On Validation of Semantic Composability in Data-driven Simulation

Claudia Szabo and Yong Meng Teo
Department of Computer Science
National University of Singapore
Computing 1, 13 Computing Drive
Singapore 117417
Email: claudias, teoym@comp.nus.edu.sg

***Abstract*—A simulation model composed using reusable components is semantically valid if it produces meaningful results in terms of expressed behaviors and meets the desired objective. This paper focuses on the validation of component-based data-driven simulation. In data-driven simulation applications, it is necessary to model entity behavior at higher resolution. In simulations such as military training scenarios where entity behavior changes dynamically, additional input data is required to express complex state transitions. This can significantly increase the composed model state space and presents a major challenge in simulation validation. Using a component-based data-driven tactical military simulation, we propose a layered and automated approach for semantic composability validation. While the expressivity of data-driven models increases the semantic equivalence of the validated model, it incurs higher validation cost.**

I. Introduction

Component-based simulation model development aims to reduce the time and cost of developing complex simulations [10] by selecting and composing previously developed simulation components in various combinations to satisfy user requirements [12]. Component-based frameworks that employ reused simulation components promise shorter development time and increased flexibility in meeting diverse user needs [12]. In modeling and simulation, two main levels of composability have been identified, namely syntactic composability and semantic composability [12]. In syntactic composability, components have to be properly connected and must interoperate, which assumes common communication protocols, data formats, as well as a common understanding of the time management mechanisms employed. In semantic composability, the composition must be meaningful for all components involved. Furthermore, the composition must be valid [12], and component-based simulation frameworks must validate semantic composability [10]. This is because simulation models are widely used to make critical decisions [2].

The validation of a simulation model is often manual and lengthy, and requires the presence of a system expert [1], [2], especially since the model is often used in critical situations where a valid answer is crucial, such as in military training simulations [9]. For example, the process of Verification, Validation and Accreditation (VV&A) for modeling and simulation in the US Department of the Navy defines seven user roles and thirteen steps [6]. The difficulty of military simulation model validation process is exacerbated by the model size and resolution. For example, in military training simulations, the state of a tank component changes dynamically based on the GPS coordinates of its enemy, and many internal attributes such as available ammunition, damage, and attack tactics (e.g. direct charge, shoot and scoot, ambush). In this respect, the tank component is considered to be *data-driven*.

The validation of composable simulations is a non-trivial problem [2], [5], [12], [18]. Challenges arise from the fact that composition is not a closed operation with respect to validation because valid components do not necessary form valid compositions [1]. Next, the interaction of reused components may result in emergent properties [8]. Similarly, the context in which a reused component was developed and validated might differ from the new context of the composed model [3], [18]. Lastly, there are various validation perspectives on the component interactions over time. The validation process must address *model behavior* aspects such as deadlock, safety, and liveness, *temporal* aspects such as the behavior of components and compositions over time, and *formal* aspects such as the need to provide a formal measure of the validity of compositions, also called "figure of merit" [10]. The motivation of our work is twofold. Firstly, simulation model validation is a lengthy, manual process that can possibly be improved if a component-based paradigm is applied. Secondly, well-established software verification techniques can be adapted for simulation validation to increase the credibility of the validation process.

In our previous work, we proposed a layered approach to the automated semantic validation of compositions in simulation model integration with increasing accuracy and complexity [15], [16]. Our approach focuses on the validation of general model properties such as semantic correctness of component communication [17], safety and liveness of the logical component coordination in the context of instantaneous transitions, and over time, as well as on providing a formal guarantee of the composition validity [15]. Our layered validation process is implemented in CoDES, a component-based modeling and simulation framework that facilitates component reuse, hierarchical composition within and across application domains, syntactic composability verification and semantic

978-1-4244-7291-8/10/$26.00 ©2010 IEEE

composability validation [14].

In this paper, we discuss the application of our proposed validation process to military training simulations, in which base components are data-driven entities and compositions are complex systems with large state space. We present the Military Training application domain as it is added to the CoDES framework. Next, we show how a military training simulation of a tank versus a soldier troop attack is validated. The validation of data-driven composed models is an improvement of our previous work where the component state machine was less complex and components were not data-driven. In our experiment, we validate a tank versus a soldier troop military training simulation. The contributions of this paper include:

1) An approach for validation of data-driven simulation composed from complex components whose actions depend on the input data received. The application is a closed system with feedback loop. Our validation process guarantees overall *model correctness* from a software engineering perspective, as well as *model validity* from a simulation perspective.
2) The application of our validation process in the validation of military training simulations. Successful application of our validation process has the potential to greatly improve the lengthy military verification, validation, and accreditation process, in the military training application domain.
3) Valuable insight into the problems that arise when a manual process such as simulation validation is automated. Complex models and components incur abstraction trade-offs and the notion of simulation validity defined as conforming to the real system is difficult to capture formally. Furthermore, the complex components result in an increased validation runtime.

This paper is organized as follows. Section II describes how composable data-driven simulations are extended in our component-based simulation framework. Section III shows how a military training simulation of a tank versus soldier troop attack is validated. We discuss related work in Section IV and present our concluding remarks and future work in Section V.

II. Composable Data-driven Simulation

A. Framework Overview

CoDES is a hierarchical component-based framework for modeling and simulation [14] in which a simulation component is modeled as a meta-component, an abstraction of the actual component implementation. The meta-component describes mandatory and specific *attributes* and *behavior* of a component and is used to support model discovery, and syntactic and semantic validation. The component behavior describes the data that it receives and outputs as a set of states. The transitions between states are defined as a set of triggers expressed in terms of input, time and conditions.

