

From CA-BRS to BPMN: Formal Approach for Modeling Adaptive Security in Cyber-Physical Systems

Ayoub Bouheroum¹, Djamel Benmerzoug², Sofiane Mounine Hemam³ and Faiza Belala⁴

¹*Khenchela University ICOSI Laboratory, Khenchela Algeria*

²*Constantine2 - Abdelhamid Mehri University LIRE Laboratory, Constantine, Algeria*

³*Khenchela University ICOSI Laboratory, Khenchela Algeria*

⁴*Constantine2 - Abdelhamid Mehri University LIRE Laboratory, Constantine, Algeria*

Abstract

Cyber Physical Systems (CPSs) are emerging systems that offer integrations of computation, networking and physical processes. Recently, the CPS field has been identified as a key area of research, and CPSs are expected to play a major role in the design and development of future systems. However, the mutual coordination and inter-dependence among cyber and physical components come at the price of increased vulnerability to failures and attacks. Hence, securing a CPS is extremely challenging. In this paper, we propose a theoretical framework to address the adaptive security in CPSs. First, we specify CPS on the basis of the CA-BRS (Control Agent and Bigraphical Reactive Systems) formalism, which combine agent and bigraphical reactive systems to deal with the virtual level (software), the physical level (execution machines and their environment) and the behavioural level (dynamics) of the CPS. The given formal model helps in answering several crucial modeling issues in CPS, such as the natural heterogeneity, the connected dynamics, the interaction between cyber and physical components and meanwhile, the non-functional properties as security and reliability. Then, this well defined specification of CPS is translated to BPMN (ISO/CEI 19510 standard of the OMG) in order to bring the formal model closer to the implementation. An illustrative example of a secure IT department in a smart factory is considered to consolidate our theoretical approach results.

Keywords

BRS, CPS, Adaptive security, Formal modeling, BPMN4CPS, Smart Factory

1. Introduction

Embedding computing power in a physical environment has provided the functional flexibility and performance necessary in modern products such as automobiles, aircraft, smart phones, and more. Thus, product features came to increasingly rely on software and network infrastructure.

Tunisian Algerian Conference on Applied Computing (TACC 2021), December 18–20, 2021, Tabarka, Tunisia


✉ ayoub.bouheroum@gmail.com (A. Bouheroum); djamel.benmerzoug@univ-constantine2.dz (D. Benmerzoug); sofiane.hemam@gmail.com (S. M. Hemam); faiza.belala@univ-constantine2.dz (F. Belala)

🌐 <https://dbenmerzoug.e-monsite.com/> (D. Benmerzoug)

🆔 0000-0002-1284-6543 (A. Bouheroum); 0000-0002-6682-2862 (D. Benmerzoug); 0000-0002-9638-8390 (S. M. Hemam); 0000-0002-4563-4061 (F. Belala)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

The latter, helped factor out common hardware, it offered sharing functionality for further innovation. A logical consequence was the need for system integration. More recently, there have been systems coming online that must perform system integration even after deployment—that is, during operation. This has given rise to the cyber-physical systems (CPS) paradigm. The CPSs are defined as the systems which offer integrations of computation, networking, and physical processes [1, 2, 3]. Some of the defining characteristics of CPS include [4]: 1) Cyber capability in every physical component, 2) High-degree of automation, 3) Networking at multiple scales, 4) Integration at multiple temporal and spatial scales and 5) Reorganizing/reconfiguring dynamics.

Software engineering poses specific challenges based on the above characteristics of CPSs, in today's networked, interconnected world. It can have a profound impact in this domain, by defining suitable modeling and specification notations as well as supporting design-time formal verification. In this paper, we aim to present a methodology supporting the modeling of CPSs and reasoning about their behavior properties. Indeed, the heterogeneous nature of most CPS applications necessitates the use of heterogeneous mixtures of computation models. Among these models, we cite those based on formal semantics like denotational, axiomatic, operational or a hybrid of these, and those based on Meta-modeling techniques and Meta programmable tools. In the same thought, our work supports this idea and proposes a correct design approach of CPS using two known specification models BRS [5] and BPMN [6].

In our previous work, we combined agent technology and BRS to define a new formalism, called CA-BRS (Control Agent and BRS) [7, 8], dealing with the cyber level (software), the physical level (execution machines and their environment) and the control/behavioral level (dynamics) of the Fog systems. The aim of this paper is to show, how this formal model helps in answering several crucial modeling issues in CPS, such as the natural heterogeneity, the connected dynamics and the interaction between cyber and physical components. On the other hand, and in order to remove the gap between the high-level specification and the actual implementation, the given well defined CPS specification is translated to BPMN4CPS [9], whereas checking some behavior property, particularly that relating to adaptive security in the Oil and Gas Refinery smart plant for instance.

The remainder of this paper is organized as follows. Section 2 reviews some related work on the existing approaches. Section 3 gives a brief overview about BRS. Section 4 explains the principle of our three-phase approach for modeling CPS and reasoning about their behavior properties. Section 5 focuses on the description of the central phase of our proposal, it shows how to define a CA-BRS model dedicated to represent all the possible interactions between the physical and cyber entities of CPS. A transcription from the proposed formal model to a BPMN4CPS-based one is explained in Section 6. Finally, conclusion and future work are presented in Section 7.

