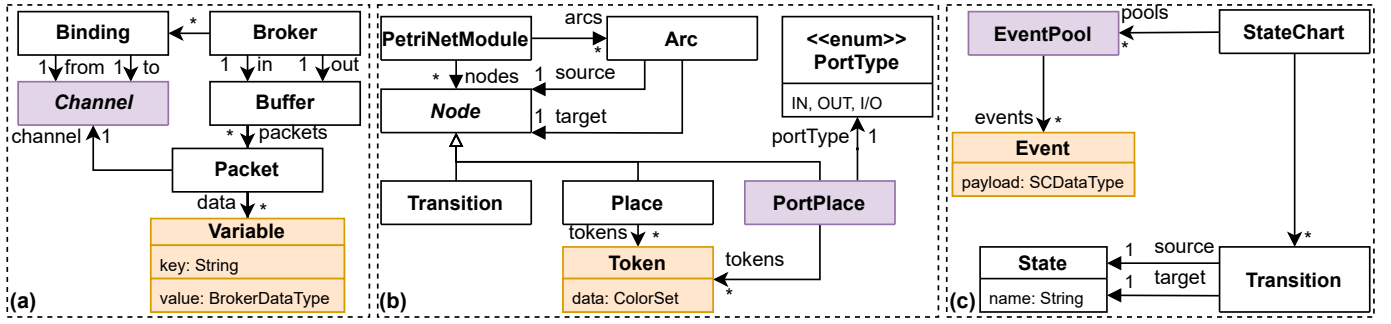


Fig. 7. Broker Metamodel (a) and CPN/Statechart Metamodel excerpts (b)/(c)

extension, which is used to augment behavioral languages non-intrusively. It introduces the concept of a **Channel**, which refers to any location where data can either be read from or written to. Linguistic extension is a widely used technique in the multi-level modeling domain, where new concepts can be added a posteriori to existing metamodels at any level of a metamodeling hierarchy. In our case, we use the broker metamodel to define the concept (**Channel**), which can be used in the participating metamodels. The channels are used to identify the behavioral interface for the participating languages, e.g., **PortPlace** for CPNs and **EventPool** for statecharts are both typed by **Channel** (see the purple colored elements in Figure 7).

The broker metamodel also introduces **Packet** containing data in a *canonical data model* [27] to enable data exchange among coordinated models while upholding separation. The *canonical data model* serves as a common intermediate to enable conversion between the varying data models of the used languages. Data-related concepts are shown in orange in Figure 7. A packet is contained in an input or output **Buffer**, which holds the packet until it is transmitted to the recipient. A **Packet** contains data, i.e., **Variables**, which are key-value pairs and references the **Channel** from which it was ingested or to which it is about to be delivered.

The broker has a set of bindings that connect **Channels**. As mentioned earlier, a **Channel** is a connection point in a given language that the broker can use to read or write. If a binding is defined between two channels, the broker will facilitate coordination, i.e., data exchange. The broker must know how to interface with each behavioral language to adapt between the heterogeneous models while maintaining language separation. By augmenting a specific element in a metamodel with the concept of **Channel**, made possible by the linguistic extension, one can define the behavioral interface for that metamodel [4].

Language integration (see Figure 1) can be further subdivided into two steps. First, one must identify the behavioral interface for the new language, i.e., define which parts of the metamodel are exposed by extending **Channel**. As a result, we obtain an *augmented* metamodel, such as the metamodel for CPNs in Figure 7 (b), where **PortPlace** is identified as a **Channel** (purple coloring). Since port places constitute the *interface* through which a CPN exchanges tokens with its environments, we utilize port places as the behavioral

interface for our framework. More broadly, one can examine how different model instances within a language interact to determine its behavioral interface. For example, in the case of statecharts, instances communicate using events dispatched through *event pools* [31]. Therefore, event pools serve as the behavioral interface for statecharts, i.e., an **EventPool** is a **Channel**, as highlighted by the purple color in the statechart metamodel in Figure 7 (c).

Second, one utilizes the augmented metamodel to create a *language adapter*, inspired by the adapter [32] or channel adapter [27] patterns. This language adapter facilitates the integration of heterogeneous languages by mediating between the specific language and the broker.

