Adding Static and Dynamic Semantics to Building Information Models

Christos Tsigkanos
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Italy

Timo Kehrer
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Italy

Carlo Ghezzi
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Italy

Liliana Pasquale
Lero - the Irish Software Research Centre
Ireland

Bashar Nuseibeh
The Open University & Lero - the Irish Software Research Centre
UK / Ireland

ABSTRACT

Smart cyber-physical spaces indicate spatial environments which include both cyber and physical elements interacting with each other. In the construction industry, Building Information Models are the de facto standard for specifying complex information about building infrastructures, a representation which can also be extended for the specification of cyber-physical spaces. By providing formal static and dynamic semantics in terms of topological concepts of locality and connectivity of entities it is possible to support many forms of advanced analyses typically performed in software engineering. Static semantics aim to broadly support reasoning about latent qualities of a design. Dynamic semantics aim to deal with the dynamism that a space exhibits when additionally considering the ways it may change along with entities inhabiting it. Motivated by the setting of a smart hospital, we show how both qualitative and quantitative properties can be specified and verified.

Keywords

Cyber-Physical Spaces; Building Information Modelling; Formal Verification

1. INTRODUCTION

A cyber-physical system (CPS) is a system where computational elements control and interact with physical entities. A cyber-physical space (CPSp) is special case of a CPS indicating a spatial environment, like a smart building, which includes both cyber and physical elements. The current practice of designing physical spaces is often disconnected from the computational components enabling smart functionalities, a great concern especially in safety-critical spaces such as industrial plants or medical environments. Because computational, communication and behavioural features are increasingly being embedded in physical spaces blurring the boundary between cyber and physical worlds, supporting the design of a CPSp has become particularly challenging [9].

A CPSp brings many of challenges from a software engineering perspective, when considering requirements such as security, safety, or reliability. For example, a bank must guarantee confidentiality of customers information, or a hospital must exhibit specific properties related to medical personnel response times or proximity to critical equipment. Understanding and formally reasoning about a CPSp is thus a key challenge. Although the literature is rich in analysis of complex software systems using formal verification, and rule-based checking methods (expressed as checklists) are widely used in the building construction industry, there is a substantial gap regarding the consideration of cyber and physical aspects in a holistic way. Additionally and most prominently, existing industry standards and practices to describe physical spaces–such as Building Information Modelling (BIM) [3]–lack precise static and dynamic semantics. As a consequence, BIM does not allow any kind of accurate and automated analysis.

To enable rigorous specification and automated analysis as these concepts are commonly understood in software engineering, such semantics needs to be provided. Static semantics aim to broadly support reasoning about latent qualities of a design, while dynamic semantics aim to deal also with the dynamism that the design exhibits while additionally considering the ways it may change.

In previous work [12, 14] we advocated that the topology of cyber and physical spaces–their structure in terms of key elements and their relationships–can provide a system with both structural and semantic awareness of contextual characteristics, especially with respect to security. In this paper, we lift these metaphors to support the design of cyber-physical spaces in the context of smart buildings, in order to facilitate reasoning on a variety of properties such as safety, reliability or security.

The Architecture-Engineering-Construction (AEC) industry has developed Industry Foundation Classes [7] (IFC) as

SEsCPS@ICSE '16 May 16 2016, Austin, Texas, USA

DOI: http://dx.doi.org/10.1145/2897035.2897042

a standard encoding BIM models, which consists of building elements in terms of their geometric and functional attributes and relationships; hereafter referred to as BIM/IFC. Starting from a BIM/IFC description of a physical space augmented with cyber-physical entities, we provide its formal semantics in terms of a *bigraph* [10]. A bigraph has two constituents: a set of trees (a forest), capturing notions of spatial locality through containment, and a hypergraph modelling linking relations among nodes. Static requirements can then be represented as bigraphical matching properties expressing configurations of interest. Regarding dynamics, possible actions that can occur in the space and change its topology are expressed as reaction rules that replace a matched portion of a bigraph with another one, yielding a Bigraphical Reactive System (BRS). Having obtained such a system, we show how analysis can be enabled through formal verification. We motivate and illustrate our approach using a substantive example concerned with safety and reliability in a smart hospital environment [11].

The rest of the paper is structured as follows. We start in Section 2 with a summary of relevant related work. Section 3 describes our motivating example and gives a brief overview of our approach. Section 4 introduces BIM/IFC as the de facto industry standard, and how it can give rise to modelling of smart spaces; Section 5 refers to its static semantics in terms of bigraphs, while Section 6 presents the form of BRS that we have used to provide dynamic semantics to cyber-physical models of space. Section 7 concludes the paper along with an outlook on future work.