2. Related Work

Obviously, a CPS is a “System Of Systems”, where complex and heterogeneous systems interact in a continuous manner [10]. Hence, computing and communication capabilities are increasingly embedded into physical spaces, thus blurring the boundary between computational and physical worlds. To enable seamless integration, the events in physical world need to be reflected in the

cyber world and the decision taken by the cyber world need to be communicated to the physical world. To address this need, researchers have proposed several modeling techniques, semantics, programming tools, for the design and the analysis of CPSs. However, the results remain limited and there are still many challenges. In this section, we cite without being exhaustive some CPS modeling approaches in order to position our contribution.

Particularly, in [11] authors survey several recent works in the field of CPSs. They classify the developmental efforts into different categories, based on whether they deal with the design and development of CPSs, or address specific issues of CPSs or discuss application of CPSs in specific domains. They also identified future challenges that need to be addressed before CPSs can be widely used.

Authors in [12] have defined in general, a CPS Framework representing its environment and stakeholder concerns, while providing an overview of the CPS Framework analysis methodology with its core concepts of facets (components of the systems engineering process with associated activities and artifacts) and aspects (groupings of cross-cutting concerns). Each facet is presented and understood from its set of activities and artifacts. The activities in turn address aspects and concerns throughout the CPS development cycle. Despite the inclusiveness of this proposal, the absence of formal models to represent CPS features poses a problem in the analysis and specification of their behavior.

An early-stage results of the ongoing SICHTEN 4.0 project was presented in [13], which reflects the goal of amalgamating existing standards from Industry 4.0, system architecture and the Semantic Web for developing a novel, multi-level approach for the viewpoint-oriented engineering of CPS. This work has facilitated the development of support for model-based engineering and seamless lifecycle management. The great benefit was the possibility of creating an open marketplace for CPS viewpoints. But, this project does not provide the development of prototype tools for editing and aligning views and achieving the given idea.

Also, a model for designing and implementing a CPS based on cooperative multi-agent system (MAS) paradigm was proposed in [14]. The identification of this model requires the use of design tools and a system architecture that are able to represent and manage the characteristic aspects of the system under analysis. Their results have been confirmed by the BigMC tool. The use of BRS through their basic version remains limited in the context of such heterogeneous and complex systems (CPS).

In [9] authors have introduced a CPS-aware BPMN 2.0 extension to handle CPS process features, called BPMN4CPS. Their work aim is to enable designers to accurately and efficiently cater for CPS elements, concepts, and properties when modeling CPS processes. Similarly, authors of [15] have addressed another BPMN extension that specifically deals with CPS management. Such an extension is realized as an enrichment of the PyBPMN meta model. Moreover, in order to obtain significant levels of flexibility and customizability, the proposed extension is implemented following a profiling-based approach, thus ensuring effectiveness in case of BP analysis carried out by the use of both simulation and analytical approaches. Although, BPMN, the de facto standard for business process specification, have proven to be suitable for formalizing high-level sequences of activities, it does not provide all the required concepts for specifying and analyzing CPS and their dynamic behavior.

These related works allow gaining insights into the frontiers of CPS, thus their study permits to propose further design innovations to continuously push these frontiers forward.

The heterogeneous nature of CPS, their geographic dispersion and the interaction between their cyber and physical components necessitate use of an extended version of the BRS model as a formal semantics framework. We consider a specific type of nodes, called Agents, equipped with their intelligence (mind) nature and relevant reaction rules. Particularly, this computational model (CA-BRS) will be able to represent virtual level of these systems. On the other hand and in order to remove the gap between the high-level specification of CPS and their actual implementation, we propose to translate the CA-BRS based models to BPMN4CPS processes in order to check and execute them thanks to some existing tools around BPMN as for instance VBPMN [16], Activiti [17] or BizAgi [18].

3. BRS Overview

According to Robert Milner and co-workers [19], a Bigraphical Reactive System is a graphical model which emphasizes both locality and connectivity. A BRS comprises a category of bigraphs and a set of reaction rules that may be applied to rewrite these bigraphs. Structurally, a bigraph consists of two independent sub-graphs; a place graph expressing usually the physical location of nodes whereas the link graph represents the mobile connectivity among them. The dynamic evolution of a system formalized by means of bigraphs is represented by reaction rules. A reaction rule is a pair of bigraphs, Redex and Reactum, where the Redex bigraph models the current state of the system and the Reactum represents its next state, after executing the rule.

Formally, a bigraph $B = (V, E, ctrl, G^P, G^L) : \langle m, X \rangle \rightarrow \langle n, Y \rangle$, has both places graph G^P , as a set of rooted tree, and links graph G^L , as a graph with nodes V and edges E . Consider for instance, the bigraph B of Figure 1a, nodes are defined by their names or in general v_i , edges are denoted by e_i . In this case, $V = \{v_0, v_1, v_2, v_3\}$ and $E = \{e_0, e_1, e_2\}$. The little dot that connects an edge and a node is called a port. In Figure 1a, v_0 node has a port that connects it to v_1 node by the edge e_2 . A basic signature is assigned to each node v_i thanks to the control map $ctrl$. In our example, the basic signature of the bigraph B shown in Figure 1a may be: $K = \{v_0 : 2, v_1 : 3, v_2 : 1, v_3 : 3\}$. In general, each control of K dictates how many ports the node has, how it behaves dynamically, and which controls are atomic, and which of the non-atomic controls are active or passive. Then, the outgoing and incoming interfaces (n, m) of the places graph, respectively represented by its roots and sites, are noted by $\{0, 1..n - 1\}$, they are disjoint from its nodes. $Roots(= n)$ can be parents of nodes and sites $(= m)$, but there is no parent for them; the sites may be the threads of the roots and knots but there is no son for them. The outgoing and incoming interfaces (X, Y) of the link graph are normally sets of names. Thus, the bigraph noted $B : (2, \{x\}) \rightarrow (3, \{y\})$ represents the bigraph of our example with 2 roots (regions), three sites and having two possible open links. The bigraph interfaces purpose is to allow the construction of (more complex) bigraphs from (simpler) bigraphs, and to consider a bigraph as a substructure of another. Moreover, bigraphs can be also expressed by term language, for example, the following is the corresponding algebraic expression of the bigraph given in Figure 1a, $V0 | V1_y.(V2 | d_1) | d_0 || V3_x | d_2$. Reader may see [19] for more details.

