Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020) Pp-271-275

BBRC
Bioscience Biotechnology Research Communications

Test Strategies for Cyber Physical Systems

Rashmitha H.R, Naresh E and Vijaya Kumar B.P
Department of Information Science and Engineering, M.S. Ramaiah Institute of Technology, Bengaluru, India

ABSTRACT

Cyber Physical Systems has been perceived as a standout amongst the most engaging area with fast development in enormous scale enterprises. That uses computer-based algorithm to control and monitor the mechanism. In this paper, a variety of testing strategy approaches are implemented to see each of their diverse roles in the field of Cyber Physical Systems with their different functionalities and use. The existing paper showcases a single strategy with in depth knowledge about the domain. The proposed model of three tier architecture grandstands assortment of testing procedures with their measurements that can be utilized in various periods of a Cyber Physical System model. Subsequently, of all the distinctive testing's on a Cyber Physical System there is additionally a little look at changed surges of testing methodologies, the tools that are popularly used in the fields, jobs that are available on the domain and research opportunities in each of these streams.

KEY WORDS: CYBER PHYSICAL SYSTEMS (CPS), TESTING STRATEGIES, EFFICIENCY, SOFTWARE, VERIFICATION AND VALIDATION

INTRODUCTION

Cyber Physical Systems (CPS) is characterized as a control and screen in various instrument with computer based calculations, which firmly interconnect the end clients with the web. They are beneficial in many ways, as in performing countless calculations simultaneously; ensure the safety and efficiency of the real world, processes very quickly. Notwithstanding, due to the extending enormous scale towards the area, high unusualness (Xin et al. 2018) and threats which can incite tremendous money related incidents or security break-ins.

The proposed work showcase the diverse testing strategies, that are used in CPS with a set of functionalities in the CPS architecture their important roles that help in identifying failure, fault, error the bugs in Cyber Physical Systems, these set of elements are done as a precautionary step towards the safety and security of the CPS models. It's carried out before the requirements gathering, in sub-phases and at the end of resultant product delivery.

The different set of important tools that are used in Cyber Physical Systems are explained in detailed with the most popular and frequently used tools in the industries, that tells the importance of CPS all around the globe with their new steady development in size from recent years. A case study on the thermostat using one of the testing strategies is proposed.

II. Related Work: The use of Cyber Physical Systems on to other domains give in an clear view of how the domains affect and strategies that can be used in order to give an accurate result during testing (Cyber Physical System Lab Projects at, www.cpse-labs.eu), Cyber Physical Systems have diverse set of strategy as in reliability and evolution in the internal and external factors of the CPS proposed by (Li and Kang 2015). The doping tests for the CPS which enables the growth of the equipment products with embedded software was given by Sebastian Biewer and

ARTICLE INFORMATION

*Corresponding Author: rashmitha.hr.hs@gmail.com
Received 11th Oct 2020 Accepted after revision 27th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31)

Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.13/40

Pedro R.D'Argenice (Biewer et al. 2018). The Model-Based testing on CPS where each of the sub-components in a model are tested with different model system proposed by Michel Adriaan Reniers and Mohammad Reza Mousavi in 2017 [(Aerts et al. 2017).

A. CPS and Embedded Systems: An embedded system is an independent framework that joins components of control rationale and true association. In contrast to a CPS, in any case, an embedded system is regularly restricted to a solitary gadget, while CPS may include numerous constituent frameworks and gadgets. Embedded systems ordinarily have a set number of undertakings to finish, with programming and equipment components planned explicitly to accomplish those errands, normally with restricted assets (Parameshachari et al. 2017).

B. CPS and Internet Of Things (IoT): IoT and CPS share numerous difficulties, yet there are a few refinements. IoT has a solid accentuation on particularly recognizable and web associated gadgets and implanted frameworks. CPS building has a solid accentuation on the connection among calculation and the physical world (example, between complex programming and equipment parts of a framework). On the off chance that the business works with IoT, especially in the event that it incorporates communicating with the physical world by means of with sensors as well as actuators (Rajendrakumar & Parvati 2019).

