A Multidimensional Approach for Formal Modeling and Analyzing Medical Cyber-Physical Systems

Ayoub Bouheroum
ICOSI Laboratory, Khenchela University, Khenchela, Algeria
ayoub.bouheroum@univ-khenchela.dz (corresponding author)

Djamel Benmerzoug
LIRE Laboratory, Constantine 2-Abdelhamid Mehri University, Constantine, Algeria
djamel.benmerzoug@univ-constantine2.dz

Sofiane Mounine Hemam
ICOSI Laboratory, Khenchela University, Khenchela, Algeria
hemam.sofiane@univ-khenchela.dz

Faiza Belala
LIRE Laboratory, Constantine 2-Abdelhamid Mehri University, Constantine, Algeria
faiza.belala@univ-constantine2.dz

Received: 18 November 2024 | Revised: 22 December 2024 | Accepted: 29 December 2024

 DOI: https://doi.org/10.48084/etasr.9646

ABSTRACT

The combination of integrated software controlling devices, networking capabilities, and sensing/actuation technologies in Medical Cyber-Physical Systems (M-CPS) highlights some specific research challenges. The major challenge is to formally ensure the confidentiality of the data or resources they handle. This study tackles this problem by proposing a formal approach that combines CA-BRS (Control Agent and Bigraphical Reactive Systems) and BPMN (Business Process Model Notation) to specify and analyze CPS in general, while respecting several dimensions. The structural dimension of the CPS, representing the space (physical and cyber entities) in which agents exist and interact, is defined with BRS. Control agents constitute the virtual dimension and observe and control the physical and cyber entities of their environment. The complex and adaptive behavior of CPS (behavioral dimension) is defined through several types of rules, each managing a possible evolution of a CPS component (physical, cyber, or virtual). Two distinctive perspectives are associated with the semantic interpretation of these rules: the states perspective and the activities perspective. This study focuses on the activities perspective that specifies the behavior of control agents with a BPMN activity diagram. This highlights how these two models (CA-BRS and BPMN) complement each other to assist the designer in defining formal models for CPS. Additionally, it reveals how to provide the CA-BRS model with means to control unauthorized access to an electronic health record system.

Keywords-access control; BPMN; BRS; formal models; medical CPS

I. INTRODUCTION

Cyber-Physical Systems (CPS) are now coming into widespread use and are controlling many different aspects of daily life, from homes to safety-critical infrastructures such as transportation, healthcare, and industry 4.0, making it important to formally model them. However, complex and contextual systems that integrate computing and communication capabilities with the dynamics of physical and engineered systems, which also sense and adapt to environmental aspects, are difficult to model and verify across all dimensions [1, 2]. Formal modeling is also notoriously difficult, especially since defined models must account for unpredictable behavior as well as the complex computation of CPS. A broad range of notations and formalisms are exploited to effectively model a CPS, including hardware, software, communication, data, control, security, and operational aspects. CPS design, focusing on the expression and use of these models, can improve their reliability and security. Thus, formal modeling becomes even more challenging but also necessary.

This study approaches the design of a given CPS by first defining its formal model while considering a set of scenarios that explain its secure behavior. Then, a simulation of these scenarios is carried out based on BPMN models, validating the CPS behavior in a controlled environment. The refinement of the proposed formal models, based on the insights gained from the simulation results, allows iterating through the model, simulation, and analysis processes until achieving the desired accuracy and reliability. The ultimate aim is to explore a new approach to CPS modeling and investigate the interactions between software and security engineering. This has raised several fascinating research challenges and opportunities. There is much to be gained by defining models and notations to integrate security policy specification into the Medical CPS (M-CPS) modeling process, specifically by using adequate formal models, such as Bigraphical Reactive Systems (BRS)-based extensions.

BRS involves rewriting systems based on a universal process algebra that deliberately encapsulates both dynamic and spatial behavior. A BRS consists of a set of bigraphs that describe spatial and interaction or communication relationships along with a set of bigraphical reaction rules that defines how bigraphs can evolve over time. This study uses the CA-BRS extension (Control Agents & BRS) [3] and shows its advantages in terms of modeling the complex interactions between cyber and physical spaces and their reflection on the security of M-CPS. BRS determines the appropriate level of abstraction and granularity to overlook important details, while agent-based models capture critical aspects accurately and allow reasoning about the dynamic and uncertain behavior of CPS. Furthermore, the proposed iterative refinement process between CA-BRS and BPMN offers insights into the behavior and performance of CPS under different design choices. More precisely, the structural part of the CPS, representing the space in which agents exist and interact, is defined with BRS. Autonomous agents observe and control physical and cyber entities of their environment through ordinary reaction rules. Observations allow agent states to evolve, acting upon and influencing their decision-making processes thanks to rewriting rules. Thus, the complex and adaptive behavior of CPS is defined through several types of rules, each managing a possible evolution of the CPS component (physical, cyber, or virtual) and its side effects. This work associates two distinctive perspectives with the semantic interpretation of control agent behaviors: the states perspective and the activities perspective. The states perspective, already used in [4], is designed to describe the behavior of control agents as reactive agents through their possible states and transitions between them in response to the events that occur. The activities perspective is used to model control agent behaviors as business processes of non-reactive agents, and it is defined as the flow of activities that include decisions, loops, and concurrent activities. Both perspectives (states and activities) can use a particular semantics interpretation and notation to represent the different states and transitions of control agents. This study focuses only on the activities perspective. Some mapping rules allow the definition of the behavioral semantics of CA-BRS as a BPMN activity diagram. Thus, any functional inconsistency, due to a faulty design of the corresponding behavior model, such as the presence of a deadlock situation, an infinite loop, or a situation of multiple terminations, can be detected when executing the corresponding BPMN model of the specified CPS. The main contributions of this work are summarized as follows:

- Defines a new formal CA-BRS model that combines two formalisms: BRS and control agents (as abstract and intelligent virtual entities). This semantics model allows for the specification of the structural, behavioral, and security aspects of CPS.
- Provides a semantics interpretation of control agents in terms of business processes of BPMN diagram activities. This notation constitutes an industry standard, developed by the OMG consortium and easily understood by both technical and non-technical stakeholders, allowing one to leverage existing standards-based tools and languages for the design and analysis activities of CPS.
- Provides CA-BRS with a means to prevent unauthorized access (confidentiality) and unapproved modification of data (integrity) in an Electronic Healthcare Record (EHR) system. The applicability of the proposed approach is demonstrated in the case of M-CPS, addressing the confidentiality property.

II. BACKGROUND

A. CPS Characteristics

CPS are defined as the integration of physical systems with sophisticated, highly automated, and autonomous computation and networking. Countless examples dominate daily life and work, such as driverless cars, implanted medical devices, and industrial control systems that control production and infrastructure. Due to their impact on the real world, CPS must be built so that they cannot harm or damage people, property, or the environment [5]. Understanding CPS characteristics is crucial to designing, implementing, and managing them effectively across various domains. Among their essential characteristics are: (i) Integration of computation and physical processes, (ii) real-time interaction, (iii) sensors and actuators to facilitate the feedback loop between the cyber and physical domains, (iv) network connectivity, (v) interdisciplinary nature (computer science, control theory, electronics, and physical processes), (vi) security challenges, (vii) scalability, and (vii) dynamic and changing environments.

Several researchers have proposed different methods and design architectures to address these diverse requirements. Currently, research is divided into isolated subdisciplines, such as communications and networking, systems theory, mathematics, software engineering, computer science, and sensors. Thus, the main directions of research needed in the CPS domain, as stated in [6], are:

- Abstraction and Architectures: Innovative approaches to abstractions (formalism) and architectures have to be developed.
- Distributed Computations and Network Control: This refers to new frameworks, algorithms, methods, and tools related to time- and event-driven computing, software, failures,

reconfiguration, high reliability, and security requirements of heterogeneous components.