4. Motivation and Principle

CPSs need to coordinate between heterogeneous systems which consist of computing devices and distributed sensors and actuators. Thus, the central question that this work asks is: How to define a suitable formal method to support the correct design and implementation of such new class of engineered systems (CPSs) that are expected to play a major role in the design and development of future systems?

In recent literature, the term CPS has been defined in several ways and in different contexts, we identify in this paper two of the most known definitions given by the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). 1) For NSF, Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other [20]. 2) For NIST, Cyber-Physical Systems comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic [21].

Thus, CPS will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas [21]. This advance holds the potential to reshape our world with more responsive, precise, reliable and efficient systems, enabling a revolution of "smart" devices and systems [20].

Obviously, in order for CPS to function properly, their behavior requires formal model for specification, verification and implementation. Figure 1b outlines our solution principle, it identifies three phases: the initialization phase, the formalization phase and the implementation one.

We begin, in the initialization phase, by giving the essential elements of CPS architecture, we identify both physical (sensors, actuators, network, etc.) and virtual (application, process, etc.) elements, according to the standard "ISO/IEC/IEEE 42010: Systems and software engineering-Architecture Description". Then, we show how a given CPS will evolve and adapt to preserve its security property, while giving some execution scenarios of the considered CPS.

In the second phase of our approach, we translate the architectural design of a CPS in a formal model based on BRS and Agents (CA-BRS [7, 8]), with the objective to gain a better understanding on how to model and manage the physical and the virtual entities of CPS in one hand, and their control and interacting during the adaptation of the CPS behavior in response to unanticipated changes on the other hand. This paper details this work step and shows that the CPS physical layer is specified using bigraphs and their cyber and control layers are described with control agents. Thus, agents operate on a physical structure and can observe, control and migrate in order to fulfill a given execution property. A new form of reaction rules are defined to support the corresponding two types of evolution over time; physical, which corresponds to a sequence of bigraphs, and virtual conducted by the agents that move and migrate (cyber mobility), while considering some material constraints through the "Observations".

Through the third phase, we strongly support the idea that such systems engineering, should be unified with the engineering of security. Thus, this phase enables verifying some important properties and requirements in the early stages of design, before implementing the actual system. We choose to apply successive BRS-BPMN based transformations in order to capture and analyze run-time behavior of CPS based on its execution traces. Indeed, BPMN is a modeling standard for business processes with accepted semantics facilitating the interaction between a system

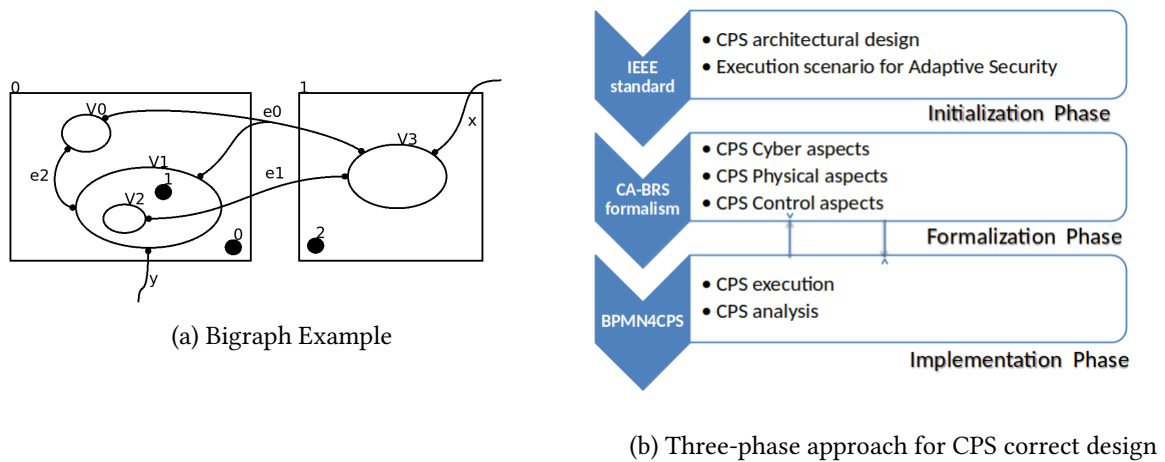


Figure 1: Principle Of Our Approach

engineer and a system modeler. It serves here as a standardized bridge for the gap between the CPS business process design (BPMN4CPS) and their implementation. This transformational approach is illustrated with a secure IT department design example in smart factory (the oil refinery).

