Microprocessors and Microsystems 41 (2016) 67–76

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

An approach to model dependability of cyber-physical systems

Teodora Sanislav*, George Mois, Liviu Miclea

Department of Automation, Faculty of Automation and Computer Science, Technical University of Cluj-Napoca, Cluj-Napoca, Romania

ARTICLE INFO

Keywords:
Cyber-Physical System
Dependability analysis
Environmental monitoring
Wireless sensor networks
Agents

ABSTRACT

Cyber-Physical Systems (CPSs) represent a new generation of digital systems, where cyber entities and physical devices cooperate towards a set of common goals. The research presented in this paper aims to contribute to the development of CPSs by proposing: (1) an analysis methodology to model the CPS's behavior in terms of dependability; and (2) a CPS architecture with dependability facilities applicable in environmental monitoring, based on the Wireless Sensor Network, multi-agent and cloud computing technologies. The proposed methodology combines a primary dependability analysis technique with the representation of knowledge in order to support the development of CPSs capable to model the dependability at run-time. A dependability domain ontology has been implemented on a CPS case study based on this methodology and its effectiveness has been demonstrated, showing how the proposed approach is able to enhance system dependability. Also, the paper provides a detailed description of each architectural layer of the CPS case study, focusing on the wireless sensor node and on the intelligent decision system.

1. Introduction

The recent advancement in information technology and the continuously increasing complexity of digital systems has led to the need for a new generation of intelligent solutions – Cyber-Physical Systems. They integrate computing, communication and storage capabilities with monitoring and control of the entities in the physical world, actions that have to be performed dependably, safely, securely, efficiently and in real-time. CPSs consist of interconnected objects, embedded with sensors, collecting information from the physical world, and actuators, acting upon the environment, and integrated under an intelligent decision system, representing the cyber world [1]. Due to their characteristics and properties, CPSs are used in a wide range of domains, such as smart manufacturing, emergency response, environment monitoring, building automation, critical infrastructure, health care and medicine, intelligent transportation and service robots. Therefore, this next generation of physically-aware engineering systems have to satisfy a set of system-level requirements/ challenges: dependability, security, interoperability, predictability, and sustainability. This paper addresses the dependability challenge in an evolving and adaptable context.

Dependability represents the ability to deliver service that can justifiably be trusted [2]. A highly dependable system should operate properly without interruption and deliver all the requested services. Therefore, assuring CPSs dependability is a very difficult task to be achieved, given that the cyber and physical components are independent and might be dynamically interconnected during system operation. In this context, it is mandatory to perform a dependability analysis of the CPSs from the early phases of the design flow to provide a feedback for the system refinement and to reduce the risk of late discovery of dependability design consequences [3]. However, this is insufficient because CPSs are adaptable and reconfigurable systems whose structure is dynamically changed depending on the context, resulting in a modification of their behavior at run-time.

The primary dependability analysis techniques, recommended by the IEC-60300-3-1:2003 international standard [4] for dependability assessment (such as: Fault Tree Analysis – FTA, Failure Mode and Effect Analysis – FMEA, Markov analysis, Petri Net analysis, Reliability Block Diagrams analysis – RBD) are used for prediction, verification and improvement of dependability attributes, especially reliability, availability, maintenance and safety. These techniques work off-line and are applied during the different stages of a system development process. In case of CPSs these techniques must be adapted in order to assure the on-line modelling of dependability at run-time. Ontologies can represent a solution in this case, since they are formal frameworks for representing the knowledge. They can be accessed by the CPSs software components through formal languages. The dependability domain

* Corresponding author. Tel.: +40 264202366.
E-mail address: Teodora.Sanislav@aut.utcluj.ro, teodora.sanislav@aut.utcluj.ro (T. Sanislav).

http://dx.doi.org/10.1016/j.micpro.2015.11.021
0141-9331/

ontology aims to provide the means to investigate the CPSs faults and failures, and the rules to eliminate/mitigate them with respect to the systems properties and functionalities. The development of dependability domain ontologies, used for achieving the analysis of CPSs behaviors, has to be performed based on a methodology that assures their scalability and reusability.

This paper proposes a methodology for developing a dependability analysis technique in order to model the behavior of CPSs at run-time. The envisioned approach is to adopt a well-known ontology development methodology and to combine it with a qualitative evaluation method that drives dependability aspects of CPSs. The effectiveness of the methodology is demonstrated on a CPS for environmental monitoring. The case study CPS architecture for the real-time monitoring of environmental status is based on the Wireless Sensors Network (WSN) technology for data acquisition and on the cloud computing technology for storing, managing and analysing the data in a large context. The CPS architecture, used for exemplification purposes here, gathers temperature and humidity information from portable low cost nodes. Within this system, data sensed by the sensors are sent to a measurements database, where they are stored and can be further processed. An intelligent cloud-based decision system transforms these measurement data into knowledge, reported to the end-users under various modalities [5].

