Spatial Ontologies and Models for Safety-Critical Cyber-Physical Systems

Leonard Petnga
Department of Civil and Environmental Engineering
University of Maryland, College Park, MD 20742, USA
Email: lpetnga@umd.edu

Mark A. Austin
Department of Civil and Environmental Engineering
and Institute for Systems Research
University of Maryland, College Park, MD 20742, USA
Email: austin@isr.umd.edu

***Abstract*—Our research is concerned with the modeling and design of safety-critical cyber-physical systems (CPS), where decision making procedures are required to take the right action at the right time, and in the right place. This paper examines the role that spatial ontologies and models can play in formally representing and reasoning with spatial domain entities occurring in CPS. We develop and introduce a new multi-dimensional spatial modeling hierarchy and reasoning framework supported by region connected calculus (RCC-8). The proposed approach is demonstrated on a problem that considers collision of two vehicles at a traffic intersection. We show that the dimensional fidelity of spatial entities (e.g., one-dimensional representations versus two-dimensional representations) strongly affects the accuracy of decision making outcomes.**

Keywords-Cyber-Physical Systems; Spatial Modeling; Transportation Safety.

I. Introduction

This paper examines spatial semantics and their use in supporting the creation of accurate, precise, scalable and reusable models of space in the context of safety-critical cyber-physical systems (CPS) design. For this family of CPS, safety and performance are dependent on correct space and time-based predictions of future system state. In other words, it's critical that the system makes the right decision and takes the right action at the right time and right place for it to remain safe [1].

The central premise of our research is that tackling these challenges requires the development of a scalable, flexible, and customizable ontological framework that supports the embedding of physical semantics into cyber models for system smartness. Thus, the need for ambiguity-free models of space that properly capture the spatial configuration of the system as it's materialized in the world. This is an essential foundation for reasoning tasks involving spatial entities. We discuss the key role that ontologies can play in capturing and formally representing the space domain. Spatial theories and Description Logic (DL) semantics supporting the formalization of spatial knowledge and the decidability of derived spatial reasoning systems are reviewed. We highlight the use of the region connectedness calculus (RCC-8) algebra (see Figure 1), and spatial relationships to support the reasoning about space and spatial regions. We develop and propose a simple, multi-dimensional tree structure of spatial models that support the representation of spatial entities at various level of granularity and enable the use of associated operations and predicates essential for reasoning using complex spatial datatypes. We demonstrate the use of our approach in the problem of establishing/predicting the glancing collision of two vehicles at an intersection. We show that the ontological commitment (i.e., how you see the world) of the model of the vehicles with regard to the dimension of the space is critical to the proper understanding of the spatial configuration of the system in the world by the cyber (vehicle on-board computer) and the prediction of the collision.

II. Spatial Ontologies and Semantics Support for MBSE of CPS

A. Overview of spatial theories

Researchers have identified the need for formal definition of space to support the ontological modeling of this domain. Given the context of this work, we will highlight those spatial theories and calculus that may be suitable for CPS. Thus, we'll lean toward geometrical or physical structures of space that are more practical for reasoning tasks. This is consistent with the Newtonian view of space which distinguishes space from the objects with a location within it as opposed to Leibnizian approach which defines space in term of inter-relationships between objects [2]. To that end, we will revisit Vieu's views in [3] and adopt a mereotopological categorization of spatial theories which mirrors - to a certain extent - the one of temporal theories, with the difference that unlike time, space is neither oriented nor cyclic. We categorize the main spatial theories and calculus as follows.

1. Space-point: Space is viewed as an arrangement of points, supported by orientation and distance concepts; lines and regions are defined as set of points. This approach is favored by mathematical theories of space.

2. Space-interval: Similar to Allen's temporal intervals, 2D intervals result from the projection (while preserving orientational information) of regular regions (i.e., rectangular shapes) onto the axes of a reference frame are the primitives.

3. Space-array: Space is a collection of arrays in a discrete coordinate system that concurrently captures topological, orientation and distance information. This is the preferred theory in computer visualization and spatial databases and linking - linguistic linking applications.