5. CA-BRS: Towards a formal model for CPS

Since the BRS introduction, several extensions and refinements have been added to the ordinary BRS [19], motivating their interests and their application in several practical fields. In this work, we are based on a generic extension of BRS, called CA-BRS (Control Agents & BRS) [7, 8], which takes advantages of [22, 23, 24] and defines specific nodes called "Control Agents" endowed with a certain intelligence, allowing them to observe, analyze and execute actions (in the form of specific reaction rules) on the bigraphs that host them. Indeed, the CPS physical layer is specified using bigraphs. Their virtual layer is described with a set of control agents. Thus, agents operate on a physical structure; their state and localization may be changed in order to fulfill a given execution property. In this section, we refine the definition of CA-BRS in order to support two types of evolution over time; physical, which corresponds to a sequence of bigraphs, and virtual conducted by the agents that evolve, move and migrate (cyber mobility), while considering some material constraints through the "Observations". The formal definition of our proposed model is illustrated through a CPS example.

5.1. Running Example

The refinery plant example that we consider, processes crude Oil from a well, being located far from its location, to meet demand, without steadily growing in fuels (Petrol, Kerosene and Diesel) and exporting other products such as Naphtha and Fuel Oil. The followed cycle to carry out this type of refining of crude Oil is reported in [25] for interested readers. In this paper, we

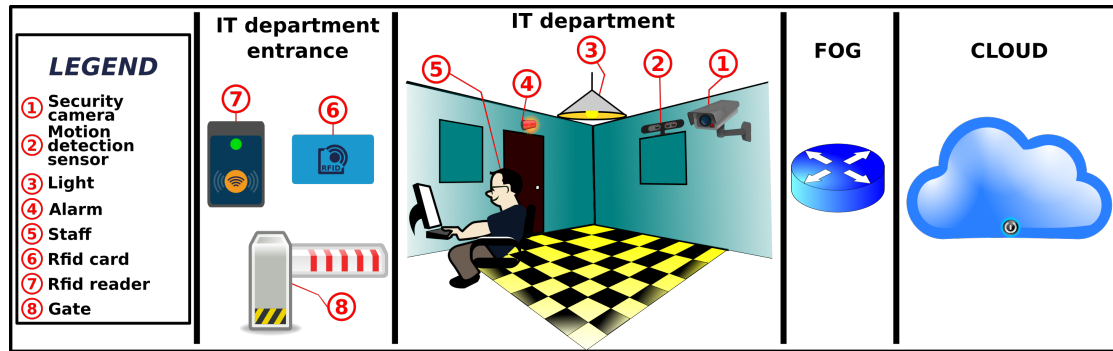


Figure 2: IT Department Architecture

try to continue some of the previous work of the refinery plant modeling, we address specifically the formalization of its IT department, whilst considering some of the security monitoring activities. For more simplification, the CPS system example (see Figure 2) is consisting in this case of the following sets of physical and cyber entities:

1. Physical entities: Security camera, Motion detection sensor, Light, Gate, Alarm, Staff, RFID reader, RFID card, Personnel (workers/staff who own RFID cards or outsiders who access the department for some reasons, but they don't have cards). We note also the existence of Cloud server and Fog nodes that may process.
2. Virtual entities: Backing camera records, security monitoring Cloud service, Cloud refinery plant, etc. and also other services to analyze and connect entities.

For experimental reasons, we consider an adaptive security system that aims to protect valuable assets in the face of changes in the IT department. This will be done by monitoring and analyzing its physical entities, and deploying security functions (may be in the Fog or Cloud regions) that satisfy some protection requirements (security, privacy, or forensic). The detection of a possible undesired topological change (such as a staff possessing a safe's RFID card entering the room, where the RFID reader is located) may lead to the decision to deploy a particular security control to protect the relevant asset. By monitoring changes in this system at runtime, one can identify new or changing threats and attacks, and deploy adequate security controls accordingly. In the Table 1, we summarize the possible states of some physical objects involved by the following scenario examples, depicting how this adaptive security system will evolve in these cases. We note that the Security Camera, for instance, may be in four distinctive pairs of contradictory states: on/off, recording/monitoring state, taking clear/unclear picture and online/offline. The combination of all these states and those of other virtual entities increases the complexity of this system and therefore requires its abstract modeling to describe its behavior.

Scenario1: The camera monitors the security state at the department.

If the camera is faulty and there is a motion, all moving persons must have RFID cards.

Scenario2: Unauthorized access.

The gate remains closed until the RFID card is presented.

Table 1
Possible states of the physical entities

Security Camera	Motion Detection Sensor	Light	Gate	Alarm	RFID Reader	RFID Card
on, off	on, off	on, off	on, off	on, off	on, off	
online, offline	online, offline	online, offline	online, offline	online, offline	online, offline	
record, monitor	detecting, not detecting		open, closed	active, inactive		valid, unvalid
clear Pic, Unclear Pic						

5.2. Modeling the CPS Physical and Cyber levels

In a preliminary step of this work, we have proceed to integrate a simplified model of our example, based on elementary bigraphs (without extension) in BigraphER [26] tool which is an environment for modeling and analyzing bigraphs. The simulation with partial amount of steps, gives a great number of states, we note then a combinatorial explosion of states. Thereby, it is necessary to provide a more expressive and efficient formalism that can overcome these drawbacks. Among them, the rewriting of the reaction rules to simulate such scenarios involving several actors, must not be conducted in all possible paths, guards must be considered to guide this execution of the rules. We will explain our solution approach step by step, in the next sections.

