Conceptual Modeling of Physical-Informatical Essence Duality of Cyber-Physical Entities

Yaniv Mordecai
Faculty of Industrial & Management Engineering, Technion – Israel Institute of Technology, Haifa, Israel yanivmor@technion.ac.il

Pathmeswaran Raju
Knowledge Based Engineering Lab, Birmingham City University, Birmingham, UK path.raju@bcu.ac.uk

Dov Dori
Faculty of Industrial & Management Engineering, Technion – Israel Institute of Technology, Haifa, Israel; Engineering Systems Division, Massachusetts Institute of Technology, Cambridge MA, USA dori@mit.edu

Abstract—Cyber-Physical Systems (CPS) interact with real world entities, and must hold internal representations of these entities in order to handle them appropriately. Physical-informatical essence duality (PIED) is the parallel existence of the entity as both the original, usually physical source, and its informatical representation, as held by each agent interacting with the entity. The distinction between the original external entity and its representation is critical for correct modeling and realization of complex interactions of CPS with the real world. The implications of this distinction must be recognized and accounted for. Conceptual modeling semantics for the PIED problem make this distinction possible, structured, and well-defined in the system model. We review a formalism based on Epistemic Logic semantics, and a model-based framework based on Object Process Methodology, and demonstrate applicability of our framework for the generic threat handling process, common to various CPS and various types of threats, such as safety hazards, terror attacks, and cyber-attacks.

Keywords- Informatics; Model-based Systems Engineering; Physical-Informatical Essence Duality; Agent-Oriented Architecture; Object-Process Methodology; Epistemic Logic; Knowledge Representation; Cyber-Physical Systems

I. INTRODUCTION

Systems are becoming ever more complex, multidisciplinary, and interconnected. Interactions with physical, biological, and social environments are constantly evolving, with a giant leap over the last two decades, with the emergence of Cyber-Physical Systems (CPS). CPSs comprise virtual and physical segments of various controllers and actuators interacting with each other to achieve virtual and physical goals alike [1]. One of the fundamental principles of Cybernetics is the dualism and duality of the physical world versus the cyber world, both of which are constituents of the natural world [2]. System architects increasingly follow robust and resilient design paradigms for systems that adapt or are easily adjustable to a variety of environments and working conditions. System integration, interconnectivity, and interoperability are critical for successful execution of complex cross-range processes [3].

Consequently, systems and agents interacting with their external environment and among themselves maintain a model of the environment. This model facilitates and affects the agent’s capability to interact with the environment. Several agents interacting with the same environment can each hold a different model of this environment. Agents’ representation of the external world can have varying levels of fidelity, related to the level of detail the agent is required to process, or capable of processing. The role of Informatical manifestations of "real-world" entities in natural, societal, and technical processes is one of the fundamental challenges in contemporary Cybernetics and Informatics [4].

Due to the distributed, stochastic nature of complex cyber-physical system-environment constructs, environment entities have a dual nature. The entity is defined once by the original (most often physical) embodiment, and once by the representation thereof, as held by each relevant agent. The way an entity is captured, understood, or perceived by each agent in the system is defined by Mizzaro as “Epistemic Information” [5], i.e., information derived from knowledge and understanding. We define the dual existence of the original-physical and representational-informatical as Physical-Informatical Essence Duality (PIED). PIED exists in virtually any type of system, including natural and societal contexts, complex systems, and systems-of-systems. This duality is also noted in the literature on Epistemic Logic [6] and Knowledge Representation [7]. Bar-Hillel’s Semantic Information Theory distinguished the meaning of content payload from the meaning of the physical carriers, namely, of information from data [8]. Hayles [9] provides an in-depth discussion on the implications of information-matter duality and dualism, including the abstraction of information from matter, the separation of information from the material source it reflects, and the separation of content from medium.

Conceptual Modeling has significant importance in conveying and clarifying system structure, behavior, and functionality [10]. However, common modeling languages like UML and SysML [11], as well as available architectures adapted for Cyber-Physical Systems [1], lack the semantics to capture this delicate but critical notion, among other notions related to Cyber-Physical constructs [12]. Traditional system modeling approaches often fail to provide the semantics needed to capture and formally represent PIED.