- Verification and validation: Hardware and software components, as well as the systems they form, have to overcome their actual stage and achieve a high degree of dependability and reconfiguration. New models, algorithms, methods, and tools are needed to verify and validate software components and the entire system from the early design stage.

This study's contribution stands in the context of the software engineering community and tackles a threefold challenge: proposes a software architecture for CPS that allows its effective development and evolution, defines the appropriate formalism for modeling the dynamic and unpredictable behavior of the system, and enables to a large extent the quality of its properties, especially safety and security.

B. Bigraphical Reactive Systems (BRS)

This section provides a brief presentation of the BRS model. For more details, the reader can consult [2, 7].

1) Definitions

A bigraph is called such because its nodes are structured in two ways. The first structure is placing, where the nodes are nested inside one another, giving an ordered set of trees, i.e. a forest. In the generic example in Figure 1, there are two trees. Each has a root represented by a dotted rectangle. The second structure is linking, where the ports of the bigraphs are partitioned into links, shown by curved lines. A link may be open or closed, and each open link has a distinct name (here x). Names allow bigraphs to be joined via their open links.

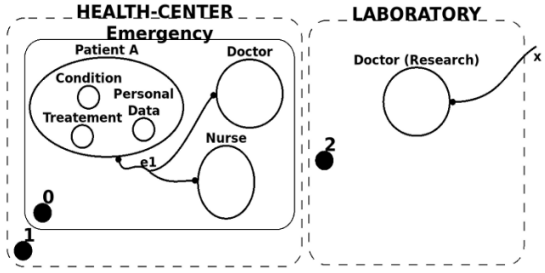

Fig. 1. B_{HC} A bigraph example of a health center structure.

The two structures are totally independent and form, through their interfaces (i, X) and (j, Y), a given bigraph structure $G = \langle G^P, G^L \rangle : (i, X) \rightarrow (j, Y)$, where G^P = (V, ctrl, prnt) is the place graph, G^L = (V, E, ctrl, link) is the link graph, i and j indicate the number of holes (sites) and regions, respectively, and X and Y are a set of inner and outer names, respectively. The pairs (i, X) and (j, Y) constitute, respectively, the inner and the outer interfaces of G. G^P and G^L share the same set of nodes V and their control ctrl. Bigraph elements are introduced by showing a simple model of a health center (B_{HC}) in Figure 1. Entities of the V set, e.g. Doctor, Nurse, Patient, Condition, Treatment, Personal Data are user-defined and may be related spatially through nesting (prnt function), e.g. Emergency contains Patient, or (non-local) hyperlinks (link function), e.g. connecting Patient to Nurse. As links are hyperlinks, they connect 1-to-n rather than more traditional 1-to-1 links. Each entity has a fixed arity that determines the number of links it must have (given by the ctrl function) e.g. each Nurse has one link. Links must always be present. Links may be named in which case they are open to extension. Dashed rectangles, called regions, represent adjacent parts of a system. Here, these refer to HealthCenter and Laboratory. In this example, $(3,\{x\})$ and $(2, \emptyset)$ represent the interfaces of the B_{HC} bigraph.

Two ways were used to represent a bigraph: as a 5-tuple with interfaces, or using a graphical notation. There also exists a third way to describe a bigraph: Textual Term (see [2] for more details). The algebraic term of B_{HC} given in Figure 1, is:

```
HEALTH-CENTER.Emergency.[PatientA.
(Condition/Treatment/PersonalData)e1/
Doctore1/Nurse/d0]/d1//Laboratory.(Doctor/
d2)
```

Dynamic behavior in terms of system evolution is defined in BRS via reaction rules. Two types of reaction rules are possible on a bigraph. The operation of mobility in the system represents the arrival or departure of an entity (represented by a node). The operation on links expresses the connection (or disconnection) of a bigraph node, through one of its interfaces. The possible system configurations, as well as the reaction rules, specify how these configurations can evolve. BRS augment bigraphs with a rewriting theory that allows models to evolve over time. The rewrite theory consists of a set of reaction rules B→B' that finds an occurrence of B in a larger bigraph C and replaces it with B'. A reaction rule R, noted (B, B', η), is a couple of bigraphs (B, B') such as the redex B specifies the bigraph to transform, the reactum B' specifies the bigraph after the transformation, and η is a transformation of ordinals. Figure 2 shows how a bigraph of Figure 1 can reconfigure itself using a reaction rule R1, which is used to model the Doctor mobility to quit his job and enter the Laboratory.

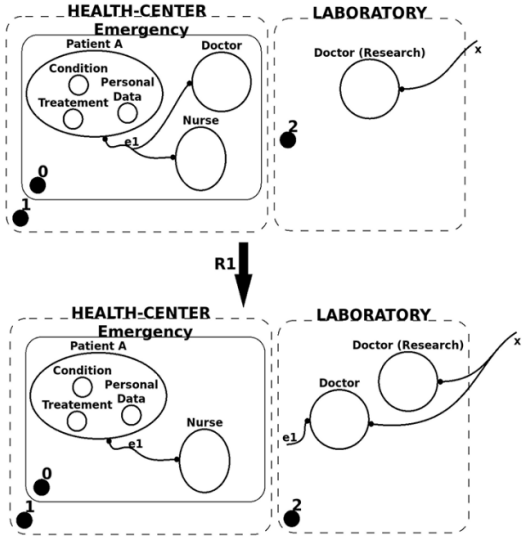

Fig. 2. R1: Example of a reaction rule.

2) BRS Extensions

This section presents some bigraph variants. First, some extensions related to the proposed model are described, and then other bigraph extensions are mentioned, adding extra information to their constituents. In [7], bigraphs were extended by introducing the agent concept. In this BiAgent model, computational or virtual entities are agents, and the physical entities form a bigraph. Entities such as vehicles, persons, computers, or smartphones are nodes related by the bigraph placing or linking graphs. Agents model disembodied or virtual entities such as computations or minds. They interact with the bigraph by observing it, being hosted in it, migrating in it, and controlling it. The study in [8] aimed to leverage the use of a widely accepted computation model, known as actor [9], to specify agents. An actor system is composed of autonomous objects, called actors, which communicate using asynchronous messages. An actor encapsulates a state and a thread and has a mail address used by other actors to send messages [9]. Adding reliable inter-agent messaging in the BiActors model constitutes a specialization of BiAgents. This may allow the implementation of agent entities in actor languages such as Erlang, Scala, and Cloud Haskell [9]. Moreover, adding a higher-level synchronous semantics to just the agent time might specialize BiAgents to a BiLustre or BiGiotto, allowing the implementation of the agent in these languages [9]. In parallel to these bigraph extensions, other works explored redefining the constraints on edge locality in link graphs by adding a probability to the edges giving rise to stochastic bigraphs [10]. Bigraphs with node sharing have also been defined, introducing the possibility that a node can inherit from several parent nodes [11].

C. BPMN Language

BPMN provides a powerful tool to model, analyze, and improve business processes. It enhances communication, standardizes notation, and supports both documentation and automation, contributing to increased efficiency and effectiveness in business operations. This specification (see Figure 3 for its main symbols) provides a clear and standardized way to represent complex business processes graphically. The fundamental elements of BPMN include:

- Flow objects, comprising events and activities that represent occurrences triggering or resulting from activities within a process and work or tasks that are performed as part of a process, respectively.
- Connecting objects: Two possible flows exist, sequence flow and message flow, representing the order in which activities are performed and the flow of messages between different pools or participants in a collaboration diagram.
- Swimlanes: The element Lanes within a pool is used to organize and categorize activities. Lanes can represent different roles, departments, or responsibilities within a pool. Thus, pools represent major participants or stakeholders in a process. Each pool typically contains its own set of flow objects and can represent a specific department or organizational unit. Additional elements can be defined to arrange process modeling as Data, Artifacts, Gateways, etc.