4. Space-region: convex region of any shape with dimension higher than one is the primitive in these theories. Region-

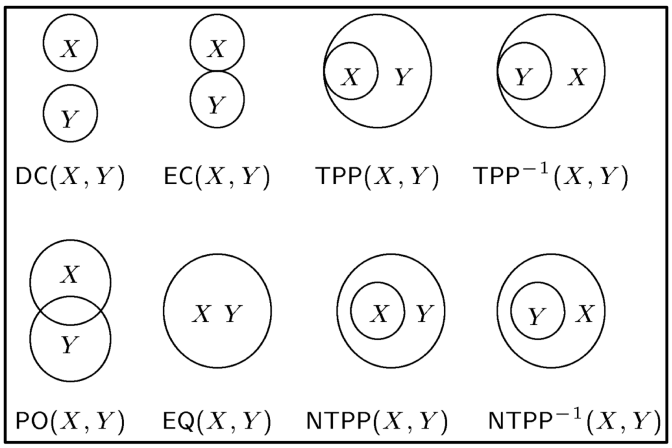

Figure 1. Eight types of relationships between spatial entities in Region Connection Calculus (RCC-8).

based theory axiomatized around the connection relation C and theories built from one mereological (part) and one topological (contact or external connection) relations belong to this category.

5. Space-multidimension: incidence relationship is used in lieu of ontological dependency with no restriction on the dimensionality of spatial primitives. The focus on non-mereotopological aspects such as (multi)dimension and boundary.

The high variety and depth of spatial theories makes a full accounting of space very challenging. Theorizing space is rendered more complex than time because of non-mereotopological aspects such as dimension, orientation, shape, length, area or volume that are relevant in safety-critical CPS applications. Also, latitude, longitude, elevation, geopolitical subdivisions or aggregates are of high importance in applications with geographic information (GIS) aspects [4]. Existing theories accounting for many of these aspects - such as CYCORD and CanConnect calculus - often involve explicit triadic relations that complicate space-based reasoning [5].

B. Ontologies of space and spatial models

Spatial Ontologies. Ontologies of space need to support models of space that are three-dimensions (or less) and work with ontologies and models of time that are one dimensional. Spatial ontologies can be organized into hierarchies of spatial concepts (a taxonomy), and can be made more rigorous through the addition of axioms [6][7]. As a case in point, axioms in the basic formal ontology (BFO) [8] are built under the premises that reality can be described using two kinds of ontologies: SNAP (purely spatial) and SPAN (space-time continuum) ontologies. With respect to ontological needs for spatially-related entities in CPS, it's necessary to enable the combination of entities from both types of ontologies for a better rendering of the reality. However, for the purpose of this work, we adopt a SNAP view of the world.

Spatial Models. Spatial models can be classified as being either symbolic or geometric. Geometric models make use of cells and/or boundaries as primitives model entities. Symbolic models use topological-based structures and/or graphs to capture connectivity, reachability and hierarchies between spatial entities. Even though the latter class of models provides semantically compliant entities location (partially) in a human-readable way along with topological relationships, their ontological commitment with regard to the spatial theories introduced in Section II-A is ambiguous and can't be systematically traced to a sound logical foundation. This makes their use in the context of reasoning for safety-critical CPS applications inappropriate.

C. Description logic formalisms and spatial semantics for CPS

It has been shown [1] that description logic semantics (DLs) offer precise capture and representation of domain knowledge with ontology languages such as OWL (Web Ontology Language) [9]. In turn, OWL can be used to formally axiomatize time according to Allen's temporal interval calculus [10]. As we will show below, its mathematical foundation remains appropriate for the unambiguous, concise and verifiable representation of the spatial domain as well (as per the qualified spatial theory). For CPS applications, modeling should provide the meaning of syntactically valid collections of spatially-related symbols expressed in a given formal language such as OWL. Moreover, in order to foster proper descriptions of space, there is a need of metadata and spatial relation semantics. State-of-the-art spatial semantics are mostly geared towards cognitive linguistic meanings of spatial concepts [11] or visual processing of spatial information [12]. However, in [13], the author investigates spatially oriented semantics for DLs, base off conceptual spaces and the region connection calculus.

