Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Fortifying the Resilience and Integrity of Cyber-Physical Systems through Meticulous Assessment

Shantanu Bhadra[1], Anudipa Goon[1], Dr. R. Naveenkumar[2], Soumya Roy[1], Tanu[3], Dr. Jayanta Aich[4]

[1]Assistant Professor, Department of Computational Science, Brainware University
[2]Associate Professor, Department of Computer Science and Engineering, Chandigarh College of Engineering, Chandigarh Group of Colleges, Jhanjeri, Mohali
[3]Assistant Professor, Department of Electronics and Communication, Chandigarh College of Engineering, Chandigarh Group of Colleges, Jhanjeri, Mohali
[4]Associate Professor, Department of Computational Science, Brainware University

This paper examines the myriad factors impacting the reliability of Cyber-Physical Systems (CPSs), both internal and external. It introduces a comprehensive strategy for testing and evaluating CPS reliability, which incorporates technological frameworks and processes. The primary emphasis is on assessing the reliability of components across hardware, software, and architecture, along with evaluating performance reliability that covers service, cybersecurity, resilience, elasticity, and vulnerabilities. A synthesized approach using multi-index methods consolidates these diverse facets into four key performance reliability indices, offering a holistic view of system reliability. The proposed strategy aims to significantly enhance the comprehensive and ongoing analysis of CPSs.

1. Introduction

Cyber-physical systems (CPSs), introduced in 2006, represent the integration of computational algorithms with physical processes. These systems are becoming increasingly essential to various foundational services and industries that support daily life and operations. Given their pervasive deployment, ensuring reliability and safety is paramount for CPSs the systems' interdependence and ability to propagate failures among themselves might have disastrous effects if they fail or are attacked. Inadequate comprehension of failure mechanisms and inadequate testing and verification lead to frequent failures and accidents. Therefore, it is crucial to investigate the causes of failures, guarantee system security and safety, and recover and get better after mistakes. Diverse viewpoints have been used in research on CPS testing

and analysis. The reliability of CPS software is examined by formal modelling, qualities that are static, and dynamic verification. To test and validate during the development process, modelling and testing techniques such as agent-based modelling, physical-entity service-oriented models, and the integration of diverse models are employed for verification and testing. A variety of quantitative analysis tools are used to study cyberattacks, including attack trees and various graph-based models. Additionally, the cyber risk of CPSs is assessed using hierarchical holographic modelling (HHM) and probability risk assessment (PRA). It has been observed that current research tends to overlook a comprehensive solution for the entire system, focusing instead on analyzing and testing individual components or key performance aspects. Consequently, this research examines both internal and external factors that influence the dependability of CPS.

OBJECTIVES

This research analyses the factors from within and outside that influence the reliability of CPSs. Taking into account the technological framework and procedures, a method for assessing and testing the dependability of CPSs is proposed. The framework includes a comprehensive reliability assessment of the entire system, along with tests and evaluations of its components, functionality, security measures, adaptability, and potential weaknesses The testing indices and methods are demonstrated in the processes of implementation.

IMPACT ELEMENTS ON THE DEPENDABILITY OF CPS

The primary determinants of CPS safety and dependability are failures, which are classified as internal and external.

A. INTERNAL FACTORS

Failures originating from within the CPS are referred to as internal factors. These include malfunctioning operational rules, flawed architectures, software bugs, and hardware malfunctions. Software and hardware are the fundamental components of CPSs. Hardware has software with calculating functions built in. Through wire or wireless networks, several components come together to realize functions like perception, link, calculation, and control . It is clear that for CPSs to operate properly, hardware and software are required. A network's topology and capacity allocation are defined by its architecture. System failures can also be caused by flawed architectures. Transportation faults can arise, for instance, if nodes that are susceptible to electromagnetic interference are grouped together in an irrational topological arrangement. Alternatively, a lack of capacity is probably going to result in traffic jams, delays, and/or data loss. The system's predetermined methods for responding to its own conditions and perception of its surroundings are known as operating rules. A flawed rule design will undoubtedly result in problems, just like with the architecture. The Western Systems Coordinating Council (WSCC) blackout, for example, was caused by faulty regulations. One trip caused the system to suddenly collapse due to an abrupt change in tide, significant voltage fluctuations, equipment overload, and equipment overload.