2. RELATED WORK

The current state of the art in the design of spatial environments mostly focuses on supporting the specification of physical layouts and structural elements. A typical case is a CAD environment through which traditional blueprints are produced. One can specify how a space is divided into rooms, the thickness of walls, doors connecting rooms, plumbing elements, etc. To go beyond purely "syntactic" spatial descriptions, human-driven processes may be defined to guide designers and inspectors to review and assess the design. To support assurance, conformance to standards or regulations is currently performed in the AEC industry through rule-based checking. Automation of rule checking of BIM/IFC building representations have concentrated on building regulations and accessibility criteria, and have been integrated in several architectural tools [4]. Such rule-based systems assess building designs according to various criteria, expressed as rules, constraints or conditions. However, such checks do not consider the topology inherent in the space, nor how the building model might change.

In [8], the topology of spatial configurations is extracted from building information models and represented as graphs, which are used for indexing and querying spatial configurations along with architectural sketches, to support early design activities. Analyses such as similarity checking are performed on the static representation of buildings, and are based on adjacency and access relationships. Focusing on security reasoning while aiming at early design phases, Porter et al. [13] propose a method and heuristics to discover security threats on building specifications via simulation, utilizing BIM. The BIM/IFC graph interpretation we employ for static mapping of BIM/IFC specifications is similar to [8] and [13]; however we further consider different topological relationships such as containment and connectivity, and our semantic domain is a process meta-calculus within which we provide also dynamic semantics and support reasoning on qualitative and quantitative requirements.

3. MOTIVATION

Our motivation lies in the setting of smart spaces; it showcases the need for providing static and dynamic semantics for Building Information Models, enabling automated analysis that is not covered by state of the art, through a modelling formalism that captures the topology of the cyber-physical space.

3.1 Example

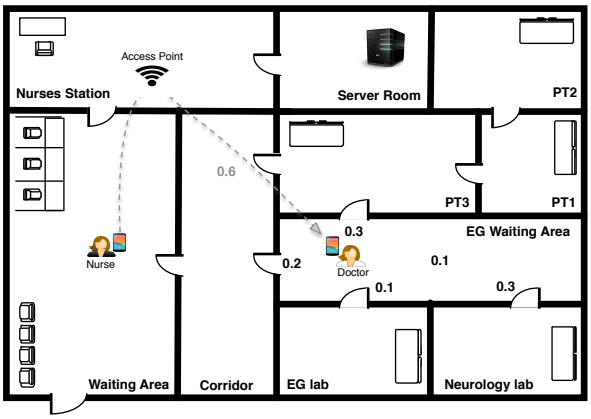

Figure 1: Cyber-physical space of a smart hospital.

A hospital environment has a complex structure. In the physical dimension, it consists of a building or even of a set of buildings on a larger area that comprise a complex spatial infrastructure, along with people (i.e. agents) with various roles as well as medical equipment. In Figure 1, a simplified version of a floor plan consists of various rooms such as a nurses station and medical-purpose areas, in which a doctor and nurse move. This plan is an intermediary design. In the cyber dimension, medical equipment or mobile devices used by doctors and staff form networks, on which patient information may also flow. In the following, we ignore construction-specifics (such as materials, dimensions, etc.), and consider a topology-driven approach; we are interested in relationships inherent in the space, be it between building entities, people or assets.

Designers have to satisfy a multitude of domain-specific requirements in their design of a smart hospital, while complying with existing building regulations. In fact, complex functional relationships between various entities must be taken into account. For instance, based on space planning criteria [15], an electroencephalography laboratory must not be adjacent to a room containing radiology equipment or a machine room, to avoid critical device interference; however it must be directly adjacent to neurology clinical facilities. We regard this as a simplified safety requirement that a design of a smart hospital must satisfy (R1).

A designer should also take into account how the space may be utilized; in this case, one must consider people moving around, such as nurses or doctors tending to patients

or emergency personnel providing services. In this context, a smart hospital under design should exhibit specific properties expressing temporal and spatial concerns. A typical scenario of interest involves a nurse needing to contact a doctor for an emergency [11]. She has two options, namely to a) page the doctor through the network with her mobile device or b) physically locate her inside the hospital.