Reusable components are divided into three categories. *Base components* are well-defined atomic entities specific to an application domain, such as *Source, Server, Sink* for Queueing Networks, and *SoldierTroop,* and *Tank* for Military Training application domain. A composed simulation can be reused as a *standalone simulator* or as *model components* in a larger simulation model. Model components can also be reused across application domains. Composition grammars determine the syntactic composability of simulation components [14]. COSMO, our component-oriented ontology and COML, our proposed component markup language, facilitate component discovery and semantic validation of compositions [17].

B. Military Simulation

To add a new application domain to the CoDES framework involves extending our component-oriented ontology by providing descriptions of the domain's base components, including defining attribute and property hierarchies. Next, the framework composition grammar is extended by adding composition rules specific to the new application domain.

Tactical Military Training Simulation

For simplicity, we present a Military Training application consisting of two base components, namely a *Tank* that models a tank unit, and *SoldierTroop* that models a troop of soldiers. As shown in Fig. 1, a new simulation model is developed using our graphical input model interface by drag-and-drop icons representing soldiers and tank. The conceptual model is a closed system with feedback loop. Next, the conceptual model

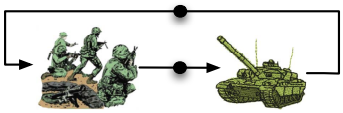

Fig. 1. Tank vs Soldier Troop Training Simulation

is syntactically verified against the new extended composition grammar. If the conceptual model is syntactically correct, each base component is individually discovered based on attributes and behavior information provided by the user.

C. Data-driven Components

Assume that the best candidates returned by the discovery service for the Tank and SoldierTroop base components are components $tank_1$ and $troop_1$ respectively. Table I presents the most important parts of the component state machines. The combined state machines for the two components is shown informally in Fig. 2, with full and dashed lines representing transition changes and message exchange respectively. Input and output messages are prefixed with "?" and "!" respectively. Both tank and soldier troop have an initial position on a two dimensional grid, a number of ammunition shots, and a speed with which they move. For both components, the moving time and the shooting time are sampled from exponential distributions with various mean values. When a component receives the opponent's position, it will move towards the opponent if the opponent is not in range (condition C_1 and attribute change A_1) or it will otherwise fire if it has enough ammunition and

Entity	Attribute	Input	Output	State Machine
$\mathbf{tank_1}$	$health = 100$ $range = 7$ $ammo = 50$ movingTime: exponential(5) shootingTime: exponential(4) $usableThreshold = 20$ $positionX = 20$ $positionY = 15$ $speed = 10$ $team = red$ ... $transient(tank_1) : (ammo == 49)$	I_1, constraints: $class = PositionInfo$ $origin = SoldierTroop$ I_2, constraints: $class = InputFire$ $origin = SoldierTroop$	O_1, constraints: $class = PositionBroadcast$ $destination = SoldierTroop$ O_2, constraints: $class = OutputFire$ $destination = SoldierTroop$	$I_1S_1(\Delta movingTime) \xrightarrow{C_1} O_1S_1A_1$ $I_1S_1(\Delta shootingTime) \xrightarrow{C_2} O_2S_2A_2$ $I_2S_1(\Delta movingTime) \xrightarrow{C_1} O_1S_1A_3$ $I_2S_1(\Delta shootingTime) \xrightarrow{C_2} O_2S_2A_4$ $I_2S_1 \xrightarrow{C_3} O_1S_1$ $I_1S_1 \xrightarrow{C_3} O_1S_1$ $null \quad S_2(\Delta movingTime) \rightarrow O_1S_1A_1$ C_1 : *no opponents in range* C_2 : *at least one opponent in range* $C_3 = health < usableThreshold$ A_1 : *modify position* A_2 : *modify target position* A_3 : *modify position, health* A_4 : *modify target position, health*
$\mathbf{troop_1}$	$health = 100$ $range = 2$ $ammo = 20$ movingTime : exponential(3) shootingTime : exponential(2) $usableThreshold = 40$ $positionX = 40$ $positionY = 45$ $speed = 3$ $team = blue$ ... $transient(troop_1) : (ammo == 49)$	I_1, constraints: $class = PositionInfo$ $origin = Tank$ I_2, constraints: $class = InputFire$ $origin = Tank$	O_1, constraints: $class = PositionBroadcast$ $destination = Tank$ O_2, constraints: $class = OutputFire$ $destination = Tank$	$S_0 \rightarrow O_1S_1$ $I_1S_1(\Delta movingTime) \xrightarrow{C_1} O_1S_1A_1$ $I_1S_1(\Delta shootingTime) \xrightarrow{C_2} O_2S_1A_2$ $I_2S_1(\Delta movingTime) \xrightarrow{C_1} O_1S_1A_3$ $I_2S_1 \xrightarrow{C_3} O_1S_1$ $I_2S_1 \xrightarrow{C_3} O_1S_1$ C_1 : *no opponents in range* C_2 : *at least one opponent in range* $C_3 = health < usableThreshold$ A_1 : *modify position* A_2 : *modify target position* A_3 : *modify position, health* A_4 : *modify target position, health*