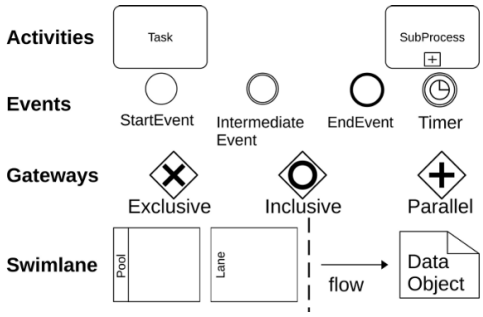

Fig. 3. Basic elements of BPMN.

BPMN creates a bridge between the design and implementation processes [12]. BPMN is extensible, and additional elements or attributes can be added for specific modeling needs. In particular, the BPMN4CPS extension [13] is designed to conveniently model the processes dedicated to CPS.

This standard extension is based on BPMN2.0 elements [14], introducing a three-part process logic: the cyber part, the controller part, and the physical part. Each part has its own type of activities that can be performed. In addition, it models the roles of CPS devices, the properties of the real-world environment, and the possible physical entities. Hence, a cyber-physical process must be composed of at least three lanes: a physical, a controller, and a cyber lane. This model is pretty common in cases where the designer wants to present the CPS as a set of processes that interact, where each process represents a physical, a control, or a cyber part. This idea is used in this CPS modeling approach, but it is more focused on the BPMN-based specification of the different agent behaviors, controlling the physical and cyber entities of the CPS.

III. RELATED WORKS

Several studies have addressed aspects of CPS engineering and highlighted the importance of formal methods. However, they differ in their specific purpose. Some focus on monitoring and formal analysis techniques, while others focus on the overall design process and the integration of formal methods into the design flow [15, 16]. This section reviews those most related to the proposed approach, highlighting the role of formal methods in addressing challenges such as heterogeneous modeling, behavior analysis, and design space exploration.

In [17], the need for different model types was shown to represent stakeholder requirements, system behavior, and system architecture. This study proposed a compositional modeling language for CPS based on category theory wiring diagrams. This categorical language aims to formalize the relationships between different model views, manage complexity, enable hierarchical decomposition of system models, and prove consistency between them. Formalism was used as first-order logic for requirements, difference and differential equations for physical behavior, and graphs for architectures. In addition, the potential of category theory to unify diverse views of system models and improve scalability was highlighted. In [18], another formal modeling method for physical entities in CPS was presented. This study extended the

traditional Timed Petri net by introducing spatial factors to describe the logical time-level behavior of physical entities, as well as state changes caused by position changes. This study contributed to the understanding of CPS to analyze and verify characteristics. In [19], a novel spatio-temporal event model was proposed to address the characteristics and requirements of CPS, providing a framework for analyzing and representing events in these systems. The event model represents events as a function of attribute-based, temporal, and spatial event conditions. It utilizes logical operators to combine different types of event conditions and capture composite events.

Some interesting works [20-22] were based on the BRS formalism. In [20], the concept of topology configuration was introduced to capture the environmental characteristics of cyberphysical spaces. The topology configuration provides contextual information for the access control system, such as the location of digital files, the access state between subjects and objects, and the proximity relationship between subjects. Based on this topology configuration, a formal interdomain access control model, called TA-CPAC, adaptively adjusts permission assignments to react to changing behaviors of subjects and objects. It considers both physical security and cyber security requirements, as well as securing the interaction between physical and cyber spaces. In [21], the TA-CPAC model was used to provide a systematic solution to specify security policies in a cyber-physical space and ensure the satisfaction of security requirements considering the dynamic topology of the environment. It also introduced a reduction algorithm to simplify the modeling process and improve the efficiency of model checking. In [22], CPS was formalized using an integrated formal analysis, combining the BPMN model and bigraphs. This study attempted to show how these models complement each other to assist the system designer in establishing formal verification of the business process workflows involved in CPS. The proposed integrated approach allows, according to different dimensions such as functional, organizational, and behavioral, to provide precise semantics for the considered process, improve efficiency, adapt them to new technologies and possible extensions, and gain a competitive advantage for the CPS-based organization modeled.

Formal methods play a vital role in addressing challenges related to heterogeneous modeling, behavior analysis, and design space exploration in CPS, as they provide techniques to ensure correctness and reliability. However, the formal models in the approaches cited above turn out to be too abstract and can neglect important details to capture the behavior and essential CPS properties. In [23], it was shown that BRS extended with specific intelligent nodes (control agents) determines the appropriate level of abstraction and granularity, because overly abstract models, such as BRS, can overlook important details, while agent-based models can capture critical aspects accurately. In addition, they allow modeling and reasoning about the dynamic and uncertain behavior of CPS. This study continues to use this formalism (CA-BRS) and shows its advantages in terms of modeling the interactions between the CPS heterogeneous constituents. An iterative refinement process between the CA-BRS and BPMN offers insight into the behavior and performance of the CPS under various design choices.

IV. SECURITY ISSUE OF CPS: MOTIVATING EXAMPLE

The healthcare industry has gone through various transformations, i.e., from Healthcare 1.0 to 4.0. The latter keeps patient records in a centralized EHR system to provide uninterrupted services in real time [24]. Patients' health can be monitored through Wearable Devices (WDs) and implantable Medical Devices (MDs). WDs are equipped with various health sensors to remotely measure blood pressure, heart rate, temperature, and glucose level of patients [24], and help to understand their behaviors. Thus, CPS may be considered an enabling key technology of Healthcare 4.0. This section emphasizes the importance of security and privacy in EHR. In general, the EHR contains relevant patient data, such as symptoms, medications, vital signs, medical history, chronic diseases, laboratory data, and radiology reports. Intruders can gain full access, for example, to patient email accounts, messages, and reports. A secure access control technique can solve this issue by helping stakeholders, including patients and caregivers, define who has the right to take a particular action on a given resource. Therefore, covered entities implement robust access control measures to protect the EHR and ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) regulations [25].

Figure 4 presents the architecture of a smart and secure M-CPS. It uses an access control model to ensure the privacy and security of patient data. This model provides some access control rules for particular users (Doctor, Nurse, or Biller) to a pre-configured subset of all available actions and content. Information gathered by EHR is distributed, i.e. physically located in different and heterogeneous hosts. In addition, access control rules can be maintained by different EHR organizations that might want to retain control over their resources. Various research efforts have been made to improve the effectiveness of models based on access control rules [26-27]. The aim here is to demonstrate the application of the proposed CA-BRS formalism to address the security of M-CPS in this context.

The following scenario is considered, which summarizes some particular situations requiring the execution of a set of access control rules. Initially, when the patient enters the hospital a number (or a nickname) is assigned for social and human purposes, which is completely mechanized by the HIS in a transparent way for privacy concerns. Thus, the healthcare service provider and the healthcare clearinghouse do not know the actual patient information [28]. The following rules express two situations identifying the access control of certain actors:

- In scenario 1, the Doctor responsible for treating patients is allowed to see all medical examinations.
- In scenario 2 neither the Doctor nor the Nurse are authorized to consult their patients' information beyond their work context, such as in the case of scientific research.

The following sections show how to represent a simple CPS model to motivate the need for bigraph-based semantics for CPS entities (cyber V_{Cy} and physical V_{Ph} ones) and their behaviors. In addition, it is endowed with some access control rules to address security aspects in CPS and thus verify security properties in healthcare systems.