A reliability requirement is thus that the nurse must be always able to reach the doctor (physically or through the network) within a timeframe[1], with at least a certain probability (R2). Regarding option a), we have to consider that access points have variable range, especially since they must not be placed near sensitive medical equipment; in Figure 1, an access point is placed in the nurses station. Coverage varies in the rooms of the hospital, and wireless connections are associated with a success probability; a design assumption is that the signal can not be strengthened. Regarding option b), we have to be aware of the fact that the doctor and the nurse may always move inside the hospital, e.g. attending to patients. Specifically, in each room, they may move to any door-adjacent room, or stay in the room. Moves may be associated with probabilities, perhaps from access logs or domain observations (the doctor may be more likely to be attending the EG lab, for instance). To locate the doctor physically, the nurse must exhaustively search rooms until she finds her. Knowing that she is more likely to find the doctor in some hospital areas, she employs a search strategy, so her moves inside the physical space are also associated with probabilities. Agent behaviours are assumed to be independent.

We can conclude from the above discussion that satisfaction of requirement R2 depends on the design of the floor plan, the wireless signal coverage, and the probabilities associated with the moves of the doctor and the nurse in the physical space.

Overall, we consider two requirements of the cyber-physical space induced by the smart hospital:

- *Safety*: An electroencephalography laboratory must not be adjacent to a room containing radiology equipment or a machine room while it must be adjacent to a neurology lab (R1).
- *Reliability*: An attending doctor must be reached by a nurse either physically or through her mobile device with a probability of at least 60%, within 8 time units (R2).

3.2 Approach Overview

The approach proposed in this paper can be realized as illustrated in Figure 2. The physical space is designed using a CAD tool as is customary. Subsequently, as the BIM/IFC standard allows new custom objects (along with attributes) to be defined using the same interface, the designer also includes physical entities of the smart space (e.g., agents or devices) in the design, placing them as desired. This allocation aims to include domain-specifics of the smart space that will be submitted for analysis, and renders the approach open to further extensions. The resulting output is a BIM/IFC representation of the physical dimension of the smart space of the design at hand, which is subsequently enriched with purely cyber entities and connectivity they may exhibit. What follows is the specification of requirements; properties of interest are specified as discussed in Sections 5-6. Should dynamic analysis be required, change primitives are also specified (Section 6).

[1]For simplicity, time is considered as discrete steps of movement or paging.

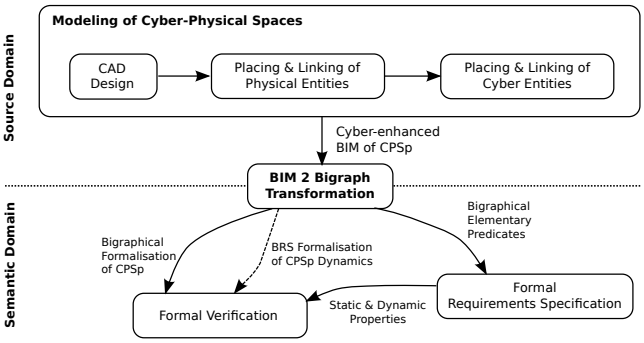

Figure 2: Overview of the approach.

4. MODELLING CYBER-PHYSICAL SPACES

BIM and software for the construction industry provide rich representations of structural and functional characteristics of buildings. The Industry Foundation Classes (IFC) [7] has become the de-facto standard to exchange BIM models for the planning, design, construction, and maintenance of physical spaces. Figure 3 shows a simplified IFC meta-model highlighting structural entities and relationships deemed relevant for our analysis. Some intermediate relationships between entities were also omitted for reasons of clarity (represented as dotted lines in Figure 3).

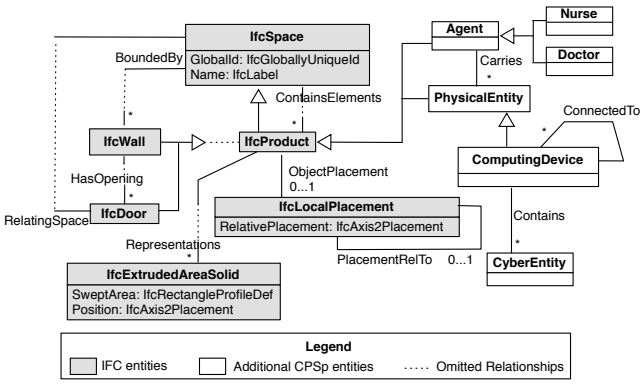

Figure 3: Extended IFC meta-model for cyber-physical spaces.

A building is represented as a collection of rooms, each of them represented as an *IfcProduct* element characterised by a name and an identifier inherited from *IfcSpace*. A room can also include other building structural elements (e.g., rooms, walls, furniture) as described by the relationship *ContainsElement* brought by *IfcSpace*. Each room can be bounded by walls (*IfcWall*), which in turn can have opening points, each of them indicating the presence of a door (*IfcDoor*). Each door allows accessibility to another room or area, as indicated by the *RelatingSpace* relationship. A building structural element (*IfcProduct*) is also characterised

by its location (*ObjectPlacement* relationship). In particular, *IfcLocalPlacement* defines the relative placement of an element in relation to the placement of other spaces that may contain it (*PlacementRelTo* relationship). Each building structural element can also be associated with a set of graphical representations. For example, for this work we assumed that each room has a rectangular shape described by the property *SweptArea* of the *IfcExtrudedAreaSolid* entity.