TABLE I
META-COMPONENT INFORMATION

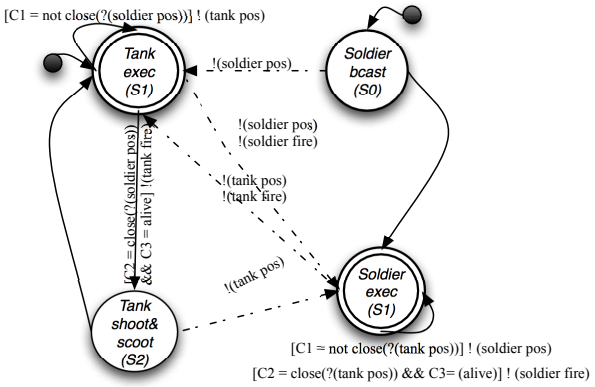

Fig. 2. Data-driven Component Interaction

is not severely damaged (condition C_2 and attribute change A_2). When a component is shot at by receiving an $InputFire$ message, it will be damaged (A_3 and A_4) depending on the closeness to the impact point. The tank component will move immediately from its position after firing at its opponent (state S_2). This is the implementation of a shoot and scoot tactic in which the tank moves after firing to prevent counter-artillery attacks [19]. For simplicity, the components assume that there are no obstacles on the two-dimensional grid battleground. Both tank and soldier troop can obtain the GPS coordinates at any time of their respective enemy. As it can be seen, $tank_1$ and $troop_1$ are data-driven base components.

The extended COML showcased in Fig. 3 caters for data-driven components in two ways. Firstly, attribute names and values can now be specified in the input and output data. Secondly, data oriented transition conditions and attribute changing sections can be specified in the behavior representation. This is in contrast with the previous COML version,

```
<component> ...
 <behavior> ...
  <condition name="C1"><value>
:methods
boolean all(int [][] positions, int n){
for (int i=0; i&lt;n; i++){
if (!( positions[i][0]&gt; positionX−range−1 ||
        positions[i][0]&gt; positionX+range+1 || ...)
        return false;}
        return true;}
:inputs
int [][] positions = new int [100][2];
positions = :init :array: input :I1: position ;
int position_length = 1;
:preamble
boolean alive = (health &amp;gt;= usableThreshold);
:main
System.out.println(all(positions, position_length)
        &amp;amp;&amp;amp; alive);
</value>
</condition>
<data type="input" name="I1">
        <class>PositionInfo</class>
        <constraints> <constraint>
                <type>origin</type>
                <value>Soldier</value>
</constraint></constraints>
<auxAttributes>
<auxAttribute name="position">
<X></X>
<Y></Y>
</auxAttribute></auxAttributes>
</data>
```

Fig. 3. Data-driven Component Representation

which could contain only simple logic such as the one from

C_3. The conditions and attribute changing sections are parsed and evaluated during our validation process by new condition and attribute parsers that determine the condition truth value and the new attribute values respectively. Using the new COML version, we show in Fig. 3 that $tank_1$ expects an auxiliary attribute with two fields in its input message. Next, complex logic is now parsed for state changing conditions and attribute modifications, such as the one for C_1.

Each component input and output message is defined in COML by data constraints. The constraints describe the primitive data present in the message (if any), as *data_type* and *range* constraints, as well as the type of components that can receive or send the output or input message respectively, as *destination* and *origin* constraints [17]. Condition C_1 in the $tank_1$ state machine aims to establish if any of the tank targets are within range. The condition parser that evaluates condition C_1 will construct a `.java` file with the structure determined by the `:methods`, `:inputs`, `:preamble`, `:main` tags. This file will be compiled and executed and the result of the execution (`true` or `false`) will determine the truth value of condition C_1. Similar structure is found in the attribute values modification section in our COML schema. In the new version of COML, Java code is used to express complex conditions, but backward compatibility with the existing components in the framework repository is preserved. This is important because the current CoDES repository has approximately two thousand Queueing Networks models [14].

III. Semantic Composability Validation

In contrast to military training simulation validated using a lengthy and manual process involving simulation experts, we show how validation is automated in our component-based simulation framework. Our approach to semantic composability validation is organized in two steps, as shown in Fig. 4. Based on our definition of semantic validity, we first validate

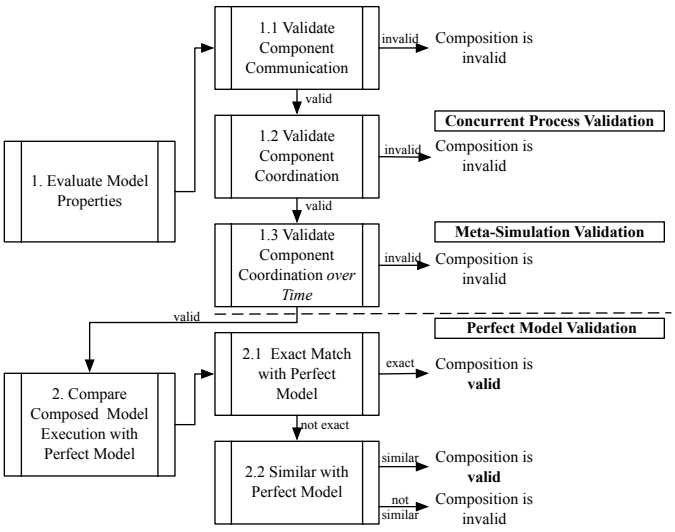

Fig. 4. Layered Approach to Semantic Validation

general properties of the composed model. These properties include component communication, and the component coordination in the context of instantaneous and timed transitions. Next, we formally compare the execution of the composed model over time with that of a perfect reference model. This second step provides a formal measure of the composition validity.