A key part of each language adapter is the translation between different data representations used by different languages. To enable seamless data exchange, the broker employs a *canonical data model* as a standardized format. Each adapter is responsible for implementing two functions that handle the data translation process: (i) The function *toBroker* translates data from the specific data model to the broker's canonical data model, and (ii) the function *fromBroker* translates data from the broker's canonical data model back to the specific data model. These two functions should be inverse functions of one another. Using a *canonical data model* addresses the problem where normally the number of translators needed to enable communication between each pair of participants increases quadratically with the number of participants [27]. The canonical data model, i.e., packets consisting of key-value variable pairs, is kept abstract but sufficient to showcase the framework's data exchange capabilities.

In addition to *syntactic mapping* between different data models, as discussed so far, schema matching, i.e., *semantic mapping* [33], is also vital to enable system interoperability. Semantic mapping is needed since systems can represent the same information structurally differently. One system might use different field names or even split information into two fields compared to another system. Semantic mapping allows reconciling these differences when data is transferred between the systems. In our coordination framework, semantic mapping can be included in the translation functions and customized for each binding or even generated from relations between the data models, often described graphically in data integration tools. However, we do not investigate this further in this paper.

Language adapters can be defined as follows. A language

adapter reads from the channels of model instances to create an intermediate packet, provided that a suitable binding source is defined (**ingest**). Additionally, for binding targets, an adapter writes to the channels and removes the previously created packets (**deliver**). These two actions can be described by rule templates [34], [35], using a Henshin-like notation [36], as shown in Figure 8, which can then be specialized for different languages to build a concrete language adapter. The rules can be interpreted as follows: the black elements represent objects that will remain unchanged during the transformation. The red elements will be deleted during the transformation process, while the green elements will be added. The dotted elements need to be filled in for a specific language adapter.

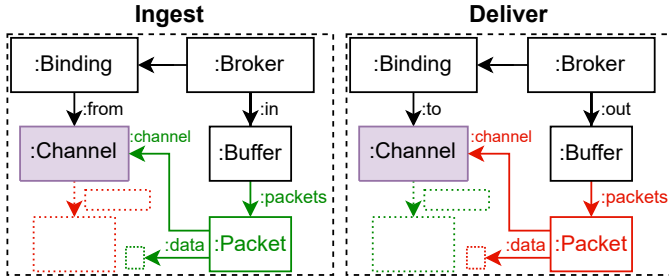


Fig. 8. Language Adapter Rule Templates **Ingest** and **Deliver**

For instance, Figure 9 shows adapter rules for CPN and statecharts, as well as the generic move rule for the broker. The **ingest** rule for CPN is displayed on the left, and the **deliver** rule for statecharts is displayed on the right. Both **ingest** and **deliver** rules require converting between different data models, for which we employ the previously defined translation functions. Specifically, the functions $toBroker_{cpn}$ and $fromBroker_{sc}$ are used for translation. Consequently, an event generated from a CPN token containing data x will have the payload $fromBroker_{sc}(toBroker_{cpn}(x))$.

The **move** rule, depicted in the middle, demonstrates how the broker transfers packets from its input buffer to its output buffer, effectively isolating the language adapters. Following the rules from left to right shows how a token is converted into an event, including associated data.

In summary, introducing a broker as a mediator achieves the *separation* of languages, models, and data. Due to the concept of language adapters and the canonical data model, we keep languages, models, and data as separated as possible. Additionally, identifying a behavioral interface for each language through a *linguistic extension* ensures *non-intrusiveness*, as models do not have to be changed for coordination. Notably, incorporating a new language into the framework involves a **one-time integration effort**. We will now detail how time separation is achieved, and we guarantee consistent passage of time across heterogeneous formalisms.

Time. Many modeling languages include the real-time functionality to specify, for example, that actions take a certain amount of time, are periodic, or can only happen after a specific amount of time. Each language will provide its own real-time elements, and the behavioral semantics of these elements

will be given as part of the semantics of the corresponding languages. For example, time inscriptions for CPNs [25] and real-time triggers in statecharts are employed in the use case. However, to guarantee consistent time treatment, individual model instances that are part of the coordinated system cannot perform timed actions as they please since all actions must be consistent with time elapse.