The rest of the paper is structured as follows. Section 2 discusses related previous work and outlines the paper's main contributions. Section 3 introduces the basic idea behind our proposed dependability analysis approach and describes in detail the steps of the methodology in order to develop a dependability domain ontology. Section 4 highlights a description of the methodology at work in one case study. It presents the proposed CPS overall architecture, emphasising the system layers, the hardware architecture of the wireless sensing devices, and the intelligent decision system. The CPS dependability domain ontology is implemented based on the proposed methodology, as a component of the intelligent decision system. Section 5 presents the experimental results of the proposed approach, highlighting the performance characteristics in terms of five dependability metrics. Finally, the conclusions are listed in Section 6.

2. Related work and contributions

2.1. CPSs dependability

Significant work has been carried out to define the CPSs characteristics, their application domains and, in relation with these, the CPSs scientific and technical challenges, as well as the societal and institutional ones [6–12]. All these studies highlight dependability as an important feature of CPSs.

Several approaches, which address the dependability issue, have been proposed in the past years. Papers [13–15] present a framework for the qualitative and quantitative understanding of dependability in the context of CPSs. This framework is an agents-based model with semantic capabilities, presented as a semantic ontology for the detection of errors in a CPS concerning a water distribution network. The ontology represents the physical entities of the CPS (e.g. sensors) and the retrieval, analysis and processing of the information taking place within these entities [15]. Paper [16] proposes a proactive health monitoring and management (HMM) system to monitor the health condition of a CPS, to diagnose and to identify the faulty components in case of failures. The HMM system uses a fault signature matrix (FSM) to associate the CPS components with the rules of the CPS normal behavior and a diagnosis quality driven adaptive health monitoring (DQAHM) system model to include several parameters in order to achieve an effective real-time HMM for a CPS. The DQAHM model includes the CPS resource constraints, the criticality of each CPS component, the resource requirements of the HMM system, and the required diagnosis quality. All these are used to control the CPS sensors activation frequency in order to optimize the overall system diagnosis quality. The approach is completed by a decision making tool to dynamically calculate the adaptive HMM system configurations. One interesting approach consists in the employment of adaptation services within the CPSs. These can be used to improve dependability in instrumented CPSs based on the principles of "computational reflection" as paper [17] shows. It separates the way of dealing with dependability into notions of infrastructure and information dependability, and illustrates the need to formally model the CPSs and their dependability requirements. Formal models can help in the process of designing cross-layer adaptation techniques at different CPS layers in order to achieve end-to-end dependability at both infrastructure and information levels.

The three approaches presented above emphasize the need to develop CPSs middleware components (e.g. semantic ontology, adaptive and formal models) dedicated to analysing and modelling the dependability of this type of systems. However, the development of these components has to be performed in a committed framework. On this line, paper [18] proposes a methodology for the design and development of CPSs in order to meet all the hardware and software classes of failures. The methodology unifies software engineering with a series of feedback control laws, and with efficient resource monitoring in a formal way.

Despite the work done so far on assuring dependability in CPSs, there are no comprehensive methodologies to support the dependability analysis of these systems. This represents the main motivation of this paper. The proposed methodology combines the primary dependability analysis techniques with the representation of knowledge in order to support the development of CPSs capable to model the dependability at run-time. The ontology is an appropriate method to represent the CPS knowledge in terms of dependability. In this context, a brief analysis of the current ontology development methodologies has been made.

2.2. Ontology development methodologies

Among the ontology generation methodologies developed at the beginning of this research area, the ones listed below are distinguished. The methodology presented in [19] is an ontology dedicated to the modelling of the processes within an enterprise, while the methodology in [20] is a business processes and activities modelling domain ontology. The methodology mentioned in [21] investigates the feasibility of knowledge reuse in complex systems.

METHONTOLOGY enables the construction of ontologies at the knowledge level, and includes: the identification of the ontology development process, a life cycle based on evolving prototypes, and particular techniques for carrying out each activity [22]. SENSUS is an ontology for use in natural language processing, developed to provide a broad-based conceptual structure for developing machine translators [23,24]. A comparison between these methodologies demonstrates that they are not unified, and that they are specific to particular domains [25].

In order to respond to the need for the development of methodologies that facilitate knowledge reusability and scalability, and that support the collaborative and distributed construction of ontologies, the DOGMA and DILIGENT methodologies have been proposed [26]. DOGMA addresses ontology reusability and scalability by separating the specification of ontology concepts from the specification of their axioms [27,28], while DILIGENT proposes a collaborative and distributed construction process for ontologies [29]. Also, in the context of ontology-based multi-agent systems, the Onto-Agent methodology has been proposed. It unifies the DOGMA approach and the multi-agent system design methodologies [30].