Modeling languages grounded in the information systems
domain mostly refer to entities as either physical or informatical, but not both. Typical UML models capture Actors as top-level external entities, interacting with the system at the Use-Case level [11]. However, the Actor is not associated with an internal representative Class, Actor designation is not replicated for subsystems at lower levels, and sub-systems are rarely defined as actors of other sub-systems. The simple notion that sub-systems in a system constitute mutual actors, is critical to the understanding of cross-structural processes in CPS, but PIED is not supported by conventional UML techniques.

This gap often leads to erroneous modeling, realization, and system behavior. In Data Integration, multiple representations must be accounted for [13], [14], but the interaction with the environment is not addressed. Cyber-physical constructs also consist of the actual physical entity, to which information holding components refer, and it must in general also be acknowledged and modeled. This complicates the problem of information integration due to the challenge of aligning information with 'real world' entities. System Safety studies have shown that systemic misconceptions led to dire consequences and catastrophes [15].

Several studies concerned with precise detection of real world events and information, thus touching on the essence duality problem of model entities, are available in the literature, especially in the fields of system safety [16], cyber security [17], and counter-terrorism [18], [19]. The common ground for all these applications is the centrality of the threat identification and handling process, which is a classic illustration of the PIED problem.

The purpose of this paper is to focus on the application of conceptual modeling semantics to reflect PIED in model based CPS engineering, including specification, design, and development. We define and analyze this duality and its implications on system models, and review the formalism and model-based framework for defining, capturing, and containing the compound essence of entities. Our formalism consists of Epistemic Logic semantics, and is also object-oriented. Our conceptual modeling approach is based on Object-Process Methodology (OPM) [20], a holistic framework for complex systems modeling, and emerging ISO 19450 standard.

The rest of this paper is organized as follows: Section II provides a brief description of OPM and its relevance to this study. Section III discusses the concept of PIED, its formal definitions and conceptual modeling semantics. Section IV illustrates PIED modeling in generic Threat Handling processes. Section V summarizes the paper and discusses future extensions.

II. OBJECT-PROCESS METHODOLOGY (OPM)

OPM [20] is a holistic framework for complex systems modeling, specification, design, and verification. OPM captures the functional, structural, and procedural aspects of the system, in a single unified, dual graphical-textual view, which consists of a set of hierarchically organized and interconnected Object-Process Diagrams (OPD). Each OPD extends the OPD above it and adds more details – thus providing for inherent complexity management and reduction. Each OPD is accompanied by a textual computer-generated description in Object-Process Language (OPL) – a subset of English.

The primary building blocks in OPM are objects and processes, collectively called things. Objects are things that exist and can have states. Processes are things that occur and transform objects: they generate and consume objects, or change their state. OPM also provides a host of structural and functional links that capture the various object-object, object-process, process-object, and process-process relationships.

OPM’s freely available CASE tool, OPCAT 1 [21] automatically generates OPL sentences in response to visual model edits. The textual description is equivalent to the graphical view, allowing for enhanced model understanding. Any model fact has to appear once in any diagram in the model, for it to be valid for the entire model. OPCAT also provides a built-in simulation engine, which supports model validation, verification, and testing, and is especially useful in visualizing the execution of complex interactions.

OPM’s unified static-dynamic view has proven complexity management and alleviation capabilities that strongly support essence duality modeling [22]. Inherent complexity management via hierarchical decomposition enables concealing or revealing representations, as required for model understanding and communicating. The semantically equivalent graphical and textual views make OPM appealing to both sides of the human brain, catering to systems architects, domain experts, professionals and practitioners. The capability to generate meta-models—generic, multi-purpose models and patterns that can be instantiated and adapted for specific systems and problems—is a threshold condition for utilizing a language for metamodeling as practiced in this research. OPM’s standardization as ISO 19450, as a basis for system and process modeling in ISO enterprise standards, enables accelerated dissemination of OPM for enterprise modeling. OPCAT fully supports the concepts and distinctions we explore and demonstrate, and allows rapid and clear demonstration and visualization of PIED situations. PIED-aware models recently submitted by undergraduate students validate OPM’s applicability for PIED.

III. PHYSICAL-INFORMATICAL ESSENCE DUALITY (PIED)

In this section, we provide some basic formal definitions and understanding of PIED. We define the formalism for describing this aspect, drawing on the semantics of Epistemic Logic, which are dedicated for capturing and describing knowledge and belief [6]. The notation is object-oriented and adjusted for conceptual modeling of complex engineering systems. We also briefly present the OPM-based conceptual modeling framework for expressing and handling PIED as part of system design and specification.