Individual model instances cannot progress time independently. There must be a model of time that is followed by all language definitions participating in the framework. As we will discuss in section V, our framework has been implemented using rewriting logic (concretely the Maude system). Therefore, we expect that the real-time features of the different language definitions adhere to the principles of Real-Time Maude [7]. We assume a *global clock*, which will advance and then synchronize with the clocks of the individual instances. The global clock is only changed by the *tick* rule, meaning all other rules can be seen as *instantaneous*. For instance, to model some duration, we will have a start action and an end action, both instantaneous. All time-related actions will have a timer or a scheduled time that will be used to fire them. Instead of keeping a centralized scheduled-time sorted list of actions, we will assume functions calculating the time to the first action, or the maximum amount of time that may elapse without an action happening (*mte*), and another one applying the pass of time (*delta*). Given these functions, the passage of time can then be modeled by a unique tick rule that calculates the maximum time elapse without an executable action (*mte*) and applies the *delta* function to the entire system. Under these assumptions, the control of time can be easily split between the different parts of the system. The *mte* function will be defined as the minimum of its results for each part of the system. Then, the *delta* function on the global system will simply consist of applying it to each of its parts. The definitions of the *mte* and *delta* functions for each modeling language will be part of the definition of each language adapter. Time-related actions will then be fired when a timer reaches time zero or a clock matches a local or global clock. As already said, this approach to real-time is based on Real-Time Maude [7], which is similar to the models used for DE-based co-simulation methods [20], where an orchestrator controls global time.

B. Coordination

The second step in our approach (see Figure 1) is the *coordination* of the system parts (models). This step can be further subdivided into the following three steps. First, the *system model* is created, which consists of individual models conforming to the previously integrated behavioral modeling languages.

Second, one instantiates the system model by instantiating its respective individual models. In the use case, each model (the barrier system, sensor system, and crossing manager) has only one instance, although multiple instances of the same model are possible.

The third step is based upon the augmented metamodel obtained from the language integration step (see Figure 1).

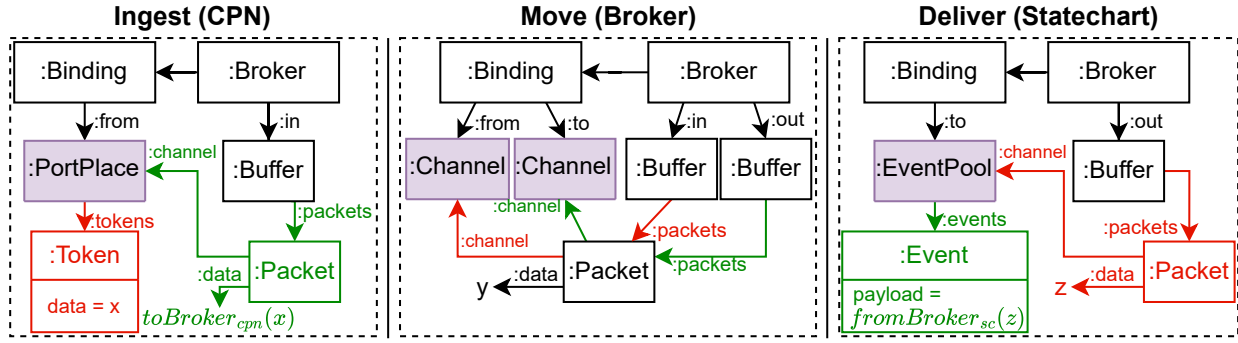


Fig. 9. Broker and Language Adapter Rules

```
Sensor.Train_inbound  -> Crossing.trainInbound,
Sensor.Train_passed   -> Crossing.trainPassed,
Crossing.unblockCarTraffic -> Barrier.openBarrier,
Crossing.blockCarTraffic  -> Barrier.closeBarrier
```

Listing 1. Bindings for the use case

The linguistic extension defines each language’s behavioral interface, specifying which channels can be linked via bindings. We utilize a textual DSL to connect channels from different modeling languages uniformly. For example, for the use case, we define the bindings as shown in Listing 1. Each line defines one binding, following the structure *bindingSource* \rightarrow *bindingTarget* in our DSL. Finally, the model instances, along with their corresponding bindings, constitute the *system configuration*, which is utilized for verification.