III. Framework for Hybrid Spatial Modeling and Reasoning

A. Space Matters: Formal models of space for CPS

In order for formal approaches (such as model checking and theorem proving), to the verification of CPS to be effective, system models need to capture the appropriate granularity of space. considering it can be under-specified in utterances and natural language expressions. For instance, consider the following expressions: (a) The car wandered *around* the 188 train accident scene (b) The car wandered *to* the 188 train accident scene. As pointed out by Thorton [11], the pairing of the non-directional verb "wander" and the prepositions "around" and "to" leads to ambiguity that needs either resolution or semantic coercion to properly interpret the notion of place (a) and path (b). Furthermore, the dimension(s) to which the two spatial concepts (i.e., place and path) is unknown, but it's very relevant as we will soon see. State-of-the-art models of safety-critical systems and formal verifiers use 0D models of space which build on space-point theories as defined in SectionII-A [14][15]. The absence of spatial boundaries in these system models makes it impossible to properly track the interactions between the system elements, especially when they are software-intensive and distributed as in most CPS [16]. In fact, among the five types of spatial theories listed in Section II-A, none of them effectively captures both the mereotopological and non-mereotopological aspects of space for CPS modeling in a practical manner. This observation points to a

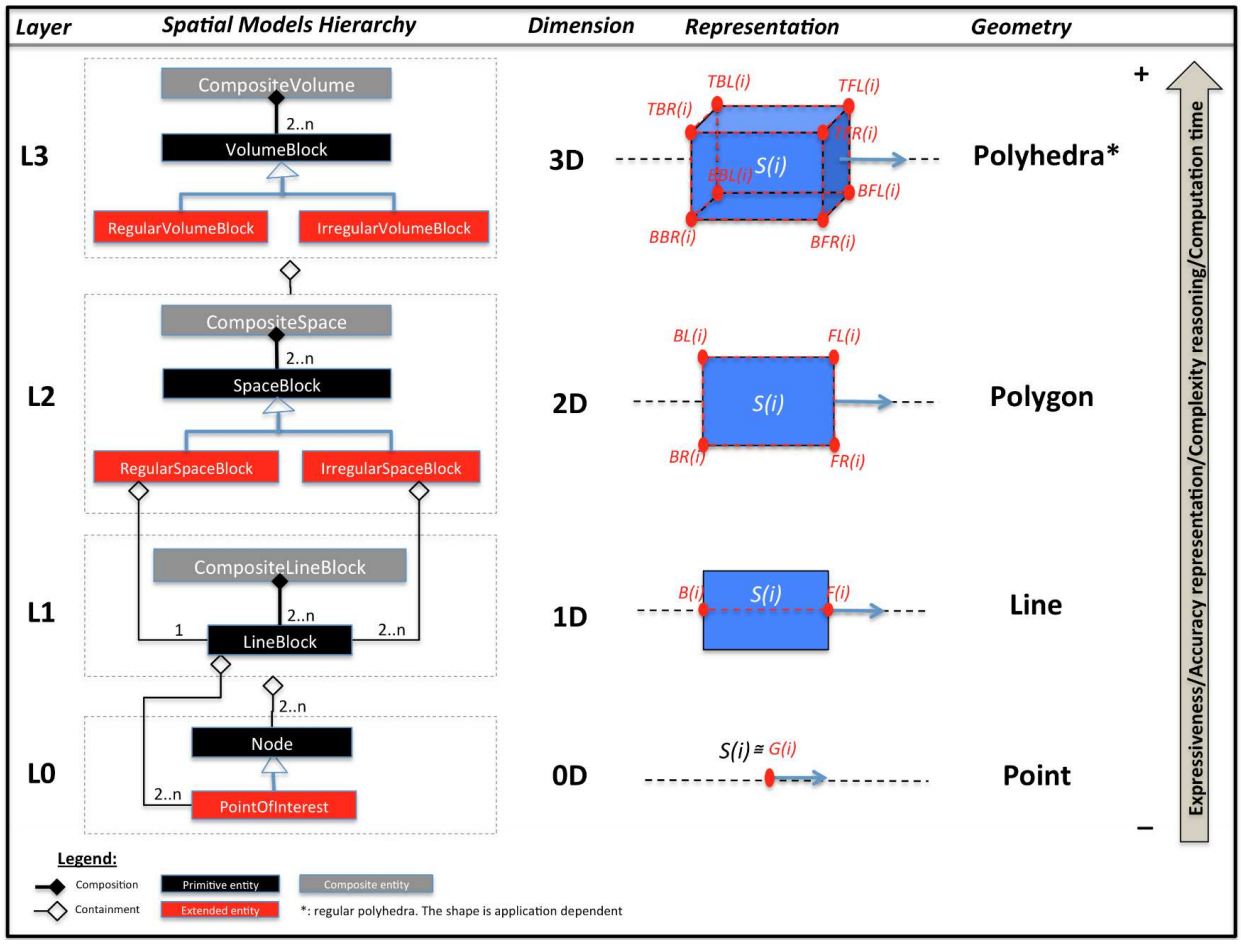

Figure 2. Spatial models hierarchy and representations.