In the validation of general model properties, we first validate that component communication is semantically meaningful according to the COSMO ontology [17]. All subsequent validation stages assume that the component communication is meaningful and correct. Next, in Concurrent Process Validation layer (CPV), we validate that the component communication is correctly coordinated, regardless of time considerations or specific computations that the components might perform, but for all possible interleaved executions. If this is true, we introduce the concept of time in the Meta-Simulation Validation layer (MSV), and validate safety, liveness and deadlock freedom using sampled time values for the time attributes. The CPV layer employs model checking to validate that the component coordination is logically correct. In MSV, we introduce simulation concepts such as sampled time intervals and simulation-oriented definitions of safety and liveness. Furthermore, we employ attribute values provided by the user. This concludes the validation of general model properties.

In the second level, we formally compare the model to a perfect model from the repository by analyzing how close the component execution is to the perfect model. We consider the perfect model to be the representation of the real system that the composed model simulates.

A. Validation of General Model Properties

Concurrent Process Validation

The *Concurrent Process Validation* layer validates the component *coordination* of the composed model. This layer guarantees that safety, liveness, as well as deadlock freedom hold for all possible interleaved executions of *instantaneous* transitions of the composed simulator abstracted as a composition of concurrent processes. The behavior of each meta-component modeled as a state machine is translated into a logical specification using a logic converter module. To prevent state explosion, each component state machine is reduced by considering only communication states and attributes that influence state transitions. The actions of non-communicating states are abstracted as a single atomic operation. Similarly, time is not modeled and transitions are considered instantaneous.

Fig. 5 shows a possible translation of the component state machine into a Promela specification to be validated by the Spin model checker [4]. Transitions between states are instantaneous. Thus, time attributes such as $\Delta shootingTime$ and $\Delta movingTime$ from Table I are ignored. Each type of connector is defined as a Promela process. For example, process *CON_ONE_TO_ONE* on line 3 describes the one-to-one connector. In the `init` method on line 20, communication channels are assigned to the connectors and components

```
1  mtype {MSG}; chan to1 = [10] of {mtype}; ...
2  proctype CON_ONE_TO_ONE(chan in, out)
3  {do :: in ? MSG -> out ! MSG; od}

5  proctype TANK(byte id; chan in, out){
6  S1: atomic{ if :: in ? MSG -> if
7    :: out ! MSG -> progress: printf("MSG sent\n");
8                    goto S1; fi fi}}

10 proctype SOLDIERTR(byte id; chan in, out){
11 bit initial = 1;
12 S0: atomic{ if
13 :: ( initial == 1) -> initial = 0;
14  if :: out ! MSG -> goto S1; fi fi}
15 S1: atomic{ if
16 :: in ? MSG -> if
17 :: out ! MSG -> progress: printf("MSG sent\n");
18                  goto S1; fi fi
19 }}
20 init { run TANK(1, to1, from1);
21 run SOLDIERTR(2, to2, from2); ...}
```

Fig. 5. Simplified Tank vs Soldier Troop in Promela

according to their connection topology. Similar to the behavior of connectors in the real system, communication in our Promela specification is asynchronous. Liveness is specified using `progress` labels such as the one on line 7, and safety is specified using `assert` statements.

Discussion: This example has led to some interesting observations on the translation from a component state machine to a feasible Promela specification. Previously for the Queueing Networks Application Domain, the non data-driven state machines could be almost exactly transformed into Promela and the process was easily automated [15]. However, when data-driven component state machines are used, the process is not easily automated. For example, if we were to interpret component coordination strictly from a message passing perspective, the resulting Promela specification would be that presented in Fig. 5. This type of interpretation is easily automated and focuses only on component coordination. However, it lacks expressivity and any coordination logic. On the other hand, if we were to exactly transform the component state machines from their COML specification into Promela like in Fig. 6 for the $troop_1$ component, we would obtain a more exact description of the attack but it is difficult to automate the translation process. In this example, we represent the composition according to Fig. 6 and consider finding a middle ground between the two approaches part of our future work.

Meta-Simulation Validation

The meta-simulation layer validates if the logical properties demonstrated previously hold through time. Our implementation translates the complete state machine of each component into a Java class hierarchy. Attributes and their values provided by the user, state transitions, and time are modeled. Next, we construct a meta-simulation of the composed model using the translated classes, and execute the model. Sampling is performed for time attributes such as

```
1  mtype {MSG_POS,MSG_FIRE, MSG_DIE}; ...
2  proctype SOLDIERTR(byte id, health, ..., posX, posY;
3                     chan in, out)
4  {bit initial = 1; byte posXFire, posYFire;
5  byte msgPosX, msgPosY, auxX, auxY, auxDistance ,...;
6  S0: atomic{
7  if :: ( initial == 1) -> initial = 0;
8    if :: out ! MSG_POS -> goto S1; fi fi}
9  S1: atomic{ if                    atomic{if
10 :: in ? MSG_FIRE, msgPosX, msgPosY ->
11    health = health - 10;
12    if :: health < health_threshold ->
13         if :: out ! MSG_DIE -> goto end; fi
14    :: else
15       if :: out!MSG_POS, posX, posY ->
16       progress: printf("MSG sent\n");
17       goto S1; fi
18    fi
19 :: in ? MSG_DIE -> out ! MSG_DIE;goto end;
20 :: in ? MSG_POS, msgPosX, msgPosY ->
21 //GPS coord
22 if
23 :: !(msgPosX<posX-range||msgPosX>posX+range
24 || msgPosX<posY-range||msgPosY<posY+range)->
25 if
26 :: ammo>0->out!MSG_FIRE,msgPosX,msgPosY;
27 ammo--; goto S1;
28 fi
29 :: else -> auxDistance = distance;
30 atomic{if
31 :: msgPosX<posX->auxX = msgPosX+range;
32 :: else -> auxX = msgPosX - range; fi} ...
33 //similar to calc nxt position
34 if //broadcast position
35 :: out ! MSG_POS, posX, posY -> goto S1; fi
36 fi fi }
37 end: skip; }
38 init {
39 run TANK(1, 100, 20, 5, 40, 45, to1, from1);
40 run SOLDIERTR(2, 100, 10, 5, 15, 20, to2, from2); ... }
```

Fig. 6. Detailed Tank vs Soldier Troop Attack in Promela

$shootingTime$ and $movingTime$.