There are two characteristics of the entity that are relevant in the PIED context: affiliation and essence. Affiliation denotes the entity as either: a) original and environmental, i.e., pertaining to the environment, or b) representational and systemic, i.e., pertaining to the system. Essence denotes the entity as either physical or informatical. While original entities

1 Downloadable for free from http://esml.iem.technion.ac.il/
are mostly physical, and representational ones are consequently informatical, all combinations of affiliation and essence are applicable and valid, especially in CPS.

In order to correctly approach PIED, we have to define the knowledge-base of the system and each agent therein. Knowledge about the environment is required so that system agents can make decisions and perform actions. The knowledge-base affects the outcome of reaction, action, and interaction. It includes what the agent needs to know, thinks, knows, and thinks it knows about each external entity.

Let $E$ constitute an original entity. A representation of the entity, $R(E)$ consists of two aspects: a) recognition of existence $X$, and b) Perceived State $S$, as defined in (1).

$$R(E) \equiv (X, S) \quad (1)$$

Recognition of existence is dichotomous, so $X$ can assume only 0 or 1. The Perceived State $S$ can assume a wide, combinatorial range of values and sub-states of the entity’s characteristics, which can be recursively referred to via (1).

Let $A. R(E)$ denote the representation of $E$ held by agent $A$. $A. R(E)$ can be defined only if $E$ is found in $A$’s knowledge base: $A. K_X(E)$, i.e., $E$ is known to $A$ when it exists. The recognition of existence is denoted by $x$. $A. R(E)$ can assume a state $s$ only if $s$ is defined in $A$’s knowledge base. $A. K_S(E)$ is the set of $E$’s states that are known to $A$. It depends on $A$’s recognition of existence, $A. K_X(E)$, but it is also distinguished from it, since agents may know the entity, but not necessarily its state. These limitations are expressed in (2).

$$A. R(E) = \{ x | A. K_X(E), s | s \in A. K_S(E) \} \quad (2)$$

Each characteristic ($i$) of the entity $E$, $E. C_i$, constitutes a bona fide entity. The agent has to be aware of its existence, indicated by $K_X(E. C_i)$, and of its possible values, denoted by $v$, as listed in $K_S(E. C_i)$. This is shown in (3).

Representations of the same entity may often be integrated, synchronized, or compared, in order to improve their fidelity. A joint representation of two or more representations $n = 1, ..., N$ is defined in (4) as $R [ R_1(E), ..., R_N(E) ]$.

$$R [ R_1, ..., R_N ] \equiv h_X( \forall A_n. R(E).X), h_S( \forall A_n. R(E).S) \quad (4)$$

$$\zeta(E, g(A. f(R(E)))) = \begin{cases} 1, & A. R(E).S = E.S \smallskip \smallskip 0, & A. R(E).S \neq E.S \end{cases} \quad (5)$$

The agent’s effect on the state of the original entity depends on its state as assumed by the agent. The entity’s response to the effect can be coherent or incoherent, depending on the match between its actual state and the state perceived by the agent, as expressed in (5), where $\zeta$ denotes the coherence of the result of the entity’s response function, $E. g$, to the agent’s action function, $A. f$, which depends on the representation $R(E)$ and the state perceived by the agent $A. R(E).S$.

The OPM metamodel for PIED-aware system models includes several hierarchical organized OPDs, followed by auto-generated OPL texts. Natural language names of model artifacts replace the mathematical symbols used above, making the text easier to read.

The topmost level (Figure 1.) describes the interaction of Agent with Entity. A Representation of the entity is required for the agent to handle the entity, using the Entity Handling process. The representation of the entity is generated by the Representation Generating process that requires the original entity, as well as a Sensor to detect the entity.
The Entity's Responding to \( f(s_i) \) process is elaborated in Figure 4. Coherence is obtained when the entity's State is equal to the agent's representation's Perceived State. Otherwise, the Result is incoherent. The result of the interaction can affect the representation of the original entity. Detecting the result (with appropriate means), representing it, feeding it back into the system, and updating the original representation, are parts of a dedicated process, Representation Refining, which is not shown in this preliminary metamodel.