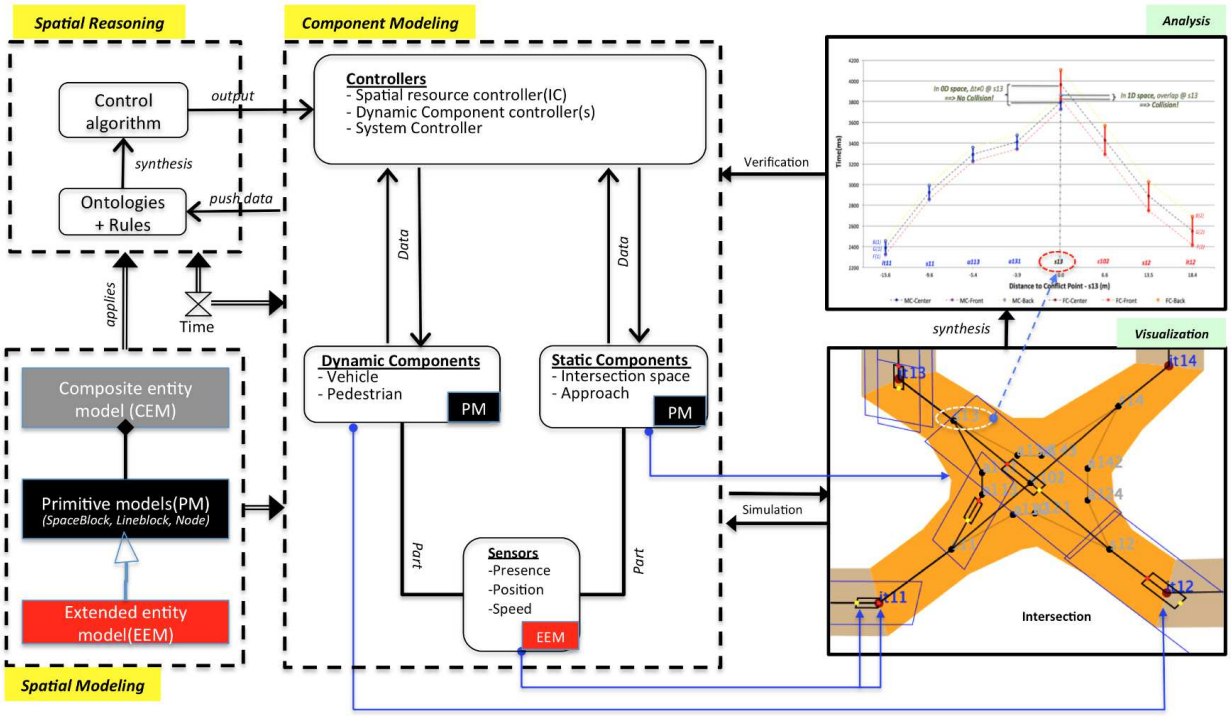

Figure 3. Spatial modeling and reasoning framework extended with views for race track simulation and analysis. The three main elements of the framework are: (1) models of space, (2) models of components, and (3) support for spatial reasoning.

strong need for multidimensional spatial representations and models for CPS, with the primitives specified at the desired granularity of space. To address these challenges, we adopt the region connectedness calculus (RCC), which is a space-region theory.

B. Region Connectedness Calculus (RCC)

Overview. The beauty of Region Connectedness Calculus(RCC) [17] lies in its strong mereotopological focus and flexibility to seamlessly integrate with "low dimension" theories and extension to account for key relevant non-topological aspects such as distance, area, volume and other relevant features. Also, this spatial calculus is precise enough to clearly distinguish convex to concave shapes and it can handle uncertainties in regions' boundaries. Moreover, it provides efficient support to inferencing in static and dynamic situations, a capability critical for qualitative reasoning about motion.