We highlight the adoption of a multi-level view to delineate physical entities, virtual entities, and dynamic aspects of a given CPS in general. Thus, the CA-BRS model includes a set of control agents (CA_{Vi}), representing Virtual entities dedicated to execute or control CPS processes, hosted in a given bigraph (B_{Ph}) expressing the real-world Physical entities.

Definition 5.1. Formally, the model CA-BRS defining a CPS is given by the tuple: $CA-BRS_{CPS} = (CA_{Vi}, B_{Ph}, Host, CRR)$, where:

1. $CA_{Vi} = A_{Ph} \cup A_{Cy}$ is a set of contol agents having two distinctive types.
2. $B_{Ph} = (V, E, ctrl, G^P, G^L) :< m, \phi > \rightarrow < n, \phi >$ is the hosted bigraph of agents.
 - a) $V = V_{Ph} \cup V_{Cy}$ a set of nodes that represents a set of physical (V_{Ph}) and logical (V_{Cy}) entities of the CPS,
 - b) E set of edges representing possible relationships and links between the CPS entities,
 - c) $ctrl$ is a mapping function, it associates each node type to its signature K ,
 - d) G^P is the derived places graph defining explicitly the parent function of all nodes types. These nodes may be grouped into roots (regions) according to their membership,
 - e) G^L is the associated links graph of nodes; each node may have a fixed number of ports. Some of these ports attached to physical entities represent their possible states (as mentioned in Table 1)
 - f) n and m are ordinal numbers indicating the number of roots and sites respectively.

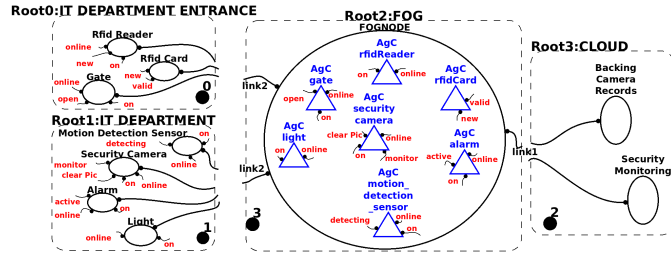


Figure 3: $CA-BRS_{CPS}$ model Example: Graphical view

3. Host is a hosting function that associates to each Control Agents type (CA_{Vi}), nodes where they may host. In our case, $Host : A_{Ph} \rightarrow V_{Ph}$ and $Host : A_{Cy} \rightarrow V_{Cy}$
4. CRR is a set of decorated reaction rules modeling physical and virtual mobility of its elements, each rule is defined by 6 elements: $(B_{Ph}, Host, B'_{Ph}, Host', AS, AR)$
 - a) B_{Ph}, B'_{Ph} are physical structures of the CPS defining respectively, the initial and the final bigraph during the execution of the CRR rule,
 - b) $Host$ and $Host'$ express respectively, the location of the control agents in the nodes of the bigraphs B_{Ph} and B'_{Ph} they manage.
 - c) AS is a set of Agent State rules, expressing the Agent state evolution given its location,
 - d) AR is a set of Action Rules representing local reaction rules applied to change the bigraph topology.

Example: Let us take our running example and define the physical and cyber levels of the IT department, while considering the $CA-BRS_{CPS}$ model. As shown in Figure 3, for the physical level (B_{Ph}) we identify 4 Roots indicating possible locations of the CPS entities. Each Root contains some of nodes, for instance, nodes of the set V_{Ph} as: Alarm, Light, Security Camera and Motion Detection Sensor are nested in the IT Department Root, on the other hand, nodes of the type Cyber ($\in V_{Cy}$) as: Backing Camera Records, Security Monitoring are nested in the Cloud Root. The presence of sites in a node or a root abstracts other entities existence, for example Site 0 indicates that other nodes may be installed in this Root as the Staff one. Concerning the virtual level (CA_{Vi}), we distinguish two types of Control Agents: $A_{Ph} = \{AgCr\ rfidCard, AgCr\ rfidReader, AgC\ gate, AgC\ alarm, AgC\ motion_detection_sensor, AgC\ security_Camera, AgC\ light\}$ and the set of possible other Agents that may be hosted in nodes of V_{Cy} to manage their execution, if it is of course an application or a given service ($A_{Cy} = \emptyset$ in our example). Initially, as shown in Figure 3, these Control Agents are hosted in a Fog node. But, during the system evolution, they may change their hosts (Migrate) and being in various states which are represented by their ports.

5.3. Modeling Adaptive Security in CPS

In this section, we define the behavior of any CPS specified with $CA-BRS_{CPS}$. Its execution model enriches the existing BRS one by appending the Trigger (AS) and Action rules (AR) information's to a new type of reaction rule (Controlled Reaction Rules –CRR). The format of

CRR rule is given by: $B_{Ph}, Host \xrightarrow[AR]{AS} B'_{Ph}, Host'$

The defined control agents (CA_{Vi}) in the CA-BRS framework observe the physical location of the distributed structure ($B_{Ph}, Host$) entities, capture the relationship between these entities (AS), and affect their state and position by executing a set of control actions (AR). The control reaction rules (CRR) then offer the ability to agents to control and adapt their corresponding services, affecting possible states of the specified system at a given time; this novel state after executing the controlled reaction rule (CRR) of the system is represented by ($B'_{Ph}, Host'$).

AS is a type of reaction rules that allows changing the state of agents, graphically, it suffices to establish a link between the port of a node, indicating its state, and that of the agent which manages it.