We represent additional cyber and physical entities that are not fully supported in IFC. In particular, we extend *IfcProduct* to represent agents (e.g. the doctor and nurse) and physical entities that do not constitute building structural elements (e.g. the server). Both agents and physical entities can be characterised by their location in the physical space, as indicated by the *ObjectPlacement* relationship inherited from *IfcProduct*. Agents can carry physical entities such as mobile devices and can be associated with a set of roles. We specify *ComputingDevices*, such as servers, pagers, or access points. These are particular types of physical entities that can store or execute *CyberEntities*, such as files or applications, and can connect to other devices. Please note that specific entity types, such as *Doctor* and *Nurse* being defined as subtypes of *Agent*, are not shown in Figure 3 due to space limitations. Moreover, attribute declarations are omitted for all entity types defined as IFC extensions.

5. STATIC SEMANTICS

A modelling formalism expressing the semantics of building information models and their topological relationships should allow the representation of the structure of spaces and the linking among entities in the space; essentially the semantic domain of our approach. In this section, the static semantics of BIM/IFC specifications is given in terms of *bigraphs* [10]. This transformation can be automated, and the resulting bigraph representation is uniquely defined.

5.1 Bigraphs as the Semantic Domain

Bigraphs are an emerging formalism for structures in ubiquitous computing, consisting of two graphs. A *place graph* is a forest, a set of rooted trees defined over a set of nodes. A *link graph* is a hypergraph over the same set of nodes and a set of edges, each linking any number of nodes to names; this graph represents generic many-to-many relationships. Connections of an edge with nodes are called ports. Place and link graphs are orthogonal, and edges between nodes can cross locality boundaries. What follows is an informal presentation; the interested reader is referred to [10] for complete definitions and proofs of the bigraphical theory.

$P.Q$	*Nesting* (P *contains* Q)	(1a)
$P \mid Q$	*Juxtaposition of nodes*	(1b)
$-_i$	*Site numbered* i	(1c)
$K_w.(U)$	*Node with control* K *having ports with names in* w. K *contains* U	(1d)
$W \parallel R$	*Juxtaposition of bigraphs*	(1e)

Bigraphs can be described through concise algebraic expressions (Formulae 1a-1e), in a process calculi fashion. The containment relationship is expressed in Formula 1a. Bigraphs can contain sites (Formula 1c) that can be used to denote placeholders; sites can be used to indicate presence of unspecified nodes. Controls are names that define a node's type; each node control can be associated with a number of named ports. P, Q, and U are controls of bigraph nodes. If a single instance node of that type exists in the bigraph, the control also uniquely identifies that node. Otherwise, port names are used as a way to uniquely identify it. In Formula 1d the node identified by control K and port name w also contains U. Ports that appear in a formula with the same name are connected, forming a hyperedge with that name, called *link* in the sequel. Bigraphs can be contained in roots that delimit different hierarchical structures; in Formula 1e, W and R are different roots.

5.2 Inferring Topology from BIM/IFC

Our objective is expressing topological information inherent in a BIM/IFC specification through locality (expressed as containment) and linking relations, mapping it to a bigraph placing and linking structure. IFC entities as well as additional cyber and physical entities are mapped to bigraph nodes. The entity type (e.g. IfcDoor, IfcWall, Server, etc.) is used to identify node controls[2], while the entity name corresponds to a port name uniquely identifying it. The placing structure of the physical space is obtained by juxtaposing all the rooms in a building and subsequently nesting in each room nodes corresponding to entities contained in that room. For a wall, more than one node is created; each is nested inside nodes representing the rooms that wall bounds. Similarly, two nodes are created for each door; these are nested inside the nodes representing the rooms that door connects. For example, the smart hospital of Figure 1 will be represented as a juxtaposition of rooms as partially shown in Formula 2. The $Server$, a physical entity, is contained in the server room.

$$Hospital.(Room_{nrs}.(-_0) \mid Room_{srv}.(Server) \mid -_1) \tag{2}$$

To populate the linking structure, connectivity relations in the space, which can be either physical or digital are obtained. In the physical space, connectivity refers to adjacency relations of physical entities. For example, to connect a room to another one via a door, a *Door* node is placed in the corresponding *Room*. The port of this *Door* is then linked to the respective *Door* node contained in the *Room* the door leads to. Analogously, rooms can be connected by walls; in Formula 3, the EG lab *Room* is connected to the Neurology lab *Room* through $Wall_q$.