At the core of this algebra is the relationship between spatial regions. Given two spatial regions *S1* and *S2*, a space-point *p* and a proposition ϕ, we might ask a variety of questions over the space domain such as: (1) **Mereological** or part-of questions (e.g., Is the region *S1* a subset of *S1*? Does *p* lie within *S1*? Is the region *S1* equals to *S1*? (2) **Topological** or "connects" questions (e.g., Do intervals *S1* and *S2* meet? Do regions *S1* and *S2* overlap ?) and (3) **Logical** or rules-based questions (e.g., Does the proposition ϕ hold within the region *S1*? If ϕ holds within the region *S1* does it hold within *S2* too?) Cohn [**?**] has identified and specified eight (8) relationships - based on the primitive relation "connection" *C* - between any pair of regions as the core of this Algebra, thus the name RCC-8(there is a RCC-5 version too). Those relationships are illustrated in Figure 1. The excerpt below illustrates the definition of part, overlap and partially overlaps relationships between 2 given regions x and y.

P(x,y) : $\forall z[C(z,x) \rightarrow C(z,y)]$; *x is a part of y*

O(x,y) : $\exists z[P(z,x) \wedge P(z,y)]$; *x overlaps y*

PO(x,y) : $O(x,y) \wedge \neg P(x,y) \wedge \neg P(y,x)$; *x partially overlaps y*

Restrictions. One limitation of RCC is that it does not make a clear distinction between open and closed regions as well as the dimension of spatial regions. On the other hand, results of the composition of spatial primitives from mereological and topological representations can result to multiple possible spatial configurations in the world which can not be properly captured by the reasoner. Thus, we need to add restrictions to RCC models with the primary concern of ensuring decidability of spatial reasoning. Those restrictions include, but are not limited to, closed convex spatial entities with shape as regular as possible. Also, in order to maintain the hyperbolicity property for space-time interactions, we restrict the dimension of space to three (3). However, this constraint keeps unchanged the possibility to navigate to and visualize lower dimension spatial entities. This allows the formulation of restricted axioms which, when expressed in an ontology language, will ensure that spatial reasoning is decidable.

C. System Architecture and Description

In this section, we introduce and briefly describe a new spatial-based modeling and reasoning framework for safety-critical CPS. The system architecture is shown on the left-hand side of Figure 3.

1. Multidimensional Spatial Modeling: This module provides to others the formal model of space in conformance to the spatial theory of interest i.e. restricted RCC-8 in this case. Model entities are organized into an hierarchy of four types of spatial entities enriching each other from top to bottom as shown on Figure 2. However, given that each type of model is from a different dimension, they can each stand by themselves while enabling the representation of spatial entities at various levels of fidelity using OD (point), 1D (line), 2D (polygon) and 3D (polyhedra) representations as shown in the middle of the figure. For each of these representations, a specific type of geometry will ultimately support the encoding and storage of spatial data of the entity subject to analysis and reasoning. A given layer of the hierarchy is typically composed of three types spatial entities as follows.

1. Primitive entity: This is the foundational model of space for the dimension considered. It directly emulates the foundational primitive concept in the restricted spatial theory. Thus, Node, Lineblock, Spaceblock and Volumeblock are respectively translations of point (space-point), and regions in dimensions 1, 2 and 3 in RCC-8.

2. Extended entity: It's an enriched version of the primitive entity with additional non-mereotopological attributes and features that may be particularly relevant for the application of interest. This entity also offers ways to differentiate between model entities of the same dimensions, as seen for 2D and 3D entities.

3. Composite entity: Composite entities are made of the composition of two or more primitive (or extended) entities within the same dimension. The "composition" of spatial entities at a given level implies the composition of lower level entities, if they are part of the top level entity.

The "containment" connector is a weaker "composition" between spatial entities of higher and lower dimensions. It helps define and refine the definition of spatial entities at various level of the hierarchy. Also, the arrow at the right of Figure 2 shows that the expressiveness and accuracy of the spatial model comes at a cost of higher complexity and computation time. Moreover, in spatial systems, the accuracy of computation and control often depends on the number and location of sensors as well as their capabilities. If the sensors are moving, then timeliness of computations will be affected by the velocities of both the sensors and objects moving throughout the environment.