IV. PIED-AWARE MODELING OF THE GENERIC THREAT HANDLING PROCESS

The formalism and OPM design pattern introduced in the previous section clearly facilitate capturing PIED. We now demonstrate the applicability of the metamodel we have presented to practical Cyber-Physical settings. The example we discuss concerns with the generic process of threat management and control, relevant to many CPS with these capabilities. A threat is an entity which is capable of harming system or stakeholder assets and activities.

A PIED-aware modeling approach includes the consideration of the real potentially threat-posing object (or simply Threat) as an external, separate entity, and the representation of the threat, Threat Profile as held by the agent Threat Manager, and generated by the Threat Profile Generating process, in response to Threat Detecting. This is illustrated in Figure 5.

The Threat Handling process is illustrated in Figure 6. It includes Attacking the Threat if it is perceived as threatening, and Ignoring the Threat if it is perceived as unthreatening. Each action by the Threat Manager is responded to by the Threat with an adequate Responding process. The result of Ignoring the Threat is elaborated in Figure 7, where a coherent Result means...
Causing No Harm, while an incoherent Result means that the Threat is actually threatening, as opposed to what the Threat Manager thought, and therefore it is Causing Harm.

Following is the auto-generated OPL text for the entire Threat Handling Process model. OPCAT supports OPL generation for the entire model, in addition to per-OPD generation. The model-level OPL text provides complete specification of all model features; It can be read fluently and logically, with no duplicate statements; and it can be integrated into existing OPM models (which is also useful of course in integrating PIED-aware modeling into existing system models based on the metamodel presented in Section III. We slightly edited the order of statements in order to improve readability for readers who are not experienced OPM and OPCAT users.

The first set of statements (1-6) describes the structural specifications of the model, i.e. which objects are defined in the model, what are their inherent properties (i.e., affiliation and essence), what other objects characterize them as attributes, and what are each object’s relevant states. The structural aspect is complemented by the functional aspect, expressed in statements 7 and 8. It includes the major processes exhibited by the model objects as their functions, services, or methods. The remaining statements describe the procedural aspect. Each process or function is specified. Process specification includes its inputs (which are consumes by the process) and resources (which merely support it but are not consumed), its outputs (which are yielded or created by it) and results (e.g., modified object states, or the invocation of other processes), its triggering events and enabling conditions, and its sub-processes (which are all characterized in the same manner).

```
1. Threat is environmental and physical.
2. Threat exhibits Threat Level.
   2.1. Threat Level can be threatening or unthreatening.
3. Threat Manager is physical.
4. Threat Manager exhibits Threat Profile.
   4.1. Threat Profile relates to Threat.
   4.2. Threat Profile can be exists or nonexistent.
   4.3. Threat Profile exhibits Perceived Threat Level.
      4.3.1. Perceived Threat Level can be threatening or unthreatening.
5. Threat Detection is environmental.
   5.1. Threat Detection can be positive or negative.
6. Result is environmental and physical.
   6.1. Result can be coherent or incoherent.
7. Threat exhibits Responding to Ignoring and Responding to Attack.
8. Threat Manager exhibits Threat Handling, Threat Profile Generating, and Threat Detecting.
9. Stimulating is environmental and physical.
   9.2. Stimulating yields Threat Detection.
10. Threat Detecting is physical.
    10.1. Threat Detecting requires Threat and positive Threat Detection.
    10.2. Threat Detecting invokes Threat Profile Generating.
```

V. Summary

This paper introduces the Physical-Informatical Essence Duality (PIED) problem as it applies to entities in Cyber-Physical Systems (CPS). We review the formalism and conceptual modeling semantics to handle and contain PIED when it applies to various entities in systems and models. This problem is significant and must be handled appropriately especially in Cyber-Physical systems (CPS).

We have applied the modeling of PIED to the generic Threat Management process exhibited by many agents in various CPS domains, e.g. safety, counter-terrorism, and cyber security. Future work will extend the PIED-aware model with layers reflecting aspects such as feedback, conflict resolution, refinement and fusion of representations, and embedded coherence analysis. We also intend to further elaborate the Threat Management model and apply it as a metamodel to various threat handling situations in practical systems, especially in the fields of defense, health, and sustainability.

Acknowledgment

The authors would like to thank the anonymous referees for their useful feedback and advice on this paper. This research was carried out with the financial support of the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 262044 – VISIONAIR, the Bernard M. Gordon Center for Systems Engineering at the Technion, and the Knowledge Based Engineering Lab at Birmingham City University, UK.
REFERENCES