$$\begin{aligned} &Room_{nrs}.(AP_{wlan}|-_0) \mid Room_{eg\_wtg}.(Doctor.(Pager_{wlan})|-_3) \\ &\mid Room_{nlg}.(Door_x \mid Wall_q|-_1) \mid Room_{eg}.(Wall_q|-_2) \end{aligned} \tag{3}$$

The semantic correspondence of connectivity and the real-world phenomena it represents is not stated explicitly; it is assumed that it is recorded separately as part of the model documentation, as the designer may choose to reason on various manifestations of connectivity (such as windows versus doors). Nevertheless, all connectivity information inherent to the IFC specification is mapped to the bigraphical representation.

Just like standard BIM/IFC and other physical entities, cyber entities are treated in the same way in the bigraphical

[2]For brevity, we will hereafter omit the prefix "Ifc" for all standard IFC entity types, i.e. use controls *Door*, *Wall*, etc.

representation, using the same notions of containment and connectivity. For instance, a server (a physical entity) being placed in the physical space may contain a cyber entity, e.g. a file representing patient's information. Logical connections between entities in the cyber space also have a correspondence in the linking structure. This may refer to wireless signals forming networks; in Formula 3, the ports named *wlan* link the access point AP and the doctor's $Pager$.

Finally, attributes of IFC objects are also mapped to the bigraphical representation. The general procedure for the treatment of IFC attributes is to create an *Attributes* node inside a node. Such an *Attributes* node serves as a container where attribute keys are represented as inner nodes; each of them is linked to a name representing the attribute value. In cases where attributes are of minor interest they can be abstracted by sites, as for example in Formulae 2 and 3.

5.3 Properties of a CPSp Configuration

A property of a given cyber-physical space can also be expressed as a bigraph. A configuration described by a bigraph satisfies a property if the bigraph specifying the property can be matched against it, meaning that it exhibits containment and connectivity relations among entities as desired. Failure of matching the bigraph representing the property means instead that the property is not satisfied. The utilization of sites in the bigraph specifying the property indicates that the portion of the configuration that matches a site does not affect satisfaction. For example, given that variables x and q range over names, utilising boolean connectives and elementary predicates expressed in terms of bigraphs, the property which formally specifies the example's safety requirement R1 has the following form:

$$\mathbf{R1}: Room_{eg}.-_0 \Rightarrow Room_{eg}.(Door_q|-_1)|Room_{nlg}.(Door_q|-_2)\wedge$$
$$\neg\big(Room_{eg}.(Wall_q|-_3)|Room_x.(Wall_q|HeavyMachinery|-_4)$$
$$\vee\ Room_{eg}.(Wall_q|-_5)|Room_x.(RadioEquipment|Wall_q|-_6)\big) \quad (4)$$

Formula 4 states that should an electroencephalography *Room* exist in the model under consideration, it must not share a wall with any *Room* containing radiology equipment or heavy machinery (signified by controls *RadioEquipment* and $HeavyMachinery$, respectively); however it should be connected through a *Door* to a neurology *Room*. Due to presence of sites in the property specification, other entities that may be contained in rooms do not affect satisfaction. Satisfaction of such a property is checked automatically through bigraph matching [1, 10]. For the example of Figure 1 matching will fail, as there is no door connecting the EG room with the neurology room; the designer must re-arrange the space.

Note that configurations that reflect properties of a physical design can also be specified by providing a BIM/IFC specification which is automatically translated to its bigraph representation, as previously showed.

6. ADDING DYNAMIC SEMANTICS

Having defined how bigraphs provide topology-driven static semantics of cyber-physical spaces, we proceed to consider how these spaces may change, thus giving rise to dynamic behaviour. This is reflected by Bigraphical Reactive Systems (BRS) [10], which extend bigraphs by adding reaction rules defining possible reconfigurations. Reaction rules are parametric and specify how a bigraph can be modified by selectively rewriting some of its portions. Reaction rules have the general form of $R \rightarrow R'$, where R is a redex and R' is a reactum; both the redex and reactum are bigraphs. In particular, if a part of a bigraph that matches the redex is identified, it can be replaced with the reactum, in a fashion similar to graph rewriting. A BRS allows us to describe possible ways in which cyber and physical spaces can evolve through reaction rules. For instance, a fundamental reaction from the scenario presented in Section 3 is the ability to allow a doctor to enter a room in the hospital, when next to a door leading to it.