2. Component Modeling: In the context of CPS modeling, spatial models do not stand by themselves. They are enrichment and properties of objects and components in the real world. For instance, a "Vehicle" object can be defined by the properties model, make, usage, maximum speed and owner.

Adding the positional information on its geographical location such as its (x,y,z) geo-coordinates turns it into a spatial object. The decision to "spatialize" components of the CPS is dictated by the purpose of the application, the targeted analyzes and the role they play in the system. Such components are marked with the stamp of the corresponding spatial entity extension as shown by the PM and EEM annotations on the central part of Figure 3. In safety-critical applications, we can categorize the components into dynamic ones to clearly distinguish those components whose location evolve with time from the ones that do not. Sensors are mounted on components (mobile or not) and they have extended entity spatial model stamp. Actuators are left out this component model, however, they can be added as part of the component in the similarly to sensors.

3. Spatial Reasoning: Reasoning occurs at various levels of CPS in support of system control, locally and globally. Thus, both control algorithms and reasoners are an integral part of reasoning in the proposed framework. Irrespective of where it occurs, reasoning involves the inputs, i.e., data from the component module the construction of facts, inferencing of new facts that are synthesized by the controller using the appropriate algorithm. It then generates outputs directly to the appropriate actuator(s) or the lower level controller. The core of the reasoning framework can be expressed using OWL which provides a powerful but still decidable ontology language.

As for the handling of spatial entities during the reasoning process, the formal definition of concepts as per the theory is handled by the Tbox of the DL knowledge base. It contains "terminological" space axioms mostly in the form of mereological and topological types of binary relations (as defined in Section III-B) embedded in the structure of the space ontology. These axioms also provide type definition to spatial objects contained in the Abox which encompasses assertional axioms on the space domain. The rules engine encodes and enforces system-level rules and calculations that affect the domains involved in the CPS behavior. Our framework makes use of rule-based reasoning which encode rules in the form of "if...then" statements.

The spatial reasoner: (1) checks for (un)satisfiability of propositions constructed with the combination of Tbox and Abox elements in order to ensure consistency of the space knowledge base and, (2) infers new relations between input/existing space concepts and objects. Tableau algorithms can be used to test and check for consistency in the database and support the construction of a clash-free tree for input spatial concepts. Put together, those trees compose triple (RDF) graphs of space concepts that can be queried. Triples contained in the graph are of the form Subject-Predicate-Object. Both Subjects and Objects in triples are convex space regions as per and Predicates are fully compatible with RCC-8 specification as defined in Section III-B.

IV. Case Study: Glancing Collision at a Traffic Intersection

A. Overview

To exercise the spatial modeling framework introduce in this paper, we consider the problem of a glancing collision between two smart cars at a non-signalized traffic intersection. We seek to understand how the ontological commitment of the spatial model of the vehicles and their representation affects the outcome of the reasoning process for collision prediction. We approach the problem from a CPS perspective in the sense that each vehicle is a dynamic (physical) object equipped with sensing, computation and communication (cyber) capabilities. For the purposes of this experiment, we assume that both vehicles move at constant but different speeds and they are within sensing range of each other. We have developed a Java-based software platform that interprets the semantic network of 2D spaces adopted by the Open Street Map (OSM) community [18] – as such, the spatial models used in this experiment are at level L2 and lower on the hierarchy of spatial modeling (see Figure 2). With the help of JavaFX, we were able to create and visualize a race track (full details not shown) that preserves the semantic information of space. The right-hand of Figure 3 shows a zoom on the intersection of the track interest for our case study.

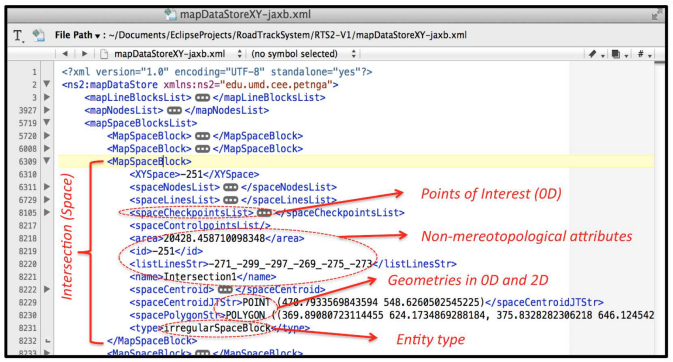

Figure 4. Data view of the model of an intersection as an irregular space block in XML.