B. EXTERNAL FACTORS

The operating modes, environmental factors, and external attacks are examples of external elements that originate from outside the CPS and have an impact on the internal issues of the

systems. Environmental components include both social and natural conditions. Physical, chemical, and biological factors influencing the system are referred to as the natural environment. Under the impact of nature, hardware failures including wear, corrosion, and aging will happen. The external attack is malicious devastation from outside CPSs. Because of their direct connection to the internet, CPSs are vulnerable to dangerous cyberattacks such as worm viruses, distributed denial of service attacks, and assaults on routers or Domain Name Systems (DNSs).

THE TECHNICAL FRAMEWORK

Taking into account all the elements discussed, a technology framework is proposed that classifies internal aspects as objectives and external aspects as conditions, as shown in Fig. 1.

The evaluation and testing process consists of three components: structured analysis, dependability testing, and extensive assessment.

At the outset, a comprehensive review of both internal and external factors that impact the system's dependability is vital, as it establishes the groundwork for subsequent initiatives.

Subsequently, dependability testing comprises two elements: component reliability and performance reliability. The former focuses on evaluating the reliability of system components, including physical devices, software, and network design. Ensuring the quality of operations and measuring the reliability of these components is essential before proceeding with performance reliability testing.

Cybersecurity, resilience, adaptability, susceptibility, and service quality are among the Cyber-Physical Systems (CPS) performance criteria. Over time, CPSs' performance characteristics change along with their architecture and environmental circumstances

It is recommended that performance reliability be the primary criterion used to assess the long-term operational quality of Cyber-Physical Systems (CPSs)

FUNCTIONAL BENCHMARK AND PERFORMANCE METRIC

Let's consider two parameters, P and P_{th}. A component or system is deemed to have failed if $P \geq P_{th}$. Here, P is known as the performance parameter, while P_{th} is referred to as the functional benchmark

Performance Reliability The ability of a performance parameter P to reach or exceed the threshold P_{th} in a specified amount of time or through a prearranged mission scenario (or group of scenarios) in a realistic operational environment is known as performance reliability. Consequently, service reliability, cybersecurity reliability, resilience and adaptability reliability, and vulnerability reliability are all included in the performance reliability measurements for Cyber-Physical Systems (CPSs)

Each parameter's performance reliability is quantified by measuring values at predetermined intervals using accepted techniques, then statistically analysing the results.

In conclusion, a comprehensive analysis of the four performance reliability indicators is carried out in order to evaluate the overall reliability of the system. Comprehensive explanations of the testing methods are given in the sections that follow. Performance reliability testing is covered in Parts D through G, while component reliability testing is the

main focus of Parts I through III. Part VIII includes a thorough assessment of the system as a whole

I. TESTING FOR HARDWARE RELIABILITY

Cyber-Physical Systems (CPS) hardware can be divided into two categories: electronic and non-electronic components. Metrics like failure rate, mean time between failures (MTBF), and mean time to failure (MTTF) are frequently used in reliability assessments. The type of component, testing goals, data accessibility, and sample size all influence the metric selection.

Stress analysis, Delphi techniques, benchmarking against comparable devices, and experimental testing are common ways to assess hardware reliability.

II. SOFTWARE RELIABILITY TESTING

Prior to deployment, software reliability testing is mostly carried out with an emphasis on compatibility and safety. Fault Tree Analysis (FTA) and Petri nets are examples of reliability analysis methodologies. Formal modelling approaches that depend on model validation and theorem proving are also used. For safety evaluation, direct testing techniques based on interface grammar and error guessing are also employed. Making ensuring the program functions well with hardware and other software systems is the goal of compatibility testing.