$$Room_r.(Doctor.-_0 \mid Door_x \mid -_1) \mid Room_v.(Door_x \mid -_2) \rightarrow$$
$$Room_r.(Door_x \mid -_1)|Room_v.(Door_x \mid Doctor.-_0|-_2) \quad (5)$$

As Formula 5 illustrates, utilising the parameter matching facilities of the formalism through sites, the *Doctor* moves into $Room_v$, while other entities contained in the *Doctor* (such as her pager) or the adjacent $Room_r$ are not modified. Variables r, x, v appearing in reaction formulae range over names. In the same fashion, we can specify a reaction that models the $Nurse$ paging the doctor through the access point AP located in the nurses station, resulting in a configuration where a token (PNG) is contained in the doctor's pager:

$$Room_r.(Nurse|AP_{wlan}|-_0)|Room_v.(Doctor.(Pager_{wlan})|-_1) \rightarrow$$
$$Room_r.(Nurse|AP_{wlan}|-_0)|Room_v.(Doctor.(Pager_{wlan}.(PNG))|-_1)$$

Essentially, using the reaction mechanism, the building designer provides elementary reconfigurations reflecting change primitives desired for the analysis required. These can include, for instance, people moving inside the physical space or establishing connections between devices interacting in the cyber-space. Definition of the dynamics of a physical space can also be specified by the designer in her standard architectural tool environment, by specifying redexes and reactums along with custom BIM/IFC entities, as shown in Figure 2. The specifications corresponding to redexes and reactums can be then translated to their corresponding bigraph representation[3].

Having obtained a BRS describing the dynamics of a CPSp along with a bigraph describing the configuration of the space, a wide range of analyses can be performed by interpreting the BRS over some form of a Labelled Transition System [2], a modelling formalism that describes systems and their evolution in terms of states and transitions. States specify configurations of the system, while transitions describe how configurations can change by moving from states to their successors. Given a bigraph that describes the initial configuration, the system evolves by applying reaction rules, which model the occurence of possible actions in the CPSp, generating new configurations. At each step, several applications of reaction rules may be possible, thus branching off new possible configurations.

6.1 Enabling Analysis of CPSp Dynamics

Having defined how dynamics can be expressed with BRS, in this section we focus on the analysis of the cyber-physical space regarding the reliability requirement R2, given the assumptions outlined in Section 3. Conceptually, our strategy

[3]This refers to the initial step; sites serving as placeholders will be added in reaction rules of the BRS.

will consist of modelling the behaviour of individual agents, and of subsequently composing these models to generate a model for the complete system, which will be used for analysis. More precisely, analysis will be performed through an interpretation of the BRS description over a form of a Labelled Transition System (LTS) [2] with probabilities on transitions, enabling reasoning with a probabilistic branching temporal logic.

Agent behaviour consists of the dynamics that an agent can exhibit, corresponding to reactions defined in the BRS. For instance, recall that the moves of the doctor inside the hospital are associated with probabilities, reflecting the likelihood that she enters a specific room from a given one. This (fully probabilistic) behaviour can be captured with a Discrete-Time Markov Chain [2] (DTMC), a discrete-time transition system with discrete probability distributions.

In Figure 4, a DTMC partially represents the doctors behaviour, where probabilities are indicated by grey labels on transitions. For example, if the doctor is in the EG Waiting Area (state a), she may either stay inside with probability 0.1, enter the patient room PT3 (state b) with probability 0.3, or enter the Neurology lab, corridor or EG Lab with probabilities 0.3, 0.2 and 0.1 respectively. For each state of the DTMC, atomic propositions label the state, declaratively representing the bigraphical configuration of the state; state a in Figure 4 represents the bigraphical configuration of Figure 1. The configuration evolves as the doctor probabilistically moves inside the physical space[4].

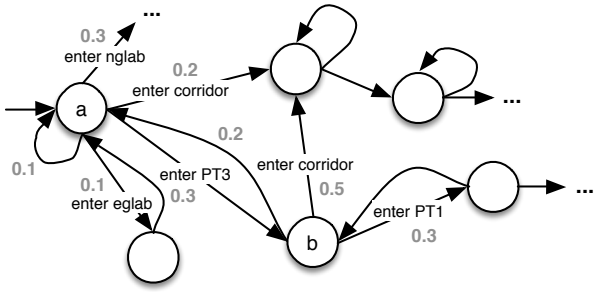

Figure 4: Fragment of doctor's DTMC.