C. Verification

Verification in our approach (see (iii) in Figure 1) is further subdivided into specification and verification of system properties.

First, one specifies the *system properties* that must be verified based on the *system configuration*. To specify the properties of the system’s global state, it is necessary to first define the *state structure* for each participating modeling language, as explained, for example, in [2], [37]. The state structure, which is also needed for execution, leads to atomic propositions for each language that can be combined to express temporal logic properties for the global system, e.g., the above formulas (1) and (2). The global state is a tuple of the local states of each model based on the system configuration. For example, the initial state in the use case is a triple consisting of the statechart start states and the two tokens in the place *Train* prepared to approach.

Second, we use the system properties and the system configuration from the previous steps to perform *automatic verification*, for example, LTL model checking [1], where the states are the tuples mentioned in the previous step. This generates verification results, including counterexamples, if any properties are unsatisfied.

V. IMPLEMENTING & VERIFYING THE USE CASE

We implemented the framework using rewriting logic and its implementation in Maude [5] as the foundational formalism. The full implementation in [38] includes the use case in addition to definitions of Labeled Transition Systems (LTS) [1] and Business Process Model and Notation (BPMN) [39]—in these cases without time or data—as well as several examples using different combinations of the available languages. Maude meets the formalism requirements outlined in the introduction: it can handle a wide variety of operational semantics (1) [40], [41], supports the modeling of data and data exchange (2) [5], enables time modeling through Real-Time Maude [7] (3), and offers built-in verification capabilities (4). Verification in Maude includes techniques such as reachability analysis, explicit-state LTL model checking [6], and time-bounded LTL model checking [7]. We now present key implementation details from each step of our approach (see Figure 1), using the use case as a practical example.

In Maude, object-oriented systems may be specified using the usual elements in object-oriented languages, which allows us to specify the models in Figure 7. For instance, there is a class *Broker* with *in* and *out* attributes of type *Packets*, representing buffers of packets, and an attribute *bindings* of channel bindings.

```
class Broker | in : Packets,
               out : Packets,
               bindings : Set{Binding} .
```

A. Language Integration

Each formalism integrated into the framework will have its own representation. For example, following the descriptions in Figure 7, CPNs will be represented by classes *CPN* and *CPNInstance*. An object of class *CPN* has a set of places, a set of transitions, and a set of arcs. In some CPN objects, a subset of the places will be port places. An object of *CPNInstance* is associated with its CPN model (*cpn*) and has a marking (multiset of tokens).

```
class CPN | places : Set{CPNPlace},
            transitions : Set{CPNTransition},
            arcs : Set{CPNArc} .
class CPNInstance | cpn : Oid,
                    marking : CPNTokens .
```


Given appropriate class declarations, objects are then represented with syntax $\langle O : C \mid \text{Atts} \rangle$, with O an object identifier, C a class identifier, and Atts a comma-separated set of attribute-value pairs with the form $a : v$, with a the attribute's name and v its value.

The behavior of these objects is then specified by rewriting rules. For the language integration, the specification includes rules **ingest** and **deliver** similar to those in Figure 9. For example, the language adapter rule **ingest** for CPNs is implemented as shown in Listing 2. Objects of classes `CPNId` of class `CPN`, `IId` of class `CPNInstance`, and `Br` of class `Broker` are involved in the rules. In it, we can see how the `CPNInstance` object `IId` corresponds to the `CPN` object `CPNId` (`cpn` attribute). We can also see how, if there is a token in the place `PlaceId` in the marking of the `CPN` instance object, with a binding for `PlaceId`, the token is removed from the `CPN` instance and added in the `in` buffer of the broker object. Notably, the data transformation to the canonical data model occurs in the operation `cpnToBroker` (lines 11 and 17) and is not fully shown in Listing 2. Furthermore, the rule presented in Listing 2 is a simplified version and does not account for the token's availability at the current global time.

```

1  omod CPN-ADAPTER is
2    inc BROKER .
3    inc CPN-SEM .
4    op cpnToBroker : CPNData -> VariableSet .
5    ...
6    rl [token_to_packet] :
7      < CPNId : CPN |
8        places :
9          (place(PlaceId, InArcs, OutArcs, Type),
10             Places) >
11      < IId : CPNInstance | cpn : CPNId,
12        marking : (token(PlaceId, Data, 0), Marking) >
13      < Br : Broker | in : Packets,
14        bindings : (PlaceId -> ChannelId, Bindings) >
15  => < CPNId : CPN | >
16      < IId : CPNInstance | marking : Marking >
17      < Br : Broker |
18        in : (packet(PlaceId, cpnToBroker(Data)),
19             Packets) > .
20  endom