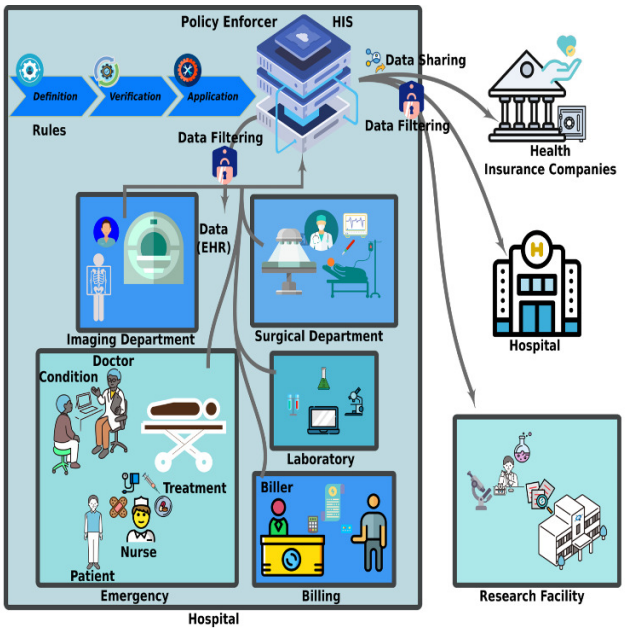

Fig. 4. Secure M-CPS example.

V. FORMAL MODELING CPS: STRUCTURAL AND VIRTUAL DIMENSIONS

This section presents the semantics of the CA-BRS model through an illustrative CPS example. For complementary details, please refer to [4]. CA-BRS combines two models, in contrast with other approaches that seek to find a single model for the overall CPS layers.

One model (based on BRS) is used to model the structural part of a CPS (the physical and cyber worlds), and another to model its virtual (or logical) part. In the CA-BRS model, multiple agents are composed with a bigraph, and computation can flow in space without flowing in time, or flow in time without flowing in space, or flow in both. CA-BRS can observe the structural part of a CPS, and map observations to control and migration actions. Informally, the CA-BRS model that defines a CPS is given by the tuple:

$$\text{CA-BRS}_{CPS} = (B_{CPS}, CA_{CPS}, Host_{CPS}, TR_{CPS}, AC_{CPS})$$

where:

- B_{CPS} is a bigraph defining the structural aspect of a CPS, including cyber and physical entities.
- CA_{CPS} is a set of control agents defined in an abstract way. Their semantics may be given in terms of bigraph [3] or another more appropriate formalism.
- $Host_{CPS}$ is a hosting function that associates each control agent ($\in CA_{CPS}$) cyber or physical entities belonging to B_{CPS} where it may host.
- TR_{CPS} is a set of trigger rules, expressing the state evolution of any control agent given its location.
- AC_{CPS} is a set of local reaction rules applied to change the bigraph (B_{CPS}) topology.

A. *Bigraph for Structural Dimension*

The CA-BRS model uses the bigraph B_{CPS} for modeling the physical and cyber components of CPS, their interactions, and their localities.

Definition 1: B_{CPS} is a bigraph given by $B_{CPS} = (V_{CPS}, E_{CPS}, ctrl_{CPS}, GP_{CPS}, GL_{CPS})$: $< m, \emptyset > \rightarrow < n, \emptyset >$, where:

- $V_{CPS} = V_{Ph} \cup V_{Cy}$ is a set of nodes that represents a set of physical (V_{Ph}) and cyber (V_{Cy}) entities of the CPS.
- E_{CPS} set of edges representing possible relationships and links between the CPS entities.
- $Ctrl_{CPS}$: $V_{CPS} \rightarrow K_{CPS}$ is a mapping function that associates each node type its signature in K_{CPS}.
- GP_{CPS} is the derived places graph defining explicitly the parent function $Prnt_{CPS}$ of all node types. These nodes can be grouped into roots (regions) according to their membership.
- GL_{CPS} is the associated links graph. Each node can have a fixed number of ports (P) allowing it to attach nodes through the link map $link_{CPS}$.
- *n* and *m* are ordinal numbers indicating the number of roots and sites respectively.

It is noted that the bigraph B_{CPS} is closed, as its inner and outer interface sets are empty. As indicated by this definition, the B_{CPS} mathematical structure is defined with two graphs: The place graph GP_{CPS} is a forest that represents the nested locality of CPS components (defined by the set V_{CPS}), and the link graph GL_{CPS} is a hypergraph that models connectivity between these components (expressed by E_{CPS}). Place graphs are contained inside regions (*n* roots) and may also contain holes (*m* sites).

Imagine the M-CPS example in Figure 4. Its corresponding B_{CPS} is defined to model not only the location of CPS components, with the $prnt_{CPS}$ function, but also their connectivity thanks to the function $link_{CPS}$ (see Figure 5). To simplify the figure, not all M-CPS constituents are considered. In this case, the physical CPS entities are decoupled, e.g. Doctor, Nurse, to cyber elements, e.g. Personal Data, Conditions. Links between the two element types allow us to track relationships between entities to represent, for instance, a relationship between the Personal Data of the patient node and the Doctor (link read). Thus, for this example, V_{Ph} = {Doctor, Nurse, PatientA, Billing, Biller, Emergency, Doctor(Research)} and V_{Cy} = {Condition, PersonalData}. The kinds of nodes and their number of ports (arity) constitute the signature K_{CPS} of B_{CPS} defined with the function $ctrl_{CPS}$. So, for instance: $ctrl_{CPS}$(Doctor) = {D: 1}, $ctrl_{CPS}$(PersonalData) = {P : 1}. The link graph in this example can contain hyperedges read, write, and partialread represented by lines connecting ports of various nodes or regions. Regions HEALTHCENTER, LABORATORY, and holes 0, 1, 2, 3 enable the composition of placing graphs, i.e., a hole 0 can be replaced by a region of another bigraph using the composition operator.

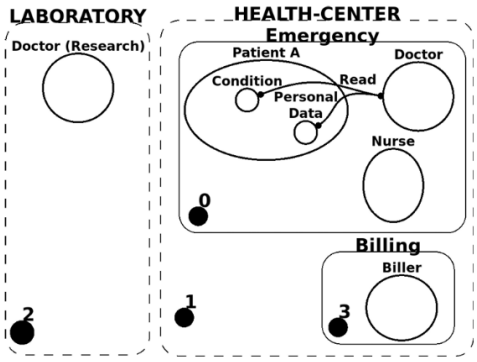

Fig. 5. The structural part of the M-CPS example.

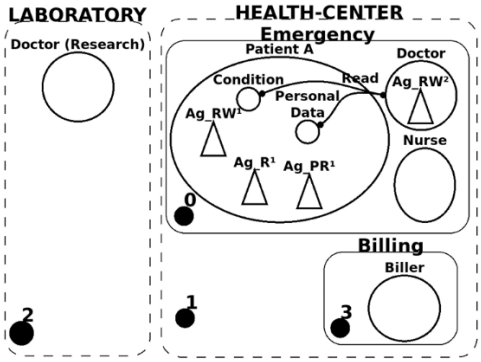

Fig. 6. Possible control agents for the M-CPS example.

B. Virtual Dimension

CA_{CPS} in the CA-BRS model refers to a set of intelligent agents that allow control of its structural entities. Each type of entity (physical or cyber) may host a distinctive type of CA: A_{Ph} to manage nodes of V_{Ph}, and A_{Cy} for nodes of V_{Cy}. CA may observe, analyze, and execute actions to alter the corresponding bigraph B_{CPS}. Thus, CPS dynamic behaviors involve close interactions between the two dimensions (structural and virtual). A certain change in one world should be reflected in the other world. The term intelligent agent used in the CA-BRS model is an umbrella that represents a wide range of software with different characteristics and abilities. These have been already specified by a specific kind of bigraphical nodes in [3] and also another formal model based on guided transition systems [4]. This fact led to the following generic definition of a control agent.