C. CPS and System Of Systems (SoS)

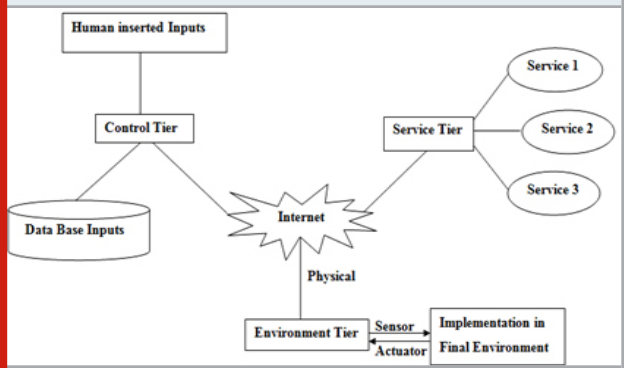
CPS and SoS likewise have many shared interests. Numerous CPSs are included autonomous constituents, and, as SoS, CPSs likewise handle difficulties of adapting to reliable rise, development and conveyance. Notwithstanding, in spite of the fact that usually the case that CPS constituent frameworks are autonomous, it is anything but a characterizing trademark for a CPS. Similarly, in spite of the fact that it's regularly the situation that SoSs do fuse components of calculation just as genuine connection, this isn't a characterizing property of a SoS.

III. Proposed Model: A model of 3-tier architecture is proposed for service-based Cyber Physical Systems, obtained from (La & Kim 2010; Hu et al. 2012), as shown in Figure 1, systems which consisted of two motivations they are as follows:

- **Motivation – I:** Tells about the comprehensibility of portable systems, for instance in Wi-Fi and 3G, using versatile web arrangement of Cyber Physical Systems which requires a decent dimension of organize availability winds up doable and broadly accessible.
- **Motivation – II:** Tells about the service technologies that can solve the resource limitation in a physical system, hence Cyber Physical System functionalities solve the limitation of resource problems.

The motivation gives in the proposed model which is a general accord on what Cyber Physical System is the thing that it can do and how it's very well utilized. But there are few drawbacks in its key elements; the architecture defines those key elements such as: Physical gadgets are associated over system to the control framework, which performs key calculations, software

Figure 1: Cyber Physical System Architecture



usefulness isn't firmly coupled to equipment components and Cyber Physical System requires ongoing and on-request preparing.

The Cyber Physical System consists of three main tiers as shown in fig 1 and description of architecture is as follows:

1. **Control Tier:** Is a get observed information, which is assembled from sensors to settle on controlling choices. Discover's the right administrations by counseling the service framework's data base and to let the administrations conjured on to the physical device.
2. **Service Tier:** Is a run of the registering condition with a set of benefits in service oriented architecture and cloud computing, with which various administrations are conveyed on to the service repositories and follows' a service framework, dials with the administrations and associates with the administration buyers.
3. **Environment Tier:** Comprises of physical gadgets and objective condition which incorporates, end clients using all the gadgets and their respective related physical condition.

IV. Testing Tools: A tool can be a programming device or a product creating apparatus which is utilized by the designers to troubleshoot, keep up, make an application, and so forth. A tool can be physical object or a program that help the developers to remove all the bugs in their product or any means of source. There are around 3000 – 5000 set of different tools.

A. Verification and Validation Tool: The hardware and the software components of the Cyber Physical System need to be tested for external and internal bugs which can be done by the Verification and Validation tool (Baheti and Gill 2011). The middleware for the system and Operating System should be developed by the developers that has to exceed beyond the future technologies so as to achieve the goals for the upcoming future problems, it requires a set of complex integration, methods, algorithm which are continuously checked for error, failure, fault free

products such tasks are carried out by the Verification and Validation tool.

B. KRONOS Tool: Gives the exact amount of reachable problems that might occur in the computation and verifies models from the real time systems with respect to the requirement specification of a real time framework (Nuzzo et al. 2015). The tool uses an approach called as the Back- Ward-Forward analysis method which extends the support towards the Hi-Tech automation.

C. d/dt Tool: This was the primary apparatus that gave the check for complex cross breed frameworks in the elements, which gives a reachable arrangement of approximations which is constrained in adaptability (Nuzzo et al. 2015). SPACEEX is a sub-tool in d/dt that improves in scalability, where 100 variables of a model have been analyzed.

D. CHECKMATE Tool: Is a MATLAB apparatus for the confirmation of straight and structure elements in a half and half frameworks of Cyber Physical Systems. An extended set of tool is the HSOLVER which supports the systems with non-linear dynamics (Nuzzo et al. 2015).