III. CONNECTIVITY RELIABILITY TESTING

The network architecture serves as the foundation for Cyber-Physical Systems (CPS) to share resources, connecting various units for data exchange and collaboration The architecture's ability to sustain system operations is shown by connection reliability. This reliability can decrease due to network disconnections. Here, "network" encompasses not just the communication systems but also all interconnected structures that facilitate the transfer of materials and information. Road closures can have a detrimental effect on link dependability in logistics networks, for example. Goods delivered late or to the wrong place jeopardize the system's overall performance reliability.

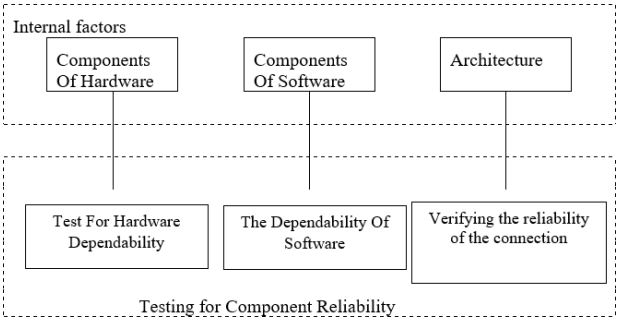

Fig. 1: Testing and evaluation technology framework

IV. ASSESSING SERVICE RELIABILITY

CPSs are capable of providing a variety of services. So there are several parameters to reflect service quality, such as time delay and error rate for networks and communication, CPU utilization for data centres, and so on. The most efficient technique to verify service reliability is to monitor all of the required indicators throughout operational time and statistically analyse

the data

V. EVALUATING DEPENDABILITY OF CYBERSECURITY

Monitoring system usage, which includes keeping an eye out for cyber attacks, identifying odd behaviour, and doing real-time security assessments, is a common component of cyber security testing. The steps are as follows: The first step is to create an evaluation model that takes into account possible risks, system reliability, and asset significance. Secondly to gather information related to these three aspects to proceed with the evaluation. By analysing network attacks, system vulnerabilities, and asset characteristics, the required data is obtained. Next, the likelihood of regarding the system failure or performance degeneration is determined based on identified threats and system reliability, while potential losses are estimated according to asset value The assessment methodology is used to determine the target nodes' security state. Finally, use the hierarchical evaluation model to evaluate the system's security grade based on node relevance. This paradigm follows a bottom-to-top evaluation policy, with a focus on local and global perspectives. Performance reliability is computed over time using a collection of cyber security testing variables and a threshold determined by security demands

VI. EVALUATING RESILIENCE AND ELASTICITY RELIABILITY

Elasticity refers to a system's capacity to adjust its configuration and resources to meet changing needs. Resilience refers to a system's ability to react to faults and continue operating under predicted and unforeseen conditions. Profile testing involves loading various profiles onto the system to monitor its behaviour. This method effectively evaluates the system's elasticity. As shown in Fig. 2, various requirements, including adjustments in load (increases or decreases) and scaling (in or out), are incorporated into the profiles. The system’s elasticity is determined based on the quality of its responses.