AR is a set of reaction rules affecting a bigraph while applying the following actions: a) Destroy a node, b) Create a node, c) Destroy a link, d) Create a link, e) Create an Agent instance, f) Communicate or not two Agents, g) Migrate an Agent from one node to another.

Example: Referring to our running example, we will model, thanks to a sequence of these guided rewrite rules (CRR), the previous given scenarios specifying how monitoring changes in the $CA-BRS_{CPS}$ topology at runtime in order to identify new or changing threats and attacks, and deploy adequate security controls accordingly (Agents migrating or their state changing). We present in Figure 4a the initial state of the adaptive security system, where we note that:

1. Each physical entity: Alarm, Security Camera, Gate, etc, is monitored by its corresponding agent, hosted in it. Its state is identified by the possible links between ports.
2. The "link2" from FogNode to the Security Camera, for instance, illustrates the streaming of the records to the IT Department; however the "link1" from FogNode to Baking Camera Records illustrates the sending and backup to the cloud. The existence of the two links specifies that the camera records the activities, monitored by the specialist person at the IT Department, and then records are stored in the cloud.
3. The "link1" from FogNode to Security Monitoring in the Cloud root, explains that the records are augmented by motion detection sensor and RFID reader.

After executing some CRR sequence rules, we will obtain new states of this model, for instance to define the scenario1, the corresponding CRR rule is $CRR1 = (B0, Host0, B1, Host1, AS1, AR1)$, B1 and Host1 are illustrated graphically in Figure 4b, while AS1 and AR1 sets of rules are presented and commented in Table 2.

Obviously, the rewriting of the reaction rules AS1 and AR1 are guided according to the involved Agents observations (state changes and locations) and may be also executed

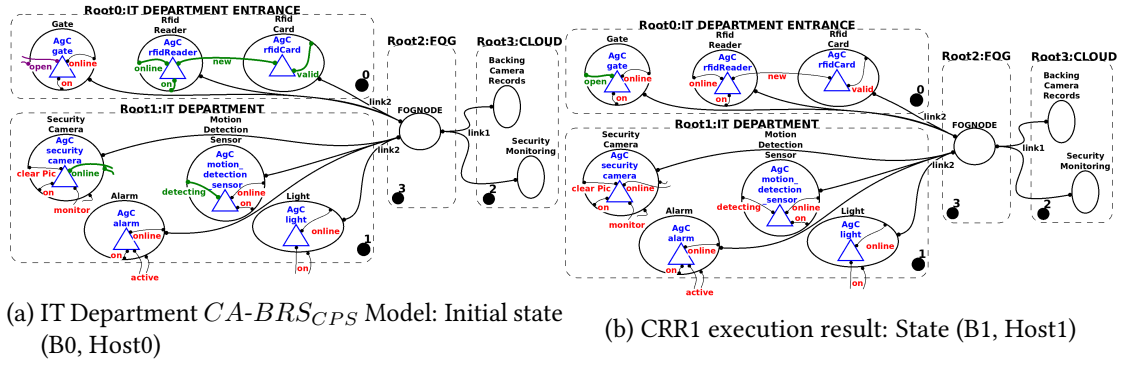


Figure 4: Initial State & Result State

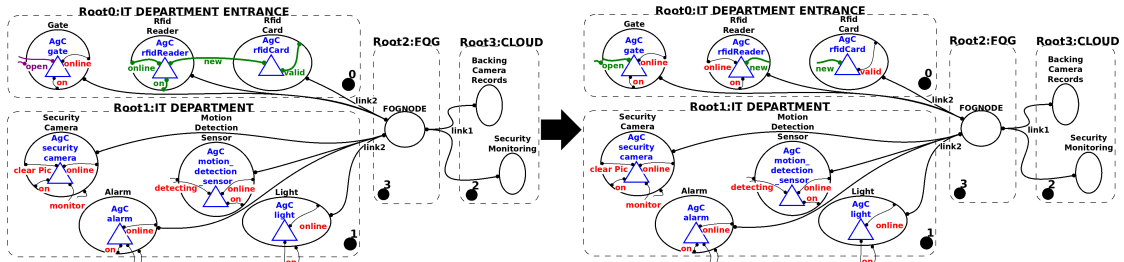


Figure 5: CRR2 execution

Table 2

AS and AR Reaction Rules for Scenario1 and Scenario2 (section 5.1).

The variables BH and BH' below stand for any CA-BRS_CPS state, i.e the tuple (B,Host).

CRR constituents	Rules	Comment
AS1	$BH \longrightarrow BH' \{ \text{Security Camera.Agc Security Camera} \ \& \ (\text{online}) \mid \text{Motion Detection Sensor.Agc Motion Detection Sensor} \ \& \ (\text{detecting}) \parallel \text{Rfid Reader.Agc Rfid Reader} \ \& \ (\text{Online}, \text{On}) \mid \text{Rfid Card.Agc Rfid Card} \ \& \ (\text{Valid}) \mid \text{Agc Rfid Reader, Agc Rfid Card} \}_{new}$	If a system state (BH) evolves toward the state BH' that contains the trigger between braces, i.e: "the camera is not online and there is a motion detected by the Motion Detection Sensor, all moving persons must have RFID cards". Then the corresponding rule (AR1) must be applied to open the gate.
AR1	$\text{Gate.Agc gate} \longrightarrow \text{Gate.Agc gate} \ \& \ (\text{open})$	One local rule is applied, to Create a link between AgC gate and the node Gate on the port "open", in the global state.
AS2	$BH \longrightarrow BH' \{ \text{Rfid Reader.Agc Rfid Reader} \ \& \ (\text{online}, \text{on}) \mid \text{Rfid card.Agc Rfid Card} \ \& \ (\text{valid}) \mid \text{Agc Rfid Reader, Agc Rfid Card} \}_{new}$	The security rules to open the gate are materialized in the trigger of this action rule, in braces: The RFID reader is online and on, the RFID card is valid and the person is identified as new one.
AR2	$\text{Gate.Agc gate} \longrightarrow \text{Gate.Agc gate} \ \& \ (\text{open})$ $\text{Gate.Agc gate} \ \& \ (\text{open}) \mid \text{Agc Rfid Reader, Agc Rfid Card} \}_{new} \longrightarrow \text{Gate.Agc gate} \ \& \ (\text{open})$	Two locale rules are applied sequentially in this case, the first one is when opening the door (Create a link) and the second allows closing the door and stopping communication via the link "new" between the two agents Agc Rfid Reader and Agc Rfid.