B. Space-based reasoning for glancing collision prediction

The three modules of the architecture are implemented as follows.

Component Models. In order to keep the experiment as simple yet explicit enough to maintain the focus on the topic of this research, we consider only 2 vehicles operating in the limited space representing the intersection. Thus, the vehicles are "dynamic" components and the intersection itself is considered a "static" component. Both component types have non-spatial features as illustrated in SectionIII-C. However, each vehicle is assigned a predefined trajectory, both intersecting at the location `s13` in the inside the space occupied by the intersection. Control points are located on the track, at trajectories intersection or curvatures to keep track of the distance of the vehicle to eventual/candidate conflict areas.

Spatial Models. Each of the component types within the system system has a spatial extension. As a case in point, the traffic intersection is modeled as an "IrregularSpaceBlock," which is an extended spatial entity of L2 in the hierarchical model on Figure 2. Figure 4 illustrates the XML representation the intersection1 as an irregular space block. The geometry is a Java Topology Suite (JTS) encoded polygon that defines

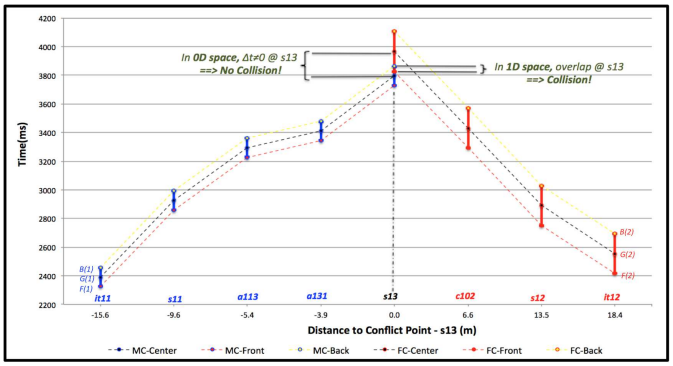

Figure 5. Space-time trajectory for two vehicles on a course of glancing collision.

the precise contour of the intersection as an ordered list of JTS point(in 0D). Also, points of interest (pois) as well as metrics (e.g., area) and features (e.g., name, identifier) can be captured by the model. The dynamic nature of vehicles along with the expected use of its spatial model for reasoning purpose pose a challenge on the choice of the appropriate level of spatial representation needed as explained in Section III-C. This choice affects the effectiveness of the reasoning. For this experiment, a vehicle *i* will be viewed either as: (a) a 2D Point which is the centroid *G(i)* of its shape in 2D, (b) a straight Line connecting its front *F(i)* to its back *B(i)* , or (c) a Polygon(rectangle) represented by its corner points as shown on Figure 2. These geometries correspond to Node (L0), LineBlock (L1) and RegularSpaceBlock(L2) spatial models, respectively. We add position sensors (0D) at those points of interest on the vehicle boundary to track their position in real-time during simulation.

Spatial Reasoning. Given the predefined trajectory of both vehicles, the opportunity for a glancing collision materializes at/around location *s13*. From a spatial perspective, a collision occurs when the spatial representations for vehicles V(1) and V(2) – let's call them S1 and S2 – are predicted to occupy the same location at some point in time. In other words, one of the RCC-8 spatial predicates $PO(S1, S2)$ or $EC(S1, S2)$ will evaluate to true. After assigning a path to each vehicle on the race track and a constant speed, we run the simulation. Figure 5 shows the space-time trajectory of each vehicle. The distance of each control point to the *s13* is computed and normalized with respect to that collision point as reference. In order for the reasoner to predict a collision, it needs the spatial data encapsulated in the geometric representation (spatial model) of the vehicle. When the vehicle geometry is a 2D point, its space-time trajectory is the black dashed line followed by the centroid of each vehicle, i.e., G(1) and G(2). The temporal gap between those two trajectories at *s13* indicates that the two vehicles (will) arrive at the collision point at different instances of time; in other words, no collision. However, if we consider a higher level spatial model for the vehicle, i.e., a straight line by tracking its front and back, we obtain two trajectories for each vehicle. The red one is the trajectory of the front sensor installed at the center point F(i) of the vehicle while the yellow one is the one at the back B(i). The solid straight blue and red lines are the "temporal lengths" of vehicles 1 and 2, respectively. Now we see that the back of vehicle 1 arrives after the front of vehicle 2 and before its back. In other words, vehicle 1 gets to *s13* first and is hit on it right flank by vehicle 2. As such, the 1D model was able to predict a collision that the 0D model was unable to catch.