```

Listing 2. CPN Language Adapter Rule **Ingest** in Maude [38]

A similar Maude rule implements the **deliver** rule, specified in Figure 9. It is important to highlight that each adapter is implemented in its own Maude module, demonstrating how the separation of the languages is reflected at the code level.

To apply our implementation to the use case, we developed a language adapter for both CPNs and statecharts in [38]. These language adapters are built on our broker metamodel (see Figure 7 (a)), and the identification of behavioral interfaces within the CPN and statechart metamodels (see Figure 7 (b)/(c)). Implementing language adapters involves converting the data models of CPN and statecharts into the broker's canonical data model. Additionally, language integration ensures that the semantics of both CPN and statecharts are aligned with the

externally provided global clock.

Global Time Elapse. As already discussed in section IV, the model of time is provided by Real-Time Maude [7]. In summary, time passing is realized by a single *tick rule*, which models the time elapse of the global clock based on the *mte* (maximum time elapse) function, and the *delta* function, which applies the time pass to each model instance. The key element in this model of time and the approach followed is that, as already said, the tick rule is the only rule that models the passage of time. All other rules in the specification are instantaneous, meaning they can use time values but not advance time. This approach allows us to keep as many clocks and timers as necessary but with one single global clock that is used to synchronize the others. Moreover, the specification of the different formalisms gets simplified because all we have to do, regarding time, is to provide the appropriate equations defining the behavior of the *mte* and *delta* functions on its instances and time-related features.

B. Coordination

The coordination is straightforward in Maude. We define models and their instances separately, as illustrated in Listing 2, where an instance links back to its model (`cpn` attribute). We define each model from the use case, instantiate it once, and add bindings to obtain the system configuration. To add bindings, we use the broker metamodel from the language integration, which implements the bindings DSL we introduced earlier (see Listing 1).

The Maude rules corresponding to the rules in Figure 9 handle the coordination. The adapter definition identifies the elements used in the specific language for communication and how to handle them. In the case of the CPN, we have seen how the **ingest** rule is in charge of taking a token from a port place (a place for which there is a binding), and placing it into the input buffer of the broker. The **move** rule then moves packets from the input buffer to the output buffer. Finally, the adapter of the formalism on which the target part is specified will handle such a packet. That is, it will take the packet and transform it into the communication element of the specified channel. For example, in our example, the target is specified as a statechart. Thus, the statechart adapter deletes the packet and creates an event in the target channel of the statechart.

C. Verification

In the case of Maude, we can perform verification using different tools, including reachability analysis, model checking and statistical model checking. Given that the system has an infinite state space, we need to use time-bounded LTL model checking [7] to verify its behavior. Although we could also check timed CTL properties, we chose time-bounded LTL for its simplicity and easier understanding. To specify LTL properties, we first must define the necessary atomic propositions. For example, consider the property (1) specifying that a train never passes the crossing while the barriers are open. To specify this property, we can define the propositions `Train-passing` and `Barriers-open`. As shown

in Listing 3, given a satisfaction predefined operator `_|= _`, we define a proposition by specifying when a state satisfies that proposition. For example, the `Train-passing` proposition is satisfied if there is a token in the "Train passed" place of the CPN instance object (lines 5-7). Similarly, the `Barriers-open` proposition is satisfied if the statechart is in the state "Barrier open" (lines 11-13).

```

1 mod PREDICATES is
2   inc BROKER-EX .
3   pr SATISFACTION .
4   --- Sensor system propositions
5   op Train-passing : -> Prop .
6   ceq { < Id : CPNInstance |
7       marking :
8         (token("Train passed", data(Int), T)) >
9         C, GT } |= Train-passing = true
10  if GT ge T .
11  --- Barrier system propositions
12  op Barriers-open : -> Prop .
13  eq { < Id : SCInstance |
14      state : scToken("Barrier open", T) >
15      C, GT } |= Barriers-open = true .
16  --- Otherwise, propositions are false
17  var S : System .
18  var P : Prop .
19  eq S |= P = false [owise] .
20 endm