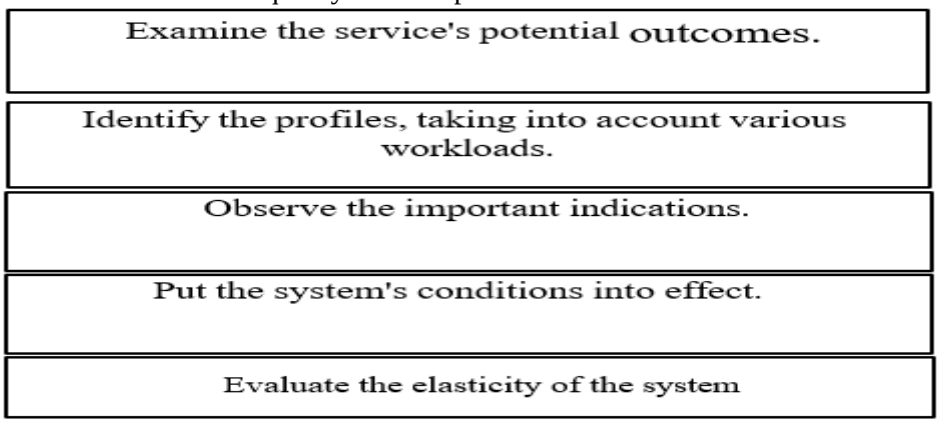

Fig. 2 Testing scalability and elasticity through profiles

Fault injection is a validation technique for fault-tolerant systems that involves conducting controlled experiments to observe system behaviour when faults are deliberately introduced. Faults are injected into the system to simulate failure scenarios. Fault injection techniques can be classified according to fault type—either hardware-based or software-based—and by

approach, either simulation-based or physical, depending on whether virtualization is applied. Resilience is assessed by monitoring the system's response to failures and disruptions, making fault injection an effective tool for evaluating resilience. Fig. 3 shows the resilience testing procedure.

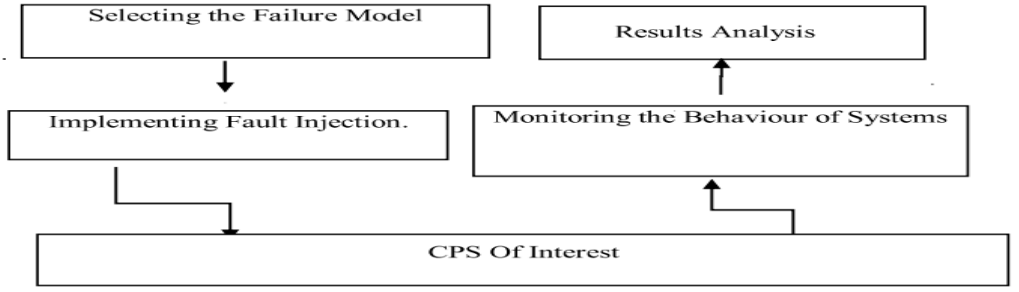

Fig:3 Resilience Testing Process

1. IDENTIFY THE FAILURE MODELS

Identify the target system inputs and move the chosen failure modes to the subsequent injection stage. The closer these chosen modes align with real-world scenarios, the more precise the results will be.

2. INTRODUCE THE FAULTS

Inject failure modes from the previous step into the target system using appropriate mechanisms.

3. OBSERVE THE SYSTEM'S BEHAVIOUR.

Monitor system behaviour based on testing objectives. Typical post-injection episodes include successful fault injection, detection, system recovery, and failure behaviour.

4. ANALYSE THE FINDINGS

A comprehensive test consists of independent experiments, each covered by four steps. When conducting a detailed test, it's important to consider the aims and confidence as the ultimate goal. Most evaluation methods rely on probability and statistics.

VII. VULNERABILITY ASSESSMENT RELIABILITY

CPSs are robust but fragile. Small incidents can lead to catastrophic outcomes due to failure propagation, making CPSs extremely vulnerable. Vulnerability is determined based on the likelihood of CPSs failing or being attacked. CPSs are characterized using complex network theory. Nodes represent system elements, while edges abstract the interactions between units. The susceptibility of the CPS is studied and analysed using complex network theory . The phases are presented as follows.

1. Preparation

Identify all potential external threats and failure modes relevant to the CPS. Next, create a knowledge base documenting the failure behaviours of the CPS.

2. System Modelling

Develop models of the network architecture and functional components of the CPS. These two aspects represent fundamental characteristics of the system and serve as inputs to understand its failure mechanisms.

3. Analysis of system failure behaviour.

Analyse the nature of system failure behaviours using system models and relevant inputs. Li Daqing's analysis of collected data reveals that traffic congestion in cities and power grid failures exhibit long-range spatial correlations, with these correlations diminishing gradually over distance

4. Analyze and calculate vulnerabilities.

Vulnerability evaluation is conducted using many technologies, including Monte Carlo simulation and percolation theory [29, 30]. By evaluating the system, we can identify important components or weak links.