concurrently to provide new states. The Scenario2 is defined by CRR2 = (B'0, Host'0, B2, Host2, AS2, AR2), illustrated graphically in Figure 5; sets AS2 and AR2 are given in Table 2.

We may note that due to the limited expressiveness of the term language in the case of

Table 3Rules Correspondence between $CA-BRS_{CPS}$ and BPMN4CPS

$CA-BRS_{CPS}$	BPMN4CPS
$Ag_{Cy}/Host(Ag_{Cy}) = V_{Cy}$ or $Host(Ag_{Cy}) = Root$	Cyber part Controller part
$Ag_{Ph}/Host(Ag_{Ph}) = V_{Ph}$	Physical part
V_{Ph}, V_{Cy} Nodes or Root	Real-world physical entity

$CA-BRS$ model, some symbols as $\&$, $[_]_{link}$, $!$, $\{_ \}$, etc. have been introduced, we will see their formal semantics in a future work.

6. Translating CA-BRS to BPMN4CPS

BPMN is a modeling standard for business processes [6] that provides a set of concepts with a clear syntax and accepted semantics to facilitate the interaction between a system engineer and a system modeler. We choose it as an intermediate notation from the bigraph-based specification of CPS to their implementation. But, in order to capture important particular CPS concepts, we propose BPMN4CPS, a CPS-aware BPMN 2.0 extension, which introduces the process logic using three parts: the cyber part, the controller part and the physical part. Each part has its own type of activities that can be performed. In addition, the extension included the CPS device roles, the properties of the real world environment and the physical entities.

Our proposal aims to transform the $CA-BRS_{CPS}$ elements into executable process models of the BPMN4CPS, pointing out the need for the modelers to improve their models before they can be used as exact specifications for CPS implementation. Most importantly, this transformation is bidirectional (see Figure 1b), each of its two orientations can be used in an appropriate context and for different motivations. One can use it, for instance, to associate a formal semantics to BPMN4CPS processes and their tasks. On the other hand, it can be used to abstract some details provided by the formal CA-BRS model and give a better interpretation to the involved agents, in terms of activities and message flows between the different BPMN processes.

In this section, we give only the transformational approach motivation, illustrating it through the following correspondence table (Table 3). Obviously, each part of the BPMN processes is managed by an Agent type of the $CA-BRS_{CPS}$ model, activities or tasks represent their behavior, according to a given scenario. Real-world entities are represented by the nodes of the $CA-BRS_{CPS}$ model, which consider even their imbrications and nesting. The interactions between the different processes parts are materialized by some functions (Parent, Host, etc.) present in CA-BRS definition. More explanation and details will be presented in an upcoming paper.

7. Conclusion

This paper presented an idea of a new formal modeling three-phase approach based on bigraphs and agents (CA-BRS) for Cyber Physical Systems. In the present paper, we have detailed the core step, showing the convenience of this formalism to provide a high level modeling of CPS. Our

contribution consisted in providing an extended BRS-based approach to formalize the physical, the cyber entities and their dynamic behavior.

In other words, since CPS represents the coupling of its environment (physical processes) and embedded computations, the proposed model includes a set of control agents (CA_{Vi}), representing Virtual entities dedicated to execute or control CPS processes, hosted in a given bigraph (B_{Ph}) expressing the real-world Physical entities.

Besides, a new set of bigraphical reaction rules, called controlled reaction rules (CRR), to deal with agent analysis and changes was proposed. These rules adopted the trigger information (AS) resulting from any agent analysis to formalize the behavior evolution of CPS, while executing some action rules (AR) in the form of a reaction rule. An illustrative example showing how to execute these complex rules to ensure adaptive security of the IT department in smart factory was considered.

On the other hand, we have paid more attention to the execution and formal analysis of the proposed BRS-based specifications of CPS systems. For this, we suggested to transcript our bigraphical model to BPMN4CPS; the agent virtual entity added to BRS is better specified in terms of processes. Our next goal is to be able to finalize this transcription and by the same time, define a formal semantics to the proposed correspondence rules. We plan also to extend the term language of bigraphs in order to express virtual entities and their corresponding evolving rules.

Acknowledgments

This work was partially supported by the LABEX-TA project MeFoGL: "Méthodes Formelles pour le Génie Logiciel".