E. KEYMAERA Tool: A verification tool for the Cyber Physical Systems that gives proving of theorem automatically, which combines all the mathematical functions of algebraic components of real worlds and the systems algorithm to give a proving of the automated theorem (Nuzzo et al. 2015). Is a tool that is best suited for verifying the hybrid systems and proven for avoidance of collision among one system to another.

F. BREACH Tool: Is the first tool for simulation verification for Cyber Physical Systems, is a MALAB/C++ toolbox. Used for security reasoning when there is any sort of malware during the testing phase. Gives verification to different set of temporary logic properties and framework dynamics of the system. It supports complex properties in CPS and synthesis parameters (Nuzzo et al. 2015).

G. DYMOLA or JMODELICA: An apparatus utilized for exhibiting and reenactment of fused and complex systems for use inside vehicle, avionics, process and various applications. It tailors the languages for the system models and simulation. That gives the modeling languages in a system that is specific to multi-physical systems (Nuzzo et al. 2015).

H. PESSOA Tool: Since there are limited set of tools for the large-scale Cyber Physical Systems, PESSOA is a tool that exploits different bi-simulations to implement the best set of efficient algorithm that is synthesis enough for the model in CPS (Nuzzo et al. 2015).

I. MATLAB Simulink and SCADE suite Tool: These are standout among the most noteworthy instruments in the organizations; these gadgets consistently start the thing structure with utilitarian model that gets all of the essentials for the functionalities of the system and later on moves towards the item and gear utilization (Zhu & Sangiovanni-Vincentelli 2018).

J. AML Tool: Is a mechanization ML which is an information position that is unbiased on XML for the capacity and trade of data modules from various areas as the mechanical structure, electrical plan, and so forth (Harrison et al. 2016). A set of different formats uses different sub-tools as CALX for the top level format, COLLADA for storage, PLC open XML for the control of logical storage.

V. Testing Strategies: Some of the most common known testing strategies is as follows that carries out Functional and Non-Functional testing's:

A. Reliability Testing Strategy: A CPS whose entire set of mechanism is controlled by a set of programs needs to have reliability and safety as it's an important factor. Reliability testing is any domain makes sure that the operations are performed without any failure for a specific period of timeframe and external environment (Reniers et al. 2017). Reliability testing for Cyber Physical Systems can be done for internal and external factors that are also considered as the safety measures.

B.Automated Testing Strategy: In Cyber Physical Systems the software that's been tested is separated from the actual software so as to control the overall execution of different tests and predict the actual outcomes.

In Cyber Physical Systems the required set of infrastructure needed for testing is gathered that's passed on to specializes testers as SysML (Chabot et al. 2018) where parallel testing of structure and behavior is carried out whose abstract and simultaneously models are designed before undergoing Verification and Validation process, where the actual automated testing is done for CPS.

C. Doping Testing Strategy: The Verification and Validation in CPS are for checking whether the item fulfills the goal. However, its seen that the initial interest of manufactures diverges from the general interest which was initially planned, so a software is being introduced to keep the general interest of the manufacturers (Parameshachari, et al. 2020). The software that's introduced is called as the doped.

The Doped software keeps all the manufactures on track but is often mistaken with cleaning software that has to be classified as the doping testing. Provides customer lock in making sure to keep the general interests of the manufactures black box tests are usually considered for doping test in CPS.

D. Model Based Testing Strategy: The SDLC is typically categorized as the use for Cyber Physical Systems design. A Model Based Testing is a testing of different phases of CPS model that can be easily implemented in the Verification and Validation model. An incorrect requirement specification leads to incorrect design that can be avoided with each Model Testing or checking the conformance testing in CPS. A conformance testing is

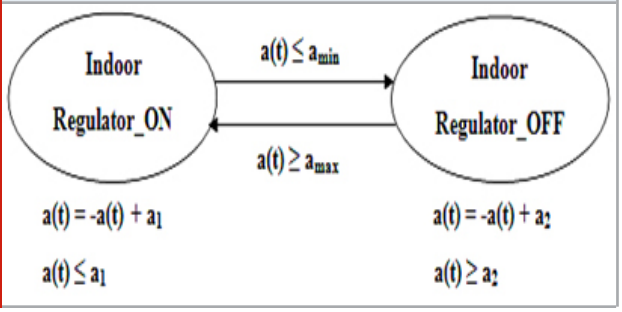
checking the correctness of the artifact parallel with its model that makes sure that the incorrect set of inputs from the specifications are eliminated.