Two important logical properties to be validated through time are safety and liveness. From a practical perspective, safety means that components do not produce invalid output. The simulator developer specifies the desired output by providing *validity points* at various connection points in the composition, which contain semantic description of data that must pass through the connection point. For example, one validity point for the data that passes through the feedback one-to-one connector in Fig. 1 could be $VP_1 = d_1\{origin = SoldierTroop, destination = Server, position.X\{range = 20; 40, type = int\}\}$, ensuring the new position for $troop_1$ is properly calculated. Liveness is validated by considering a *transient* predicate assigned to each component ideally by the component creator as shown in Table I. A component is considered *alive* if its liveness observer has evaluated the transient predicate to *true* and then to *false* in a time interval smaller than the specified timeout.

B. Perfect Model Validation

In step 2, a model M composed of $tank_1$ and $troop_1$ is validated by comparison with a perfect model M^* consisting

of perfect components $tank^*$ and $troop^*$. A perfect component is a generic, desirable representation of a base component ideally provided by domain experts when the new application domain is added to the framework. Ideally, the perfect components should describe what the system experts consider to be the desirable base component behavior. It should be generic in the sense that their description lacks any real data values. It follows that the perfect model composed from the generic perfect components is only a description of the desired simulation, without an attached implementation. Throughout the validation process, the generic perfect components attributes will be instantiated using the same attribute values used by the corresponding components in the composed model M. The attribute correspondence is established by using the COSMO ontology. For the military training application domain, we assume the perfect component $troop^*$ to be the same as component $troop_1$ from Table I. Let component $tank^*$ state machine be the one presented in Table II. Notice that the difference between $tank^*$ and $tank_1$ is in the missing state S_2. This is because $tank^*$ implements a direct attack tactic whereas $tank_1$ implements a shoot and scoot tactic.

Entity	Data	State Machine
$\mathbf{tank}^*$	**Input** I_1, constraints: $class = PositionInfo$ $origin = SoldierTroop$	$I_1S_1(\Delta movingTime) \xrightarrow{C_1} O_1S_1A_1$ $I_1S_1(\Delta shootingTime) \xrightarrow{C_2} O_2S_1A_2$ $I_2S_1(\Delta movingTime) \xrightarrow{C_1} O_1S_1A_3$ $I_2S_1(\Delta shootingTime) \xrightarrow{C_2} O_2S_1A_4$
	I_2, constraints: $class = InputFire$ $origin = SoldierTroop$	$I_2S_1 \xrightarrow{C_3} O_1S_1$ $I_1S_1 \xrightarrow{C_3} O_1S_1$
	Output O_1, constraints: $class = PositionBroadcast$ $destination = SoldierTroop$	C_1 : *no opponents in range* C_2 : *at least one opponent in range* $C_3 = health < usableThreshold$ A_1 : *modify position* A_2 : *modify target position*
	O_2, constraints: $class = OutputFire$ $destination = SoldierTroop$	A_3 : *modify position, health* A_4 : *modify target position, health*

TABLE II
PERFECT COMPONENT STATE MACHINE

Our formal validation layer is divided into five steps, namely (i) *Formal Component Representation* in which component state machines are translated into our proposed time-based formalism, (ii) *Unfolding and Sampling* in which time attribute values are sampled, (iii) *Mathematical Composability* in which the mathematical composability of functions is validated, (iv) *Representation of Model Execution* in which the execution of the composed model is represented as a Labeled Transition System (LTS) [13], and (v) *Bisimulation Validation* in which the execution of model M is validated against the execution of model M^* [16].

Formal Component Representation

Definition 1 describes the formal representation of a component as a mathematical function.

Definition 1. *(*Component) A simulation component, C_i, is defined as a function $f_i : X_i \rightarrow Y_i$, where $X_i = I_i \times S_i \times T_i$, and $Y_i = O_i \times S_i \times T_i$. I_i and O_i are the set of input/output messages, S_i is the set of states, and T_i is the set of simulation time intervals at which the component changes state.

The state machine for component $tank_1$ is translated to a formal component representation specified by f_1 as

$f_1 : \{I_1, I_2\} \times S_1 \times T_1 \rightarrow \{O_1, O_2\} \times S_1 \times T_1$, $f_1(I_1, s_i, t) \rightarrow (O_1, s_i', t+\Delta t)$, $f_1(I_1, s_i, t) \rightarrow (O_2, s_i', t+\Delta t)$, ..., where Δt is sampled from a specific distribution (either the distribution for $movingTime$ or $shootingTime$) and the function is recalled until $t > T$, where the simulation runs for time $T = 400$ wall clock units.