```

Listing 3. Atomic Propositions in Maude [38]

Given the propositions in Listing 3, we can then verify the desired Property (1) with the following command.

```

red modelCheck(system,
    []~(Barriers-open /\ Train-passing)) .
result Bool: true

```

Property (2) can be encoded similarly in Maude by defining the missing proposition `Barriers-closed` accordingly. Both properties are fulfilled.

To use the model checker, in addition to the executability of the specification (i.e., the equational part of the specification must be terminating and Church-Rosser, and equations and rules must be coherent), the reachable state space must be finite. In this case, the search space is finite only if we limit the global time. The upper time bound for the verification is defined in the Maude rule that advances the global time in the system; it is not part of the property specification.

Atomic propositions can be defined in different Maude modules and then later combined into a system property as shown Listing 3. By instantiating single models, adjusting bindings, or stubbing models, one can verify not only system properties but also properties for each individual model or a certain subset of the system model.

If a property is not fulfilled, the Maude model checker provides a counterexample, i.e., a sequence of states (set of objects) connected by transitions (rewriting steps). These steps in the sequence reflect steps in terms of the operational semantics of the corresponding formalisms. Our formal implementation

strives to minimize the representation distance, ensuring near-zero cost when translating between a formalism's semantics and its Maude encoding. Thus, going from a sequence of states back into a trace in the corresponding formalism is straightforward. In the future, we plan to trace problems found by the model checker to the individual models used in our approach or the specified coordination, which might be faulty.

VI. CONCLUSION & FUTURE WORK

We introduced a *non-intrusive* coordination framework that can coordinate system parts described in *heterogeneous* behavioral modeling languages into a *global system* and allows for formal analysis of the system's properties. The framework uses language adapters and a broker to integrate the heterogeneous languages, allowing for *data exchange* and *real-time capabilities* while upholding the *separation* of the languages and models. Furthermore, we implemented our framework using rewriting logic in Maude and used it to verify the correctness of an active level crossing system modeled with Colored Petri Nets and statecharts. Additionally, the framework provides a general methodology for coordination, making it independent of any particular formalism for implementation; that is, the coordination DSL will ultimately hide the details of the underlying implementations. It can be applied to software systems with real-time capabilities, i.e., continuous time that can be approximated or discretized by time-sampling in Maude.

As future research directions, we plan to improve our approach to address the following observations. The coordination DSL supports only binding instance channels; with user-friendliness in mind, it should also include syntax and constructs to support the specification of properties which the system configuration should satisfy—while hiding the underlying implementation. Currently, our implementation in Maude is only applied to one specific use case, and further enhancements are needed to support all possible CPN and statechart features. Nevertheless, it effectively demonstrates the overall architecture proposed in our approach and the proposed patterns for integrating various behavioral languages into our framework. Following the same architecture, we investigated additional behavioral languages (BPMN, LTS) and synchronous communication besides asynchronous communication (see [38]). Furthermore, the broker must not be a single, centralized component as it is currently presented, since multiple message brokers exist in a realistic distributed system. In addition, we want to make bindings multi-ary to model advanced communication patterns directly, such as broadcasting and publish/subscribe. Currently, such patterns must be implemented in a dedicated model that duplicates messages together with multiple corresponding bindings. Finally, we aim to validate our approach in a real scenario, not only the presented use case.

REFERENCES

- [1] E. M. Clarke, T. A. Henzinger, H. Veith, and R. Bloem, Eds., *Handbook of Model Checking*. Cham: Springer International Publishing, 2018.