E. Random Testing Strategy: Cyber Physical System has several components that are in need of testing and are tested normally. Random based technique is applied to trigger all the complex set of bugs by giving a set of random input that is later on checked with the outputs for fail and pass test cases of the variable. A quick check tool generates a set of random test cases, which results in finding a set of complex bugs which the human testers miss normally (Claessen 2018). Test cases are given to products to see the overcome.

F. Uncertainty – Wise Testing Strategy: Unlike the normal classical software testing, the Uncertainty Wise Testing tells the uncertainty about the systems behavior, its interaction to the environment, test design, test optimization, etc of a System Under Test (Ali et al. 2017).

Uncertainty – Wise Testing makes sure that the System Under Test meets the uncertainty and later on learns the new uncertainties that occur in phases as in the System Under Tests implementation, test case generators, optimizer.

Figure 2: Thermostat State-Model with $a_{min} \leq a(t) \leq a_{max}$



VI. Case Study Using Model Based Testing Strategy: To understand the concept of Model Based Testing a Case Study on the Thermostat is taken. The example is a framework that includes an indoor regulator gadget situated in a live with a window. Since the indoor regulator can be either completely ON or turned OFF, and no precise (criticism) control is connected, the framework is considered unregulated (Reniers et al. 2017). In Fig.2, a half and half robot model of the indoor regulator precedent is appeared. The elements a(t) of every mode speak to the temperature conduct in the live with the a(t) variable displaying temperature and the a1/a2 factors being input-subordinate temperature constants connected to the window position (input-subordinate framework), the temperature is controlled among amin and amax degrees. Consequently, by opening and shutting (to various degrees) the window elements of the framework gives in a value of true or false based on temperature_low which is as shown in Algorithm 1

Algorithm 1: A Discrete Behavior of the Indoor Indicator/Thermostat

```
Indoor_Indicator
{
Indoor_Indicator *: {ON, OFF}
        Indicator: = OFF;
        do
temperature_low = true -> Indicator: = ON;
temperature_low = false -> Indicator: = OFF;
    }
    return temperature_low
```

Table 1. List of Job Oppurtunities In Cyber Physical Systems (Jobs Provided with the field Cyber Physical System Tester, www.indeed.co.in)

Job Post	Company	Place
ICS Cyber Security Tester	Honewell	Duluth
Penetration Tester	1. ICF 2. Northrop Grammar	1. Norfolk, VA 2. Redondo Beach CA
Security Analyst	RSI Security	San Diego CA
Cyber Security Assessment and Compliance Specialist	General Dynamics Info Tech Booz	Washington DC
Cyber Penetration Tester Senior	Allen Hamilton	Mc Lean
Cyber Security Engineer	1. MELE Associates 2. Chenega Corporation	1.Washington DC 2. Fort Huachua, AZ
Cyber Physical Systems Security Researcher	1. PARC, a Xerox Company 2. Johns Hopkins Applied Physical Laboratory	1. PaltoAlto 2. Laurel, MD
Cyber Physical Analyst	Electrosoft Services	Rockville

VII. Research Scope In Testing CPS: A Cyber Physical System is one of the most highly scoped domain that initially evolved from network and now adopted to many of the fields. It includes expertise from streams as in automation, network control, etc. It has been highly adopted in countries as United States and Europe, where students are coming up with degrees in CPS. In India there is a complete committed researching in Robert Bosh Center for Cyber Physical Systems and Indian Institute

of Science; Headquarters – Bangalore, Karnataka, Year Founded – 2011.

Indian Research field of Cyber Physical System is more abundantly found in Robert Bosch (Robert – Bosch center for Cyber Physical Systems project facility in India, www.rbccps.org.) which consists of Faculty Participants, Inspire Faculty, Research Staff, PhD Student's, Project Staff, Administrative Staff and Visiting Professors. Researches about Cyber Physical Systems are carried out in other countries in US at Idaho Nation Laboratory in Idaho Falls, New York. The variety companies that provide jobs opportunities in Cyber Physical System is as shown in Table 1, where salaries are estimated to be around $ 70,000 - $ 120,000 in US Dollars and Rs 48,55550 - Rs 83,23800 in Indian Rupees.