Unfolding and Sampling

As it can be seen, the above expression for f_1 is not useful because during a simulation run, t and Δt have specific values. In this step, we unfold the function definition for $\tau = 5$ times and sample the values for Δt from $\Delta movingTime$ or $\Delta shootingTime$, using mean values provided by the user. For f_1, Δt takes values as necessary from the sampled values of $movingTime, exponential(mean = 5) = \{20, 40, 70\}$, and $shootingTime, exponential(mean = 4) = \{10\}$, as shown in Table III.

	Unfold	Δt	Formula		
f_2	1	-	$f_2(\emptyset, s_1^2, 0 \geq 0)$	$\rightarrow$	$(O_1, s_2^2, 0)$
	2	20	$f_2(I_1, s_2^2, var_1 \geq 0)$	$\rightarrow$	$(O_1, s_3^2, var_1 + 20)$
	3	40	$f_2(I_2, s_3^2, var_2 \geq var_1 + 20)$	$\rightarrow$	$(O_1, s_4^2, var_2 + 40)$
	4	10	$f_2(I_1, s_4^2, var_3 \geq var_2 + 40)$	$\rightarrow$	$(O_2, s_5^2, var_3 + 10)$
	5	80	$f_2(I_2, s_5^2, var_4 \geq var_3 + 10)$	$\rightarrow$	$(O_1, s_6^2, var_4 + 80)$
f_1	1	50	$f_1(I_1, s_1^1, var_{21})$	$\rightarrow$	$(O_1, s_2^1, var_{21} + 50)$
	2	10	$f_1(I_1, s_2^1, var_{22} \geq var_{21} + 50))$	$\rightarrow$	$(O_2, s_3^1, var_{22} + 10)$
	3	3	$f_1(\emptyset, s_3^1, var_{22} + 10)$	$\rightarrow$	$(O_1, s_4^1, var_{22} + 13)$
	4	30	$f_1(I_1, s_4^1, var_{23} \geq var_{22} + 13)$	$\rightarrow$	$(O_2, s_5^1, var_{23} + 30)$
	5	7	$f_1(\emptyset, s_5^1, var_{23} + 30)$	$\rightarrow$	$(O_1, s_6^1, var_{23} + 37)$

TABLE III
FORMAL COMPONENT REPRESENTATION

Mathematical Composability

Next, the function composability is validated in the *Mathematical Composition* step. Following Definition 2, we obtain constraints for the values of var_1, var_2,var_3, var_4 and $var_{21}, var_{22}, var_{23}$ respectively.

Definition 2. *(*Mathematical Composability) Given a composed model $M = \{(f_i, f_j) | i \neq j, i, j = \overline{1, n}\}$, where f_i outputs and f_j requires input with time values $T_i^{out} = \{t_m^{(i)} | 1 \leq m \leq |O_i|\}$, and $T_j^{in} = \{t_n^{(j)} | 1 \leq n \leq |I_j|\}$, respectively. Then f_i and f_j are composable iif there exists the bijective binary relation $R = \{(t_n^{(j)}, t_m^{(i)}) \in T_j^{in} \times T_i^{out} | t_n^{(j)} > t_m^{(j)}\}$.

It is evident that the first call to function f_1 has to take place after *at least one* call to f_2 has completed and produced output, since f_1 requires output from f_2. Because there exists a *feedback loop* between f_2 and f_1, the second call for f_2 at time var_1 has to take place at least after the first call to f_1, resulting in the $var_1 \geq var_{21} + 50 + w_{21}$, where w_{21} is the average time spent in the connector queue from f_2 to f_1. From a realistic perspective, we also consider the average time spent by messages in the connector queues, which is obtained from the meta-simulation validation layer. Assuming that the average times spent in the connector queues are $\Delta w_{12} = 2$, $\Delta w_{21} = 3$ for the connector between f_1 and f_2 and vice-versa, the most trivial constraints that can be derived are:

$var_1 \geq 0, var_1 \geq var_2 1 + 50 + \Delta w_{12},$
$var_2 \geq var_1 + 20, var_2 \geq var_{22} + 10 + \Delta w_{12},$
$var_3 \geq var_2 + 40, var_3 \geq var_{22} + 13 + \Delta w_{12},$
$var_4 \geq var_3 + 10, var_4 \geq var_{23} + 30 + \Delta w_{12}.$

$var_{21} \geq 0 + \Delta w_{21}$,
$var_{22} \geq var_{21} + 50, var_{22} \geq var_1 + 20 + \Delta w_{21}$,
$var_{23} \geq var_{22} + 13, var_{23} \geq var_2 + 40 + \Delta w_{21}$.
Next, the constraints are solved by the Choco constraint solver. Assume that a solution is:
$f_2 : (var_1 = 56, var_2 = 91, var_3 = 131, var_4 = 166)$,
$f_1 : (var_{21} = 4, var_{22} = 79, var_{23} = 134)$.

The same process is applied for perfect functions f_i^* using the same sampled values and average waiting times. However, the set of constraints and the number of variables are different because of the different implementation for component $tank_1$. The constraint solver returns the following solution:
$f_2^* : (var_1 = 56, var_2 = 91, var_3 = 166, var_4 = 201)$,
$f_1^* : (var_{21} = 4, var_{22} = 79, var_{23} = 134, var_{24} = 179, var_{25} = 284)$.