- [2] T. Kräuter, H. König, A. Rutle, Y. Lamo, and P. Stünkel, "Behavioral consistency in multi-modeling," *The Journal of Object Technology*, vol. 22, no. 2, p. 2:1, 2023.
- [3] M. Vara Larsen, "BCOol : The behavioral coordination operator language," Ph.D. dissertation, Université Nice Sophia Antipolis, Apr. 2016.
- [4] M. E. Vara Larsen, J. Deantoni, B. Combemale, and F. Mallet, "A Behavioral Coordination Operator Language (BCOoL)," in *2015 ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MODELS)*. Ottawa, ON, Canada: IEEE, Sep. 2015, pp. 186–195.
- [5] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. Talcott, *All About Maude - A High-Performance Logical Framework*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, vol. 4350.
- [6] S. Eker, J. Meseguer, and A. Sridharanarayanan, "The Maude LTL Model Checker," *Electronic Notes in Theoretical Computer Science*, vol. 71, pp. 162–187, Apr. 2004.
- [7] P. C. Ölveczky, "Real-Time Maude and Its Applications," in *Rewriting Logic and Its Applications*, S. Escobar, Ed. Cham: Springer International Publishing, 2014, vol. 8663, pp. 42–79.
- [8] N. Carriero and D. Gelernter, "Linda in context," *Communications of The Acm*, vol. 32, no. 4, pp. 444–458, Apr. 1989.
- [9] G. Ciatto, S. Mariani, M. Louvel, A. Omicini, and F. Zambonelli, "Twenty Years of Coordination Technologies: State-of-the-Art and Perspectives," in *Coordination Models and Languages*, G. Di Marzo Seruendo and M. Loreti, Eds. Cham: Springer International Publishing, 2018, vol. 10852, pp. 51–80.
- [10] L. J. B. Nixon, E. Simperl, R. Krummenacher, and F. Martín-Recuerda, "Tuplespace-based computing for the Semantic Web: A survey of the state-of-the-art," *The Knowledge Engineering Review*, vol. 23, no. 2, pp. 181–212, Jun. 2008.
- [11] D. Rossi, G. Cabri, and E. Denti, "Tuple-based Technologies for Coordination," in *Coordination of Internet Agents*, A. Omicini, F. Zambonelli, M. Klusch, and R. Tolksdorf, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 83–109.
- [12] F. Arbab, I. Herman, and P. Spilling, "An overview of manifold and its implementation," *Concurrency: Practice and Experience*, vol. 5, no. 1, pp. 23–70, Feb. 1993.
- [13] G. A. Papadopoulos and F. Arbab, "Modelling activities in information systems using the coordination language MANIFOLD," in *Proceedings of the 1998 ACM Symposium on Applied Computing - SAC '98*. Atlanta, Georgia, United States: ACM Press, 1998, pp. 185–193.
- [14] F. Arbab, "Reo: A channel-based coordination model for component composition," *Mathematical Structures in Computer Science*, vol. 14, no. 3, pp. 329–366, Jun. 2004.
- [15] G. A. Papadopoulos and F. Arbab, "Coordination Models and Languages," in *Advances in Computers*. Elsevier, 1998, vol. 46, pp. 329–400.
- [16] P. Clements, "A survey of architecture description languages," in *Proceedings of the 8th International Workshop on Software Specification and Design*. Schloss Velen, Germany: IEEE Comput. Soc. Press, 1996, pp. 16–25.
- [17] N. Medvidovic and R. Taylor, "A classification and comparison framework for software architecture description languages," *IEEE Transactions on Software Engineering*, vol. 26, no. 1, pp. 70–93, 2000.
- [18] N. Medvidovic and R. N. Taylor, "A framework for classifying and comparing architecture description languages," in *Software Engineering — ESEC/FSE'97*, G. Goos, J. Hartmanis, J. van Leeuwen, M. Jazayeri, and H. Schauer, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, vol. 1301, pp. 60–76.
- [19] M. Ozkaya and C. Kloukinas, "Are We There Yet? Analyzing Architecture Description Languages for Formal Analysis, Usability, and Realizability," in *2013 39th Euromicro Conference on Software Engineering and Advanced Applications*. Santander, Spain: IEEE, Sep. 2013, pp. 177–184.
- [20] C. Gomes, C. Thule, D. Broman, P. G. Larsen, and H. Vangheluwe, "Co-Simulation: A Survey," *ACM Computing Surveys*, vol. 51, no. 3, pp. 1–33, May 2019.