Definition 2: The pair (CA_{CPS}, $Host_{CPS}$) is designed to represent the virtual part of a CPS, where $CA_{CPS} = A_{Ph} \cup A_{Cy}$.

$Host_{CPS}$ is a hosting function that associates with each control agent ($\in CA_{CPS}$) node from B_{CPS} where it may host. In this case, $Host_{CPS} = (Host_{Ph}, Host_{Cy})$ such that $Host_{Ph}$: $A_{Ph} \rightarrow 2^{V_{Ph}}$ and $Host_{Cy}$: $A_{Cy} \rightarrow 2^{V_{Cy}}$.

Example: In the case of this M-CPS example, we define hierarchically $CA_{CPS} = A_{Ph} \cup A_{Cy}$, such that A_{Ph} = {AgRW, AgPR, AgR} and A_{Cy} = {AgTR}. Each Agent (A_{Ph} or A_{Cy}) controls a given entity that may be physical or cyber.

These agent types may have several instances according to the system behavior considered, and thus, each instance ($AgRW^1$, $AgRW^2$, etc.) can be in various states, for example, $St(AgRW^1)$ = {read, noread, write, nowrite}. As shown in Figure 6, the control agents $AgRW^1$, AgR^1, $AgPR^1$ observe the entity PatientA on which these agents host. This CA-BRS model deals with the structural and virtual aspects of the corresponding CPS, consisting of physical or cyber entities hosted by CA-BRS agents, along with their complex behavior aspects. To handle security in M-CPS, observations of these agents and their state's evolution are related to access control rules.

V. FORMAL MODELING CPS BEHAVIOR

This section provides a generic definition of the complex and adaptive behavior of CPS (its third dimension) through several types of rules, each managing a possible evolution of a CPS component (physical, cyber, or virtual). It is noted that two distinctive perspectives may be associated to semantically interpret these definitions: the states perspective and the activities perspective.

A. Generic Definitions

Figure 6 illustrates a possible configuration (or state) of the CPS considered example. Its structural part is combined graphically with the current hosting function (H_{CPS}) applied to each agent instance defined in this example. For instance, $H_{CPS}(AgRW^1)$ = PatientA, knowing that $AgRW^1$ is of type AgRW (belonging to the A_{Ph} set), and in a similar way, $H_{CPS}(AgRW^2)$ = Doctor. Thus, at a given time of the CPS evolution, its model CA-BRS may be in a given configuration defined as follows:

Definition 3: Given a CPS specified with CA-BRS, a configuration C describing its current state is defined by the pair $C = (B_{CPS}, H_{CPS})$, where:

- B_{CPS} describes the structural part of the CPS at a given time
- H_{CPS} is the distribution of the agent instances through the nodes of B_{CPS}, or precisely their hosting nodes at a given time, i.e. if $H_{CPS}(As_i) = \{N_1, N_2, ...\}$, then As_i is a possible instance of A_i ($\in CA_{CPS}$) and $N_1, N_2, ... \in Host_{CPS}(As_i)$.

By modeling the interactions and behaviors of individual CA_{CPS} agents, emergent properties can arise at a higher level that may not be immediately predictable from the behavior of individual agents alone. More precisely, CA-BRS state evolution is dictated by three types of local rules, allowing the behavior of the structural and virtual dimensions to evolve separately:

- The state change altering only the topology of the CA-BRS is possible thanks to the action rules AC_{CPS}. Autonomous agents (CA_{CPS}) control physical and cyber entities of their environment through these ordinary action rules.
- Agents' observations or trigger rules (TR_{CPS}) allow agent states to evolve through rewriting rules, acting upon and influencing their decision-making processes.

- A second set of Rearrangement Rules (GR_{CPS}) is also defined to represent possible changes in the virtual dimension of the CA-BRS. So, control agents in CA_{CPS} can communicate with each other, they can migrate from one node to another, and we can even create new instances of agents or destroy them.

In addition, dynamic CPS behaviors, involving close interactions between the structural (B_{CPS}) and virtual (CA_{CPS}) worlds (a certain change in one world must be reflected in the other world) should be defined by a set of global rules, noted Controlled Reaction Rules (CRR_{CPS}), involving the two previous definitions of the local rules (AC_{CPS} and TR_{CPS}). They are applied to CPS states (or configurations) to represent the dynamic behavior evolution of these systems. Each CRR rule α_i expresses the conditioned change of any CPS state, triggered by one or more controlling agent observations ($\gamma_i \in TR_{CPS}$), and materialized by a change ($\lambda_i \in AC_{CPS}$) in the topology (B_{CPS}) of the CPS. So, the two dimensions (structural and virtual) of the CA-BRS are involved. Formally, the definitions of these rules are given below:

Definition 4 (controlled reaction rules): A CCR of label α, defines how the initial configuration $C_1 = (B1_{CPS}, H1_{CPS})$ of a given CA-BRS evolves, according to a trigger TR_{CPS}, to another configuration $C_2 = (B2_{CPS}, H2_{CPS})$, following the execution of a set of actions AC_{CPS}.

The rule CRR is noted:

$\gamma_1, \gamma_2, ..., \gamma_n$

α: $(B1_{CPS}, H1_{CPS}) \rightarrow (B2_{CPS}, H2_{CPS})$

$\lambda_1, \lambda_2, ..., \lambda_m$

Labels $\gamma_1, \gamma_2, ..., \gamma_n$ decorating the rewriting rules belonging to the Trigger Rule set (TR_{CPS}), form a sequence (';') or a parallel ('/') composition application of these rule labels.

Labels $\lambda_1, \lambda_2, ..., \lambda_m$, decorating the rewriting rules belonging to the action rule set (AC_{CPS}), form a sequence (';') or a parallel ('/') composition application of these rule labels.

Definition 5 (Rearrangement rules). A rearrangement rule (GR) of label β is a local rewriting rule which may be of the following type:

- New(Ag_i, Ag, S, H_{CPS}): creates a new instance Ag_i of agent *Ag* having the state S in a hosting node defined by H_{CPS}
- Des(Ag, Ag_i, H_{CPS}) destroys an existing instance Ag_i of agent *Ag* hosting in a given node defined by H_{CPS}
- Mig(Ag_n&{S}, H_{CPSi}, H_{CPSj}) migrates the agent instance Mig(Ag_n) in its current state S from its hosting node H_{CPSi} to another possible hosting node H_{CPSj}
- $[Ag_i, Ag_j]_x$ creates a communication link of type *x* between the two agent instances Ag_i and Ag_j, and *x* refers to the message type between agents.

Example 3: This example formally defines and explains CRR rules specifying the dynamic and adaptive behavior of the M-CPS example that can be controlled or influenced by agents' observations. More details can be found in [4]. Two CRRs of Table I are considered to represent the dynamic and secure evolution of the M-CPS regarding scenarios 1 and 2 given in Section IV, respectively.