Representation of Model Execution

Interleaved execution schedules are next obtained for both composition and perfect composition and further represented as a Labeled Transition System (LTS), $L(M)$ and $L(M^*)$ respectively, as shown in Fig. 7. Each node represents

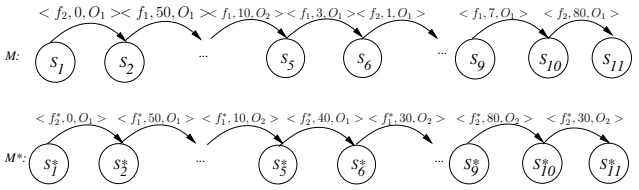

Fig. 7. LTS Representation of Model Execution

an annotated composition state $S_{j=1,n*\tau}$. Edges are the function calls f_i and f_i^* respectively, and labels are the tuple *<function_name, duration, output>*, where $duration$ represents the function execution time.

Bisimulation Validation

In the *Validation* step, we check the bisimulation between $L(M)$ and $L(M^*)$ using the BISIMULATOR tool in the CADP toolset [7]. It is evident that the two LTS are not strongly equivalent (see the outgoing labels from S_5, S_6, S_9, S_{10} and S_5^*,S_6^*,S_9^*,S_{10}^* respectively), hence the BISIMULATOR tool returns `false`. Next, we relax the validation constraints by defining a semantic metric relation V with parameter ϵ. V_ϵ considers only semantically related LTS nodes for which our defined semantic distance is smaller than ϵ. A node S_i from $L(M)$ is related to a node S_j^* from $L(M^*)$ iif $d(S_i, S_j^*) \leq \epsilon$. The calculation of d considers (i) the function that is called to exit the two nodes respectively, and (ii) the similarity of the composition states in nodes S_i and S_j^*. The composition state refers to all attribute values for all components in the composition. As such, for attribute names that are the same or similar (according to the COSMO ontology), we consider whether their values are the same or have followed a similar modification trend (e.g. $ammo$ has been decreasing) throughout the unfolding. From the related states set we construct two new LTS, $L_1(M)$ and $L_1(M^*)$ as follows. For each pair of related states (S_i, S_j^*), with $S_i \in L(M)$ and $S_j^* \in L(M^*)$ we add to $L_1(M)$ all pairs (S_i, S_k), where there exists an edge between S_i and S_k in $L(M)$. Similarly, we add to $L_1(M^*)$ all pairs (S_j^*, S_r^*), where there exists an edge between S_j^* and S_r^* in $L(M^*)$. Next, we try to determine the relation between the new $L_1(M)$ and $L_1(M^*)$. We iteratively try possible relations including equivalence, smaller than ($L_1(M)$ included in $L_1(M^*)$), and greater than ($L_1(M^*)$ included in $L_1(M)$). Space constraints prevent us from showing the detailed process here, but for $V_\epsilon = \{(S_i, S_j^*) \| i \neq 5, 6, 9\}$, with $\{\|S_i - S_j^*\|_\sigma = 0.07 | \forall i \neq 5, 6, 9\}$, we can see that $L_1(M)$ is included in $L_1(M^*)$.

Discussion: The execution time for the formal validation layer is clearly affected by the size and complexity of the components. The runtime increases with the number of attributes per component because in the calculation of V_ϵ *all* combinations of component attributes are considered when querying the COSMO ontology. Similarly, a larger number of state transition conditions translates into increased number of calls to the condition parsers. To determine the runtime increase of the data-driven simulation model compared to a non-data driven simulation, we analyze the execution runtime of simpler queueing network models. In the Queueing Networks (QN) application domain, components are not data-driven, have at most two states and a reduced number of attributes. To determine the effect of the component complexity on the runtime, we compare with a single-server queue simulation model, which is the simplest Queueing Networks model. While an entirely fair comparison between the above models cannot be made, our findings from Table IV show that for roughly the same number of components and states, the data-driven model has twice the number of attributes and incurs a runtime almost eight times higher. However, the runtime penalty is still acceptable considering the increased expressivity gains.

	Single-Server Queue	*Tank vs Soldier Troop*
Data-driven	x	✓
# comp	3	2
avg #states/comp	1.6	2
avg #att/comp	7.6	20
avg #delay time/comp	1	2
Runtime (s)		
Exact Match	3.0	6.2
$\mathbf{V}_\epsilon$	2.7	16.1

TABLE IV
EXECUTION RUNTIME EVALUATION

The Tank vs SoldierTroop example example raises some interesting issues. Firstly, a valid model is defined as *close enough* with respect to the states, sequence and duration of component execution, to a perfect model. Yet, what exactly is close enough (i.e. the values of ϵ), as with all thresholds, remains an open problem. Furthermore, the impact of different values of the degree of unfolding τ remains to be studied. Intuitively, τ should be large enough to capture all deviating behaviors, but an optimal value of τ is difficult to obtain beforehand. Next is the difficult problem of defining the perfect models and components. While it is acceptable to assume their existence, how they are obtained is still an open question. For example, perfect components could be decomposed from perfect models specified by the simulation composer, or can exist a priori as we previously suggested.

IV. Related Work

Petty and Weisel pioneered a formal theory of composability validation which allows for a composed simulation model to be checked for semantic validity [12]. A composition is modeled as a mathematical functional composition over one-dimensional integer domains. The composition simulation is represented as an LTS where nodes are model states, edges are function executions, and labels are model inputs. However, time is not modelled and the component function is instantaneous. This permits only a *static* representation of the composition. Furthermore, the LTS representation considers the functions strictly in the order they appear in the mathematical composition, which might not be representative of complex compositions. In contrast, we propose a new formal component definition where states change over *time*. Based on this definition, we represent the dynamic change of the entire simulation over time. To provide a more accurate measure of validity, we consider semantically related composition states in the definition of semantic relation V_ϵ.