V. Conclusions

In this paper we have introduced a space-based modeling and reasoning approach to the study of CPS behavior. We have examined the role that spatial ontologies and models can play, and introduced a new multi-dimensional spatial hierarchy and reasoning framework supported by RCC-8. By looking at the problem of collisions at traffic intersections, we have shown that fidelity of spatial models strongly affects the accuracy and prediction of decision making outcomes.

References

[1] L. Petnga and M. A. Austin Ontologies of Time and Time-based Reasoning for MBSE of Cyber-Physical Systems 11th Annual Conference on Systems Engineering Research (CSER 2013), Georgia Institute of Technology, Atlanta, GA, March 19-22, 2013.

[2] S. Borgo, N. Guarino, and C. Masolo Pointless Theory of Space Based On Strong Connection and Congruence L. Carlucci Aiello and S. Shapiro (eds.): Proceedings of KR'96, Principles of Knowledge Representation and Reasoning, San Mateo, CA, USA, pp. 220-229 1996

[3] L. Vieu Spatial Representation and Reasoning in Artificial Intelligence Spatial and Temporal Reasoning, pp 5-41, Ed Springer 1997

[4] J.R. Hobbs DAML Space - An Ontology of Spatial Relations for the Semantic Web Invited Talk, Workshop on the Analysis of Geographic References, Edmonton, Canada 2003

[5] R. Rohrig A Theory of Qualitative Spatial Reasoning based on Order Relations 2nd American Confernce on AI(AAAI-94), pp. 1418-1423 1994

[6] SUMO2014 Suggested Upper Merged Ontology (SUMO) Available at http://http://www.ontologyportal.org/, Accessed on 05/27/14 2014

[7] C. Masolo, S. Borgo, A. Gangemi, N. Guarino, A. Oltramari and L. Schneider WonderWeb Deliverable D17 - The WonderWeb Library of Foundational Ontologies - Preliminary Report IST Project 2001-33052 WonderWeb: Ontology Infrastructure for the Semantic Web, Commission of the European Communities 2003

[8] B. Smith, and P. Grenon The Cornucopia of Formal-Ontological Relations Dialectica, Vol. 58, No. 3, pp. 279 296 2004

[9] W3 See http://www.w3.org/TR/owl-features/, February 2004

[10] J.F. Allen Maintaining Knowledge about Temporal Intervals Communications of the ACM, Vol. 26, No. 11, pp. 832-843 1983

[11] R. Thornton Integrating the Spatial Semantics of Verbs and Prepositions during Sentence Processing The Oxford Handbook of Cognitive Linguistics, 2010.

[12] A. Dillon Spatial-semantics: how users derive shape from information space Journal of the American Society for Information Science, 51(6), 521-528, 2012.

[13] L. Ozgur Spatial Semantics for Concepts Institute for Software Systems (STS), Hamburg University of Technology Hamburg, Germany, 2012.

[14] D. Giannakopoulou NASAs State-Space Exploration: Verifying Safety-Critical Systems CMU / NASA Ames Research Center 2009.

[15] B. Sunanda and P. Seetharamaiah Modeling of Safety-Critical Systems Using Petri Nets ACM SIGSOFT Software Engineering Notes archive, Volume 40 Issue 1, January 2015, pp. 1–7 2015.

[16] N. Leveson Engineering a Safer World: Systems Thinking applied to Safety MIT Press, 2011.

[17] A. Cohn, B. Bennett, J. Gooday, and N. Gotts Qualitative spatial representation and reasoning with the region connection calculus Geoinformatica,1:144, 1997.

[18] Open Street Map OpenStreetMap https://www.openstreetmap.org, Accessed May,14, 2015.