TABLE I. CRR RULES FOR ACCESS CONTROL IN M-CPS

	Scenario1	**Scenario2**
Description	The Doctor responsible for treating patients is allowed to see all medical examinations.	Neither the Doctor nor the Nurse is authorized to consult their patients' information beyond their work context, for example in the case of scientific research.
CRR	β_1 γ_1/γ_2 $C_1 \rightarrow C_2 \rightarrow C_3$ $\lambda_1; \lambda_2$ where $C_1 = (B_1, H_1)$, $C_2 = (B_1, H_2)$, $C_3 = (B_2, H_2)$	β_2 γ_5/γ_6 $C_4 \rightarrow C_5 \rightarrow C_6$ λ_5 where $C_4 = (B_4, H_4)$, $C_5 = (B_4, H_5)$, $C_6 = (B_5, H_5)$
Observations	γ_1: PatientA.$AgRW^1$& [Noread, Nowrite}→ PatientA.$AgRW^1$&[read, Nowrite} γ_2:Doctor.$AgRW^2$& [Noread,Nowrite} → Doctor.$AgRW^2$& [read, Nowrite}	γ_5: PatientA.$AgPR^1$& [Nopartialread}→ PatientA.$AgPR^1$&[Partialread} γ_6: Doctor-Research.$AgPR^2$& [Nopartialread}→ Doctor-Research.$AgPR^2$&[Partialread}
Actions	λ_1: $B_1 \rightarrow B_{21}$ Create a link "Read" between nodes: Doctor and PersonalData λ_2: $B_{21} \rightarrow B_2$ Create a link "Read" between nodes: Doctor and Condition	λ_5: $B_4 \rightarrow B_5$ Create a link "Partialread" between nodes: Doctor-Research and Condition
Rearrangement rules	β_1: New($AgRW^2$, AgRW, <Noread, Nowrite>, Doctor)	β_2: New($AgPR^2$, AgPR, Nopartialread, Doctor-Research)

The first CRR gives the right to the Doctor to read the medical examinations (Condition and PersonalData) of a given patient. The agent $AgRW^1$ hosting in PatientA to control it has changed its state thanks to the rule γ_1. Similarly, an instance of the AgRW agent (i.e $AgRW^2$), created by the rule β_1 to control the Doctor node, also has changed its state (rule γ_2). The execution of the two rewriting rules can be done in parallel (γ_1/γ_2). Therefore, the link "Read" will be established (λ_1; λ_2) between corresponding nodes.

The second CRR expresses that the doctor may only read partial patient information when he is in the research laboratory. It serves to control the Doctor's access to the PatientA's personal information (Condition). It is materialized by the establishment of a "Partialread" link between the nodes DoctorResearch and Condition. This constitutes the result of different observations (γ_5 and γ_6) and evolution β_2 of the agent instances in question ($AgPR^1$ and $AgPR^2$).

Figure 7 summarizes the configurations (C_1, C_2, …, C_6) involved in defining the secure behavior of the example (scenarios relating to Rules 1 and 2). According to CA-BRS behavior execution, transition rules, observations of CA_{CPS}, actions altering the CA-BRS topology, and rearrangement rules are defined, allowing to form CRR.

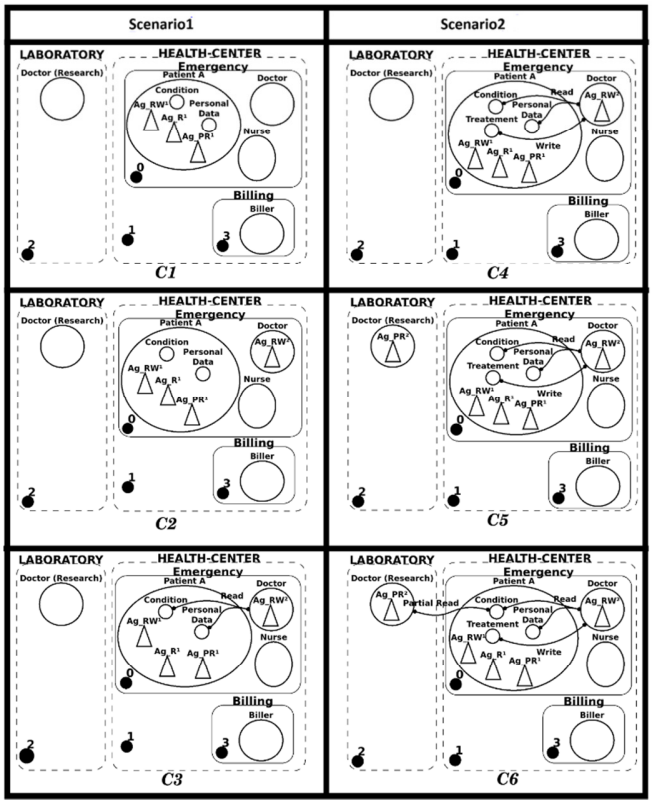

Fig. 7. CA-BRS configurations defining M-CPS behavior.

B. Control Agents Semantics of CA-BRS

Until now, CA_{CPS} behavior was defined in terms of states and transitions between them in response to occurring events. This perspective (states perspective) has already been addressed in previous work, and its implementation may be achieved using an appropriate language (Maude language [29]) based on transition systems. Another alternative to model the behavior of CA_{CPS} as activities processes, including decisions, loops, and concurrent activities, is also possible. This section explores the activities perspective.

The activities perspective is approached by defining CA_{CPS} behavior with the BPMN language (see Table II). Thus, the CA_{CPS} are considered as participants of the different processes, and their behaviors are specified by the corresponding workflows including the possible activities and events during their execution. Thus, the behavior of each control agent Ai is defined by the sets Event(A_i) and Act(A_i). Any functional inconsistency, due to a faulty design of the CA_{CPS} behavior model, such as the presence of a deadlock situation, an infinite loop, or a situation of multiple terminations, can be detected when executing the corresponding BPMN model of the specified system. Table II illustrates the BPMN-based semantics of the virtual and behavioral dimensions of CPS. The corresponding mapping rules translate the main features of the CA-BRS virtual and behavioral dimensions to BPMN ones. The obtained result forms standard models for business processes with accepted semantics facilitating the interaction between a system engineer and a system modeler.

TABLE II. BPMN-BASED SEMANTICS OF VIRTUAL AND BEHAVIOR DIMENSIONS

CA-BRS virtual dimension	**BPMN semantics**
CA-BRS	Pool Types: Physical, Cyber, Control Physical Agent, Control Cyber Agent
$CA_{CPS}=A_{Ph}\cup A_{Cy}$	Virtual participants:
A_{Ph}	Lanes of the Control Physical Agent Pool. Each Agent type A_{phi} has its own lane
A_{cy}	Lanes of the Control Cyber Agent Pool. Each Agent type A_{cyj} has its own lane
$V_{CPS}=V_{Ph}\cup V_{Cy}$	Physical/Cyber Participants:
V_{Ph}	Lanes of a given physical pool. At each physical entity N_{Phi} corresponds to its lane $_i$
V_{Cy}	Lanes of a given cyber pool. At each physical entity N_{Cyj} corresponds to its lane
$Host_{Ph}$: $A_{Ph}\rightarrow 2^{VPh}$	Connecting objects between participants of lane A_{Ph} and those of lane V_{Ph}
$Host_{Cy}$: $A_{Cy}\rightarrow 2^{VCy}$	Connecting objects: between participants of lane A_{Cy} and those of lane V_{Cy}
CA-BRS behavioral dimension	**BPMN semantics**
C=(B_{CPS}, H_{CPS})	A given scenario of BPMN model (collaboration diagram)
A trigger rule γ_i of a control agent A_{Cyj} hosting in N_{Cyi}	Flow/Connecting objects: Behavior of a process A_{Cyj} in terms of events Event(A_{Cyj}) and activities Act(A_{Cyj}). Each trigger rule represents a sequence flow γ_i
A trigger rule γ_i of a control agent A_{Phi} hosting in N_{Phi}	Flow/Connecting objects: Behavior of a process A_{Phi} in terms of events Event(A_{Phi}) and activities Act(A_{Phi}). Each trigger rule represents a sequence flow γ_i
A Rearrangement rule (in GR_{CPS}) of label β_i,	Connecting objects:
$\beta_i = [A_i, A_j]_x$	Each rearrangement rule represents a message flow β_i between the two participants A_i and A_j
β_i = New(A_i, H_{CPS}, Event(A_i), Act(A_i)), or β_i = Des(A_i, H_{CPS}, Event(A_i), Act(A_i))	β_i permits to add (resp. destroy) a new virtual participant A_i to (from) the collaboration diagram, its hosted entity (physical or cyber) should be given, as well as its events Event(A_i) and activities Act(A_i)
β_i = Mig(A_i, H_{CPSi}, H_{CPSj})	In this case, β_i is used to change the hosting H_{CPSi} (location) of a virtual participant A_i to another H_{CPSj} conserving its activities and events sets
Controlled reaction rules of label α	BPMN models simulation, γ_i and λ_i are executed sequentially