A more informal approach to composition validation uses the Base Object Model (BOM) as a component abstraction [11]. A BOM captures component behavior information including participating entities and their state machines, and information about the possible usage scenarios of the component. This approach assumes that a detailed user specified composition scenario exists to represent a valid composition. Component discovery is done based on the specified scenario. A valid composition of discovered components is one in which the sequence of actions or events is the same as or includes the sequence specified in the scenario. However, the somewhat informal validation process includes the composition and execution of discovered components in *all* possible combinations in order to be compared with the specified scenario. Furthermore, a detailed execution scenario for validation might not be available from the model composer.

V. Conclusions

Data-driven military simulations have complex behavior that changes rapidly with received data. To support component-based simulation and its semantic validation, a new data-driven component representation is proposed for specifying state transitions and attributes changes. Most military simulations are manually validated using a lengthy and costly multi-step process. We propose to address this using a two-step automated semantic composability validation approach. Firstly, we validate a component-based model for general model properties including safety and liveness for instantaneous transitions and through time. In addition, safety and liveness are considered from a software verification perspective as logical statements, and from a simulation perspective in terms of output data and the desired composed model state changes. We show that a composed model consisting of components at higher level of abstraction can be easily translated into a concurrent process specification for verification using a model checker. However, real-life components may require lower-level of abstraction and higher expressivity to support validation. To increase the validation accuracy, we next validate the composed model with a perfect model. Components are represented using a new time-based formalism, and bisimulation is used to reason the composition validity. As expected, data-driven model validation incurs higher runtime but the overhead is small for the examples used.

While this paper addresses the semantic validation of data-driven simulation with *base components*, the complexity and scalability of component-based models can be increased by reusing the composed model as a *model component* in new models. This involves extending our current formal validation process. However, addressing the important design trade-off between the degree of model component opacity and the accuracy of validation is an open question.

References

[1] O. Balci. Verification, Validation and Accreditation of Simulation Models. In *Proc. of the Winter Simulation Conference*, pages 135–141, Atlanta, USA, 1997.

[2] J. Banks, J. Carson, B. Nelson, and D. Nicol. *Discrete-Event System Simulation*. Prentice Hall, 2005.

[3] R. Bartholet, D. Brogan, P. Reynolds, and J. Carnahan. In Search of the Philosopher's Stone: Simulation Composability Versus Component-Based Software Design. In *Proc. of the Fall Simulation Interoperability Workshop*, Orlando, USA, 2004.

[4] M. Ben-Ari. *Principles of the Spin Model Checker*. Spr. Verlag, 2008.

[5] P. Davis and R. Anderson. Improving the Composability of Department of Defense Models and Simulations, 2003.

[6] Department of the Navy. *Modeling and Simulation Verification, Validation, and Accreditation Implementation Handbook* . 2004.

[7] H. Garavel, F. Lang, R. Mateescu, and W. Serwe. CADP 2006: A Toolbox for the Construction and Analysis of Distributed Processes. In *Proc. CAV'07*, pages 158–163, Berlin, Germany, 2007.

[8] R. Gore and P. Reynolds. Applying Causal Inference to Understand Emergent Behavior. In *Proc. of the Winter Simulation Conference*, pages 712–721, USA, 2008.

[9] D. S. Hartley. Verification & Validation in Military Simulations. In *Proc. of the Winter Simulation Conference*, pages 925–931, Georgia, USA, 1997.

[10] S. Kasputis and H. Ng. Composable Simulations. In *Proc. of the Winter Simulation Conference*, pages 1577–1584, Orlando, USA, 2000.

[11] F. Moradi, R. Ayani, S. Mokarizadeh, G. H. A. Shahmirzadi, and G. Tan. A Rule-based Approach to Syntactic and Semantic Composition of BOMs. In *Proc. of DS-RT*, pages 145–155, Crete, Greece, 2007.

[12] M. Petty and E. W. Weisel. A Composability Lexicon. In *Proc. of the Spring Simulation Interoperability Workshop*, pages 181–187, Orlando, USA, 2003.

[13] J. Srba. On the Power of Labels in Transition Systems. In *Proc. of the 12th International Conference on Concurrency Theory*, pages 277–291, Aalborg, Denmark, 2001.

[14] C. Szabo and Y. Teo. On Syntactic Composability and Model Reuse. In *Proc. of the International Conference on Modeling and Simulation*, pages 230–237, Phuket, Thailand, 2007 (invited paper).

[15] C. Szabo and Y. Teo. An Approach for Validation of Semantic Composability in Simulation Models. In *Proc. of the 23rd ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation*, pages 3–10, Lake Placid, USA, 2009.

[16] C. Szabo, Y. Teo, and S. See. A Time-based Formalism for the Validation of Semantic Composability. In *Proc. of the Winter Simulation Conference*, pages 1411–1422, Austin, USA, 2009.

[17] Y. Teo and C. Szabo. CODES: An Integrated Approach to Composable Modeling and Simulation. In *Proc. of the 41st Annual Simulation Symposium*, pages 103–110, Ottawa, Canada, 2008.

[18] A. Tolk. What Comes After the Semantic Web - PADS Implications for the Dynamic Web. In *Proc. of the 20th Workshop on Principles of Advanced and Distributed Simulation*, pages 55–62, Singapore, 2006.

[19] US Army Field Manual No. 3-09.22, Headquarters, Department of the Army. Tactics, Techniques, and Procedures for Corps Artillery, Division Artillery, and Field Artillery Brigade Operations, 2001.