System behaviour refers to the collective behaviour of the agents in the CPSp that can be conceived as a system in which processes operate concurrently and asynchronously. The overall model of the system will be a parallel composition of DTMC models representing the behaviour of individual agents, reflecting the fact that agents may freely perform actions (from the ones available to them) at any time. This will introduce non-deterministic *choices* in the model, yielding a Markov Decision Process (MDP) [6].

The probabilistic distributions that describe behavior of individual agents are independent. The non-determinism characteristic of the system model appears in a state when two different agents perform probabilistic actions and independently change their states; their distributions are essentially in conflict. The overall behaviour of the system will be defined by the concurrent execution of all agents and captured by the MDP. In each state, a non-deterministic *choice* occurs between several discrete probability distributions of agent's moves to successor states. Figure 5 shows a fragment of the MDP generated from the parallel composition of DTMCs corresponding to the doctor's and the nurse's moves (dotted transitions) inside the CPSp; state *a* represents the bigraphical configuration of Figure 1 as the initial state, while state b represents the configuration where the doctor moved to PT3 while the nurse stayed in the waiting area. State c corresponds to a configuration resulting from a successful paging operation by the nurse, while state d where she entered the corridor. Note that as bigraphical predicates encode configurations in each state, states labelled b in Figures 4 and 5 represent the same configuration.

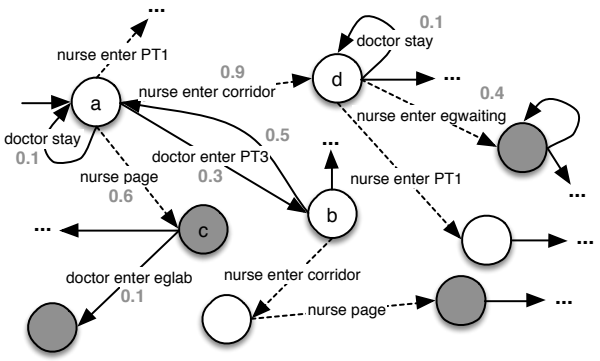

Figure 5: Fragment of system's MDP.

6.2 Verification of a Reliability Property

The MDP formalism enables automated analysis of a wide range of quantitative properties specified through a probabilistic temporal logic. Probabilistic Computation Tree Logic (PCTL) [5] is such a branching time logic which extends CTL [2] with a probabilistic operator, manifested as quantitative extensions of CTL's *all* (A) and *exists* (E) operators. Model checking for PCTL involves determining states of an MDP satisfying a PCTL formula.

$$\mathbf{R2} : emergency \Rightarrow ([P_{\geq 0.6} F^{\leq 8} Nurse|Doctor.{-_0}] \vee [P_{\geq 0.6}\ F^{\leq 8}\ Doctor.(Pager_{lnk}.(PNG))] \quad (6)$$

Formula 6 specifies reliability requirement R2, to be evaluated over MDP $\mathcal{M}$ describing the probabilistic evolution of the CPSp, where elementary predicates are expressed in terms of bigraphical configurations. In Figure 5 states where elementary predicates $Doctor.(Pager_{lnk}.(PNG))$ or $Nurse|Doctor.{-_0}$ are true, are shown in dark grey. Essentially, Formula 6 expresses that if an emergency occurs, then either the nurse is co-located with the doctor within 8 steps with probability 0.6 in the physical space or a ping successfully reaches the doctor's pager with probability 0.6. Reliability requirement R2 regarding the physical space as reflected in Formula 6, is violated in the configuration of Figure 1. However, even minute changes in the design of the floor plan can have effects on requirement satisfaction in non-trivial ways. For example, merging patient rooms PT1 and PT2 would render property R2 satisfied.

[4]A full BIM/IFC specification, bigraphical and Markov models of the example can be found at home.deib.polimi.it/tsigkanos/smarthospital/.

6.3 Towards Designer Feedback

The evaluation of Formula 6 over MDP $\mathcal{M}$ through model checking for all states of the model gives some preliminary insights; the designer can receive states belonging to the evolution of the configuration, where the property is not satisfied and can change the design accordingly. However, this form of feedback is limited for understanding, as it corresponds only to a list of configurations.

Verifying properties as described above is useful to check satisfaction of requirements for designs modelled along with dynamics they exhibit when deployed. Observe that the dynamics presented in this paper reflected how the space may be actually utilized; for the smart hospital example, this included medical personnel moving inside or paging through the wireless network. However, this type of modelling and analysis does not provide insights on how the design of the space should actually be modified to ensure requirements satisfaction; this feature is essential for design process integration. To this purpose, the dynamics defined must also include operations that the designer performs when editing the model in her standard architectural tool environment (assuming changes lead to syntactically valid models). These should include action primitives that the designer may perform to alter a configuration, such as adding a door, placing or moving entities. By modelling design-time operations, state exploration can be utilized for the purpose of finding sequences of such edit operations that can modify a model under construction as to exhibit no requirement violations.