- [21] Modelisar, "Functional Mock-up Interface Specification," <https://fmi-standard.org/docs/3.0.1/>, Jul. 2023.
- [22] J. Dahmann, "High level architecture for simulation," in *Proceedings First International Workshop on Distributed Interactive Simulation and Real Time Applications*, 1997, pp. 9–14.
- [23] C. Ptolemaeus, Ed., *System Design, Modeling, and Simulation: Using Ptolemy II*, 1st ed. Berkeley, Calif: UC Berkeley EECS Dept, 2014.
- [24] European Union Agency for Railways., *Report on Railway Safety and Interoperability in the EU 2024*. LU: Publications Office, 2024.
- [25] K. Jensen and L. M. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.
- [26] M. B. Dwyer, G. S. Avrunin, and J. C. Corbett, "Patterns in property specifications for finite-state verification," in *Proceedings of the 21st International Conference on Software Engineering*. Los Angeles California USA: ACM, May 1999.
- [27] G. Hohpe and B. Woolf, *Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions*, ser. The Addison-Wesley Signature Series. Boston: Addison-Wesley, 2004.
- [28] R. C. Martin, *Clean Architecture: A Craftsman's Guide to Software Structure and Design*, 1st ed. USA: Prentice Hall Press, 2017.
- [29] C. Atkinson and T. Kühne, "Rearchitecting the UML infrastructure," *ACM Transactions on Modeling and Computer Simulation*, vol. 12, no. 4, pp. 290–321, Oct. 2002.
- [30] J. de Lara and E. Guerra, "Generic Meta-modelling with Concepts, Templates and Mixin Layers," in *Model Driven Engineering Languages and Systems*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, D. C. Petriu, N. Rouquette, and Ø. Haugen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, vol. 6394, pp. 16–30.
- [31] Object Management Group, "Unified Modeling Language, Version 2.5.1," <https://www.omg.org/spec/UML>, Dec. 2017.
- [32] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*. USA: Addison-Wesley Longman Publishing Co., Inc., 1995.
- [33] M. Cheatham and C. Pesquita, "Semantic Data Integration," in *Handbook of Big Data Technologies*, A. Y. Zomaya and S. Sakr, Eds. Cham: Springer International Publishing, 2017, pp. 263–305.
- [34] F. Macías, U. Wolter, A. Rutle, F. Durán, and R. Rodríguez-Echeverría, "Multilevel coupled model transformations for precise and reusable definition of model behaviour," *Journal of Logical and Algebraic Methods in Programming*, vol. 106, pp. 167–195, Aug. 2019.
- [35] J. Sánchez Cuadrado, E. Guerra, and J. De Lara, "Generic Model Transformations: Write Once, Reuse Everywhere," in *Theory and Practice of Model Transformations*, J. Cabot and E. Visser, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, vol. 6707, pp. 62–77.
- [36] D. Strüder, K. Born, K. D. Gill, R. Groner, T. Kehrer, M. Ohrndorf, and M. Tichy, "Henshin: A Usability-Focused Framework for EMF Model Transformation Development," in *Graph Transformation*, J. De Lara and D. Plump, Eds. Cham: Springer International Publishing, 2017, vol. 10373, pp. 196–208.
- [37] T. Kräuter, A. Rutle, H. König, and Y. Lamo, "A higher-order transformation approach to the formalization and analysis of BPMN using graph transformation systems," *Logical Methods in Computer Science*, vol. Volume 20, Issue 4, p. 12533, Oct. 2024.
- [38] T. Kräuter, A. Rutle, Y. Lamo, H. König, and F. Durán, "Artifacts for MODELS-2025," Zenodo, Jul. 2025. [Online]. Available: <https://zenodo.org/doi/10.5281/zenodo.15784978>
- [39] Object Management Group, "Business Process Model and Notation (BPMN), Version 2.0.2," <https://www.omg.org/spec/BPMN/>, Dec. 2013.
- [40] N. Martí-Oliet and J. Meseguer, "Rewriting Logic as a Logical and Semantic Framework," *Electronic Notes in Theoretical Computer Science*, vol. 4, pp. 190–225, 1996.
- [41] J. Meseguer and G. Roşu, "The rewriting logic semantics project: A progress report," *Information and Computation*, vol. 231, pp. 38–69, Oct. 2013.