It is important to represent a CA_{CPS} behavior as a collaboration diagram that consists of a collection of virtual, physical, or cyber participants that are represented by distinctive pools. The BPMN model illustrated in Figure 8 is deduced from the behavior definition of CA_{CPS} during the execution of scenario 1. It is pretty common in cases where the designer wants to present the CA_{CPS} and their hosting entities as a set of processes that interact. In this case, each process represents a physical, a control, or a cyber entity of CA-BRS. The control part of this example is divided into a physical control part ($AgRW^1$ and $AgRW^2$) or a cyber control part (not considered in the given example). The physical and cyber parts represent the physical and cyber entities as Doctor, PatientA, Personal Data, and Condition. There is also a need to represent

the different interactions between the above participants. So, interactions connecting the pools are represented with message flows. Interactions between activities Act(A_i) or Act(V_j) triggered by Event(A_i) or Event(V_j) represent the behavior of a participant A_i or V_j in a given pool. Similarly, the CRR of scenario 2 is represented by the BPMN model in Figure 9. The resulting BPMN models' simulation helps to execute the M-CPS, while respecting the access control rules, and improve the current activities of the agents by refining the process.

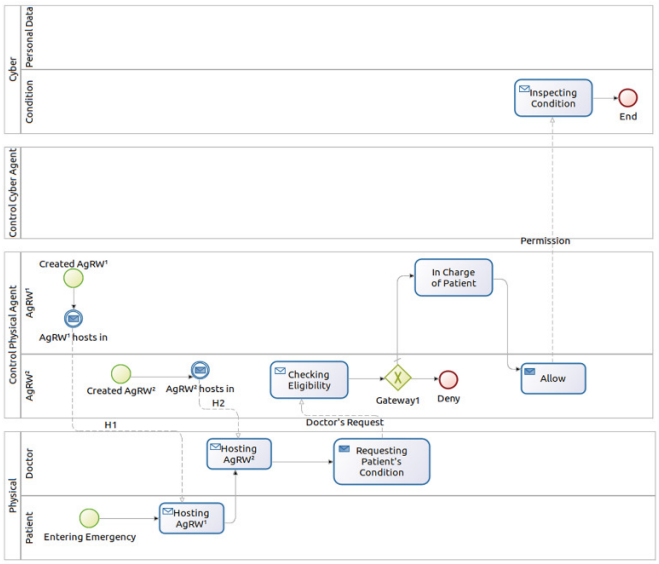

Fig. 8. CA_{CPS} behavior in terms of BPMN: Scenario 1.

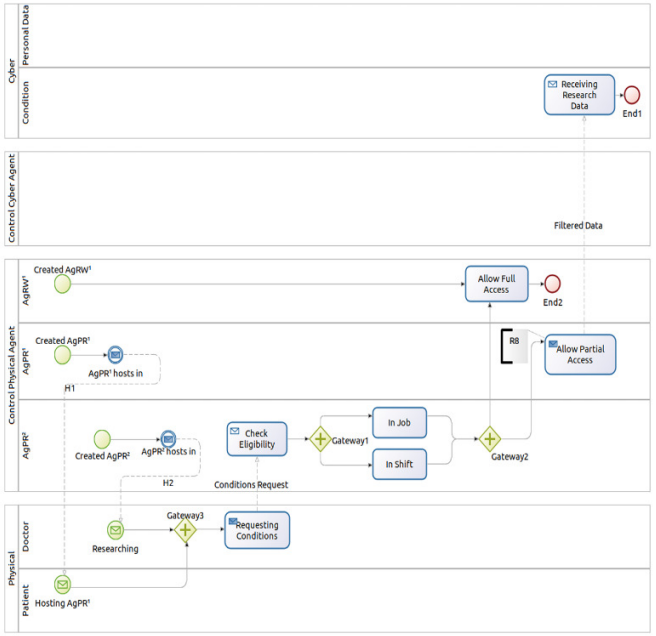

Fig. 9. CA_{CPS} behavior in terms of BPMN: Scenario 2.

The given approach, translating CPS formal models into BPMN ones, serves as a standardized bridge for the gap between the CPS formal specification (CA-BRS model) and their implementation. Then, successive CA-BRS are applied to BPMN transformations to capture and analyze the runtime behavior of a CPS based on its execution traces. An initial BPMN model execution may reveal limits in the formal models, causing a return to the modeling phase and revision of the models. Furthermore, finding the appropriate balance between capturing essential details (in BPMN models) and abstracting irrelevant complexities (in CA-BRS for CPS) can be a challenge within this approach. This trade-off may affect the accuracy and fidelity of the resulting BPMN model obtained after transcription. It is important to be aware of these limitations when applying the multidimensional modeling approach to CPS.

VI. CONCLUSION

Privacy concerns emerge with the digitization of healthcare services, the availability of Internet-of-care-things, and the usage of online services for medical data. Therefore, privacy considerations for medical records (EHR) aim to protect patients and their data by preventing unauthorized access by third parties. The main goal of this paper was to formally describe and analyze the security of the high-level behaviors of M-CPS to ensure privacy. This paper first extended the BRS formalism with control agent entities to understand and model secure M-CPS while addressing three essential factors, namely the structure change (the arrival or departure of a physical or cyber entity in the CPS), the agent evolution (transition from one state to another), and finally, how does the first change affect the second one and vice versa. Then, this study proceeded to mitigate the computational complexity of the M-CPS model by associating the activities semantics to the virtual part of these systems. The BPMN model was chosen, which is a modeling standard for business processes with accepted semantics that facilitates the interaction between the CPS engineer and the CPS modeler.

In the future, the development of a toolchain is planned to leverage the CA-BRS model involving the following roles collaborating closely to ensure that the CPS meets its security requirements and behaves as expected [30]: (i) The formal modeler, who uses formal languages and tools to specify CPS behavior and properties, (ii) The software engineer/developer, who is responsible for implementing the CPS based on its formal specification provided by the formal modeler and translates the CA-BRS model into an executable based on Maude and BPMN, and (iii) The verification engineer who will use formal verification techniques, such as model checking (Maude) and simulation (based on BPMN), to identify potential errors or inconsistencies in the CPS design.

REFERENCES

[1] N. Zhang, "A Cloud-Based Platform for Big Data-Driven CPS Modeling of Robots," *IEEE Access*, vol. 9, pp. 34667–34680, 2021, https://doi.org/10.1109/ACCESS.2021.3061477.

[2] O. H. Jensen and R. Milner, "Bigraphs and mobile processes (revised)," University of Cambridge, Computer Laboratory, UCAM-CL-TR-580, 2004, https://doi.org/10.48456/tr-580.

[3] Z. Benzadri, A. Bouheroum, and F. Belala, "A Formal Framework for Secure Fog Architectures: Application to Guarantee Reliability and Availability," *International Journal of Organizational and Collective*

Intelligence (IJOCI), vol. 11, no. 2, pp. 51–74, Apr. 2021, https://doi.org/10.4018/IJOCI.2021040103.

[4] A. Bouheroum, A. Derhab, D. Benmerzoug, S. M. Hemam, and A. Bouras, "A BRS-based Modeling Approach for Secure Medical Cyber-Physical Systems." Authorea, Sep. 06, 2023, https://doi.org/10.22541/au.169397646.61660455/v1.