References

- [1] M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. Tröster, G. Tsudik, F. Zambonelli, Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence, *Pervasive and Mobile Computing* 8 (2012) 2–21. URL: <https://www.sciencedirect.com/science/article/pii/S1574119211001271>. doi:<https://doi.org/10.1016/j.pmcj.2011.10.001>.
- [2] L. Sha, S. Gopalakrishnan, X. Liu, Q. Wang, *Cyber-Physical Systems: A New Frontier*, Springer US, Boston, MA, 2009, pp. 3–13. URL: https://doi.org/10.1007/978-0-387-88735-7_1. doi:10.1007/978-0-387-88735-7_1.
- [3] I. Horvath, B. Gerritsen, Cyber-physical systems: Concepts, technologies and implementation principles, in: I. Horvath, Z. Rusak, A. Albers, M. Behrendt (Eds.), *Proceedings of the ninth international symposium on tools and methods of competitive engineering - TCME-2012*, Delft University of Technology, Netherlands, 2012, pp. 19–36. TCME 2012, Karlsruhe, Germany ; Conference date: 07-05-2012 Through 11-05-2012.
- [4] L. Miclea, T. Sanislav, About dependability in cyber-physical systems, in: *2011 9th East-West Design & Test Symposium (EWDTS)*, IEEE, 2011, pp. 17–21.
- [5] K. Zarour, D. Benmerzoug, N. Guermouche, K. Drira, A bpmn extension for business process outsourcing to the cloud, in: *World Conference on Information Systems and Technologies*, Springer, 2019, pp. 833–843.

- [6] K. Zarour, D. Benmerzoug, N. Guermouche, K. Drira, A systematic literature review on bpmn extensions, *Business Process Management Journal* (2019).
- [7] A. Bouheroum, Z. Benzadri, F. Belala, Towards a formal approach based on bigraphs for fog security: Case of oil and gas refinery plant, in: 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2019, pp. 64–71.
- [8] Z. Benzadri, A. Bouheroum, F. Belala, A formal framework for secure fog architectures: Application to guarantee reliability and availability, *International Journal of Organizational and Collective Intelligence (IJOCI)* 11 (2021) 51–74.
- [9] I. Graja, S. Kallel, N. Guermouche, 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), IEEE, 2016, pp. 152–157.
- [10] R. von Hanxleden, E. Lee, C. Motika, H. Fuhrmann, Multi-view modeling and pragmatics in 2020: position paper on designing complex cyber-physical systems, in: G. D. e. Calinescu R. (Ed.), *Large-Scale Complex IT Systems. Development, Operation and Management*, volume 7539 of *Lecture Notes in Computer Science*, Monterey Workshop 2012, Springer, Berlin, Heidelberg, 2012, pp. 209–223. doi:10.1007/978-3-642-34059-8_11.
- [11] S. K. Khaitan, J. D. McCalley, Design techniques and applications of cyberphysical systems: A survey, *IEEE Systems Journal* 9 (2014) 350–365.
- [12] C. P. S. P. W. Group, et al., Framework for cyber-physical systems, release 1.0, Report, National Institute of Standards and Technology, May. URL: <https://pages.nist.gov/cpspwg/library> (2016).
- [13] U. Kannengiesser, H. Müller, Multi-level, viewpoint-oriented engineering of cyber-physical production systems: An approach based on industry 4.0, system architecture and semantic web standards, in: 2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), IEEE, 2018, pp. 331–334.
- [14] V. Di Lecce, A. Amato, A. Quarto, M. Minoia, Bigraph theory for distributed and autonomous cyber-physical system design., *IAENG International Journal of Computer Science* 47 (2020).
- [15] P. Bocciarelli, A. D’Ambrogio, A. Giglio, 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), IEEE, 2017, pp. 599–604.
- [16] G. Salaün, P. Poizat, A. Krishna, Vbpmn framework, 2017. URL: <https://pascalpoizat.github.io/vbpmn/>.
- [17] I. Alfresco Software, A. community, Activiti bpm platform, 2010. URL: <https://www.activiti.org/>.
- [18] BizAgi, Bizagi, 2010. URL: https://portal.bizagi.com/index.php?option=com_content&view=article&id=233catid=10&Itemid=95.
- [19] O. H. Jensen, R. Milner, Bigraphs and mobile processes (revised), Technical Report, University of Cambridge, Computer Laboratory, 2004.
- [20] National Science Foundation, Cyber-physical systems, 2014. URL: https://www.nsf.gov/news/special_reports/cyber-physical/.
- [21] The National Institute of Standards and Technology, Cyber-physical systems, 2018. URL: <https://www.nist.gov/el/cyber-physical-systems>.
- [22] E. Pereira, C. Kirsch, R. Sengupta, Biagentsa bigraphical agent model for structure-aware computation, *Cyber-Physical Cloud Computing Working Papers, CPCC Berkeley* (2012) 1–13.
- [23] E. Pereira, C. M. Kirsch, R. Sengupta, J. B. de Sousa, Bigactors—a model for structure-aware computation, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPs), IEEE, 2013, pp. 199–208.
- [24] S. Marir, F. Belala, N. Hameurlain, A formal model for interaction specification and analysis in iot applications, in: *International Conference on Model and Data Engineering*, Springer, 2018, pp. 371–384.
- [25] A. Bouheroum, Vers la modélisation d’un Cloud sécurisé: Approche basée Fog Computing (Memoire

de master 2), Master's thesis, Abdelhamid Mehri, Constantine2-University, Constantine, Algeria, 2019.

[26] M. Sevegnani, Bigrapher, 2015. URL: <https://dcs.gla.ac.uk/michele/bigrapher.html>.