CONCLUSION

In this paper, different diverse set of testing strategies and a proposed model for Cyber Physical Systems is given, where individual testing strategies is explained with their functionalities towards CPS different modeling phases. The most popular once include Verification and Validation known as VV model and Model Based Testing methods which are normally used for CPS testing. Different tools are stated for the phases internally and externally that gives optimal solutions for the bugs with in a Cyber Physical System. The goal is to give all the diverse approaches so that, the one who tests for CPS can use any one of the testing strategy that is suitable. The CPS gives different job opportunities in terms of analysts and research fields in the future scope of the software industry, that tells how the evaluation of Cyber Physical System has exaggerated over a period of five years till now. With different sub-strategies to develop an error, fault, failures free system.

REFERENCES

Aerts, A & Reniers, Michel & Mousavi, Mohammad. (2017). Model-Based Testing of Cyber-Physical Systems.

Ali S, Lu H, Wang S, Yue T, Zhang M "Uncertainty-wise testing of cyber-physical systems", InAdvances in Computers, Elsevier, vol. 107, pp. 23-94, 2017.

Robert – Bosch center for Cyber Physical Systems project facility in India, www.rbccps.org.

Claessen K, Smallbone N, Eddeland J, Ramezani Z, Åkesson K "Using valued booleans to find simpler counterexamples in random testing of cyber-physical systems", IFAC-PapersOnLine. vol. 51, no. 7, pp. 408-415, 2018.

Cyber Physical System Lab Projects at, www.cpse-labs.eu

Hyun Jung La , Soo Dong Kim, "A Service-based Approach to Designing Cyber Physical Systems," in 2010 IEEE/ACIS 9th International Conference on Computer and Information Science, Yamagata, 2010, pp. 895-900.

IoCT Cyber-Physical Systems Radhakisan Baheti and Helen Gill 2011. Available at www.ieeecss.org.

Jobs Provided with the field Cyber Physical System Tester, www.indeed.co.in

L. Hu, N. Xie, Z. Kuang and K. Zhao, "Review of Cyber-Physical System Architecture," 2012 IEEE 15th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops, Shenzhen, Guangdong, 2012, pp. 25-30.

M. Chabot, L. Pierre and A. Nabais-Moreno, "Automated Testing for Cyber-physical Systems: From Scenarios to Executable Tests," 2018 Forum on Specification & Design Languages (FDL), Garching, 2018, pp. 5-16.

P. Nuzzo, A. L. Sangiovanni-Vincentelli, D. Bresolin, L. Geretti and T. Villa, "A Platform-Based Design Methodology With Contracts and Related Tools for the Design of Cyber-Physical Systems," in Proceedings of the IEEE, vol. 103, no. 11, pp. 2104-2132, Nov. 2015.

Parameshachari, B.D., Panduranga, H.T. and liberata Ullo, S., 2020, September. Analysis and Computation of Encryption Technique to Enhance Security of Medical Images. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012028). IOP Publishing.

Q. Zhu and A. Sangiovanni-Vincentelli, "Codesign Methodologies and Tools for Cyber–Physical Systems," in Proceedings of the IEEE, vol. 106, no. 9, pp. 1484-1500, Sept. 2018.

R. Harrison, D. Vera and B. Ahmad, "Engineering Methods and Tools for Cyber–Physical Automation Systems," in Proceedings of the IEEE, vol. 104, no. 5, pp. 973-985, May 2016.

Rajendrakumar, S. and Parvati, V.K., 2019, January. Automation of irrigation system through embedded computing technology. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (pp. 289-293).

S. Biewer, P. R. D'Argenio and H. Hermanns, "Cyber-Physical Doping Tests," 2018 IEEE Workshop on Monitoring and Testing of Cyber-Physical Systems (MT-CPS), Porto, 2018, pp. 18-19.

Z. Li and R. Kang, "Strategy for reliability testing and evaluation of cyber physical systems," 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 2015, pp. 1001-1006.

Zhou, Xin & Gou, Xiaodong & Huang, Tingting & Yang, Shunkun. (2018). Review on Testing of Cyber Physical Systems: Methods and Testbeds.