[5] S. Lou, Y. Feng, G. Tian, Z. Lv, Z. Li, and J. Tan, "A Cyber-Physical System for Product Conceptual Design Based on an Intelligent Psycho-Physiological Approach," *IEEE Access*, vol. 5, pp. 5378–5387, 2017, https://doi.org/10.1109/ACCESS.2017.2686986.

[6] T. Sanislav and L. Miclea, "Cyber-Physical Systems - Concept, Challenges and Research Areas," *Journal of Control Engineering and Applied Informatics*, vol. 14, no. 2, pp. 28–33, Jun. 2012, https://doi.org/10.61416/ceai.v14i2.1292.

[7] E. Pereira, C. Kirsch, and R. Sengupta, "Biagents - A bigraphical agent model for structure-aware computation," Cyber-Physical Cloud Computing Lab, University of California, Berkeley, CA, USA, Working Paper CPCC-WP-2012-08-01, Aug. 2012.

[8] E. Pereira, C. M. Kirsch, J. B. De Sousa, and R. Sengupta, "BigActors: a model for structure-aware computation," in *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems*, Philadelphia, PA, USA, Apr. 2013, pp. 199–208, https://doi.org/10.1145/2502524.2502551.

[9] G. Agha, I. A. Mason, S. Smith, and C. Talcott, "Towards a theory of actor computation," in *CONCUR '92*, 1992, pp. 565–579, https://doi.org/10.1007/BFb0084816.

[10] J. Krivine, R. Milner, and A. Troina, "Stochastic Bigraphs," *Electronic Notes in Theoretical Computer Science*, vol. 218, pp. 73–96, Oct. 2008, https://doi.org/10.1016/j.entcs.2008.10.006.

[11] M. Sevegnani and M. Calder, "Bigraphs with sharing," *Theoretical Computer Science*, vol. 577, pp. 43–73, Apr. 2015, https://doi.org/10.1016/j.tcs.2015.02.011.

[12] T. Skersys, R. Butleris, and K. Kapocius, "Extracting business vocabularies from business process models: SBVR and BPMN standards-based approach," *AIP Conference Proceedings*, vol. 1558, no. 1, pp. 341–344, Oct. 2013, https://doi.org/10.1063/1.4825493.

[13] I. Graja, S. Kallel, N. Guermouche, and A. H. Kacem, "BPMN4CPS: A BPMN Extension for Modeling Cyber-Physical Systems," in *2016 IEEE 25th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Paris, France, Jun. 2016, pp. 152–157, https://doi.org/10.1109/WETICE.2016.41.

[14] P. Bocciarelli, A. D'Ambrogio, A. Giglio, and E. Paglia, "A BPMN extension for modeling Cyber-Physical-Production-Systems in the context of Industry 4.0," in *2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)*, Calabria, Italy, May 2017, pp. 599–604, https://doi.org/10.1109/ICNSC.2017.8000159.

[15] J. Fitzgerald, C. Gamble, P. G. Larsen, K. Pierce, and J. Woodcock, "Cyber-Physical Systems Design: Formal Foundations, Methods and Integrated Tool Chains," in *2015 IEEE/ACM 3rd FME Workshop on Formal Methods in Software Engineering*, Florence, Italy, May 2015, pp. 40–46, https://doi.org/10.1109/FormaliSE.2015.14.

[16] E. Bartocci *et al.*, "Specification-Based Monitoring of Cyber-Physical Systems: A Survey on Theory, Tools and Applications," in *Lectures on Runtime Verification: Introductory and Advanced Topics*, E. Bartocci and Y. Falcone, Eds. Springer International Publishing, 2018, pp. 135–175.

[17] G. Bakirtzis, C. Vasilakopoulou, and C. H. Fleming, "Compositional Cyber-Physical Systems Modeling," *Electronic Proceedings in Theoretical Computer Science*, vol. 333, pp. 125–138, Feb. 2021, https://doi.org/10.4204/EPTCS.333.9.

[18] G. Zhang, M. Zhang, R. Yan, M. Chen, C. Xu, and Y. Li, "Modeling and Analysis for CPS Physical Entities Based on Spatio-Temporal Petri Net," *Journal of Computers*, vol. 9, no. 2, pp. 499–505, Feb. 2014, https://doi.org/10.4304/jcp.9.2.499-505.

[19] Y. Tan, M. C. Vuran, and S. Goddard, "Spatio-Temporal Event Model for Cyber-Physical Systems," in *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, Montreal, Quebec, Canada, Jun. 2009, pp. 44–50, https://doi.org/10.1109/ICDCSW.2009.82.

[20] Y. Cao, Z. Huang, C. Ke, J. Xie, and J. Wang, "A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification," *Computers & Security*, vol. 87, Nov. 2019, Art. no. 101478, https://doi.org/10.1016/j.cose.2019.02.013.

[21] Y. Cao, Z. Huang, S. Kan, D. Fan, and Y. Yang, "Specification and verification of a topology-aware access control model for cyber-physical space," *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 497–519, Oct. 2019, https://doi.org/10.26599/TST.2018.9010116.

[22] A. Bouheroum, D. Benmerzoug, S. M. Hemam, F. Belala, A. Lehamdi, and R. Aouissate, "A Formal Integrated Approach for Cyber Physical Systems," in *2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, Oum El Bouaghi, Algeria, Oct. 2022, pp. 1–7, https://doi.org/10.1109/PAIS56586.2022.9946900.

[23] A. Bouheroum, D. Benmerzoug, S. M. Hemam, and F. Belala, "From CA-BRS to BPMN: Formal Approach for Modeling Adaptive Security in Cyber-Physical Systems," presented at the Tunisian Algerian Conference on Applied Computing (TACC 2021), Tabarka, Tunisia, Dec. 2021.

[24] J. Merhej, H. Harb, A. Abouaissa, L. Idoumghar, and S. Ouchani, "ELSO: A Blockchain-Based Technique for a Reliable and Secure Healthcare Information Exchange," *Arabian Journal for Science and Engineering*, vol. 49, no. 9, pp. 12005–12025, Sep. 2024, https://doi.org/10.1007/s13369-023-08586-y.

[25] W. Moore and S. Frye, "Review of HIPAA, Part 2: Limitations, Rights, Violations, and Role for the Imaging Technologist," *Journal of Nuclear Medicine Technology*, vol. 48, no. 1, pp. 17–23, Mar. 2020, https://doi.org/10.2967/jnmt.119.227827.

[26] A. Salehi Shahraki, C. Rudolph, and M. Grobler, "A Dynamic Access Control Policy Model for Sharing of Healthcare Data in Multiple Domains," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, Aug. 2019, pp. 618–625, https://doi.org/10.1109/TrustCom/BigDataSE.2019.00088.

[27] F. Chen *et al.*, "Data Access Control Based on Blockchain in Medical Cyber Physical Systems," *Security and Communication Networks*, vol. 2021, no. 1, 2021, Art. no. 3395537, https://doi.org/10.1155/2021/3395537.

[28] I. Essefi, H. B. Rahmouni, and M. F. Ladeb, "Integrated privacy decision in BPMN clinical care pathways models using DMN," *Procedia Computer Science*, vol. 196, pp. 509–516, Jan. 2022, https://doi.org/10.1016/j.procs.2021.12.043.

[29] M. Clave *et al.*, "Towards Maude 2.0⋆," *Electronic Notes in Theoretical Computer Science*, vol. 36, pp. 294–315, Jan. 2000, https://doi.org/10.1016/S1571-0661(05)80137-9.

[30] S. R. Idate, T. S. Rao, and D. J. Mali, "Context-Based Aspect-Oriented Requirement Engineering Model," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10460–10465, Apr. 2023, https://doi.org/10.48084/etasr.5699.