7. CONCLUSIONS & OUTLOOK

To facilitate the design and engineering of smart cyber-physical spaces, we proposed static and dynamic semantics of such composite spaces in terms of topological concepts of locality and connectivity of entities, giving rise to opportunities for a number of advanced analyses. In particular, starting from a BIM/IFC description of a physical space, we provided its semantics in terms of a *bigraph* which is also enriched with the cyber dimension of the space. We showed how static requirements can be represented as bigraphical matching properties expressing configurations of interest, while possible change primitives occuring in the space can be expressed as reaction rules. Having obtained such a system, we show how analysis can be enabled through formal verification. In particular, we showcased how properties both qualitative (in the form of static matching properties) and quantitative (e.g. over DTMCs/MDPs), in a smart CPSp setting can be verified.

We have identified and are pursuing a number of promising avenues for investigation. Firstly, an identification of appropriate formalisms to reason on requirements particular for smart cyber-physical spaces would be advantageous, as so far extensive formal verification practices have not been considered in the current state of the art in the AEC industry. Secondly, regarding the design phase of the engineering of smart spaces, a high-level mechanism along with graphical interfaces to specify dynamism at the BIM/IFC level would be desired to lower the technological barrier of entry. Towards effective designer feedback, a transformation mechanism from a bigraphical model back to a BIM representation would be useful to facilitate use by practitioners. Moreover, techniques utilizing synthesis or reasoning with incomplete models are also highly relevant, as they can provide insights during the early design process. Finally, in order to enable experiments and evaluate the approach by involving real users and domain experts, we plan to integrate our approach in a toolchain along with existing state of the art software used in the AEC industry.

8. ACKNOWLEDGMENTS

This work was partially supported by ERC Advanced Grants no. 227977 (SMScom) and no. 291652 (ASAP) and Science Foundation Ireland grants 10/CE/I1855 and 13/RC/2094.

9. REFERENCES

[1] L. Birkedal, T. C. Damgaard, A. J. Glenstrup, and R. Milner. Matching of Bigraphs. *Electronic Notes in Theoretical Computer Science*, 175(4):3–19, 2007.

[2] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model checking*. MIT press, 1999.

[3] C. Eastman, C. M. Eastman, P. Teicholz, and R. Sacks. *BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors*. J.W & S, 2011.

[4] C. Eastman, J.-m. Lee, Y.-s. Jeong, and J.-k. Lee. Automatic rule-based checking of building designs. *Automation in Construction*, 18(8):1011–1033, 2009.

[5] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal aspects of computing*, 6(5):512–535, 1994.

[6] H. Hermanns. Interactive markov chains: The quest for quantified quality, volume 2428 of lncs, 2002.

[7] ISO 16739. Industry Foundation Classes (IFC): Data Sharing in the Construction and Facility Management Industries. iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51622, 2013.

[8] C. Langenhan, M. Weber, M. Liwicki, F. Petzold, and A. Dengel. Graph-based retrieval of building information models for supporting the early design stages. *Advanced Engineering Informatics*, 27(4):413–426, 2013.

[9] E. A. Lee. Cyber Physical Systems: Design Challenges. Technical report, EECS Department, University of California, Berkeley, 2008.

[10] R. Milner. *The Space and Motion of Communicating Agents*. Cambridge University Press, 2009.

[11] H. Nakashima, H. Aghajan, and J. C. Augusto. *Handbook of ambient intelligence and smart environments*. Springer Science & Buss. Media, 2009.

[12] L. Pasquale, C. Ghezzi, C. Menghi, C. Tsigkanos, and B. Nuseibeh. Topology Aware Adaptive Security. In *Proc. of the 9th Int. Symp. on Software Engineering for Adaptive and Self-Managing Systems*, 2014.

[13] S. Porter, T. Tan, T. Tan, and G. West. Breaking into bim: Performing static and dynamic security analysis with the aid of bim. *Automation in Construction*, 40:84–95, 2014.

[14] C. Tsigkanos, L. Pasquale, C. Menghi, C. Ghezzi, and B. Nuseibeh. Engineering Topology Aware Adaptive Security: Preventing Requirements Violations at Runtime. In *Proc. of the 22nd Int. Requirements Engineering Conf.*, pages 203–212, 2014.

[15] US Department of Veterans Affairs, Veterans Health Administration. PG-18-9 Space Planning Criteria, Electroencephalography Laboratory Functional Relationships. cfm.va.gov/til/space/SPchapter226.pdf.