5. Evaluation and Enhancement of Results

Through meticulous collection and analysis of evaluation outcomes, the vulnerabilities within the CPS are comprehensively assessed and confirmed. In light of these findings, strategic enhancements and preventive actions are recommended to fortify the system against potential collapse. The evolving vulnerability metrics over time serve as the foundation for determining the system's reliability, ensuring continuous operational resilience.

VII HOLISTIC ASSESSMENT OF RELIABILITY METRICS

After evaluating the entire system, including the reliability of individual components and overall performance, we gain insights into various aspects of the CPS's reliability. However, to determine the system's overall condition, it is essential to integrate all the results. A comprehensive assessment is crucial for effectively monitoring the CPS and identifying areas for improvement. Several factors influence the reliability of the system from various perspectives. To assess the system's reliability holistically, a multi-index method is employed. This approach is well-suited for comprehensively evaluating the overall reliability of a cyber-physical system (CPS). The weight assigned to each index reflects its relative importance. As illustrated in Fig. 4, the overall reliability score (S_{YR}) is determined by the weighted aggregate of four key indices: Service Consistency (S_c), Vulnerability Resilience (V_R), Robustness and flexibility reliability (E_R), and Cyber Resilience (C_R). The evaluation process is expressed through the equation below, where β_i(for i=1,2,3,4) represent the respective weights of these indices.

$$S_{YR=} \beta_1 S_c + \beta_2 V_R + \beta_3 E_R + \beta_4 C_R$$

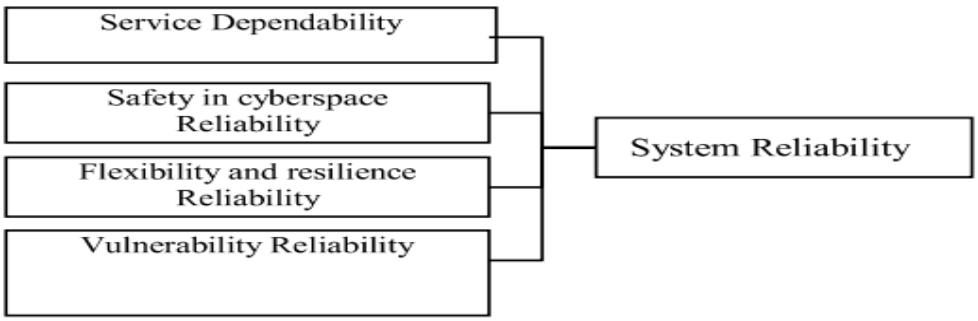

Figure 4: Holistic Evaluation of System Reliability

2. CONCLUSION

This research explores internal and external factors that impact the influence reliability of CPSs. This study proposes an approach for evaluating and testing CPS dependability, focusing on aspects like technology frameworks and associated processes. The major effort involves testing and evaluating component dependability (hardware, software, and system architecture), along with performance reliability factors such as service stability, cyber security, resilience, elasticity, and vulnerability control. The multi-index method synthesizes the four performance reliability indices to provide a comprehensive overview of system dependability. This strategy ensures ongoing, comprehensive evaluation of CPSs, combined with the technical planning necessary for developing a test bed.

References

[1] Bao, J., & Wang, L. (2014). Reliability evaluation and optimization of cyber-physical systems. IEEE Transactions on Reliability, 63(2), 461-470.

[2] Dr R. Naveen Kumar, Amit Kumar Bhore, Sourav Sadhukhan, Dr G. Manivasagam, Rubi Sarkar "Self-Monitoring System for Vision-Based Application Using Machine Learning Algorithms" DOI: 10.5281/zenodo.10547803, Vol 18 No 12 (2023), Page No 1958 –1965, Published on 31-12-2023.

[3] Chowdhury, S., & Banerjee, S. (2022). FARE: A framework for benchmarking CPS reliability. CORE Proceedings, 15(1), 22-34.

[4] K.Yemunarane Dr. R Naveenkumar Trisha Nath R. Sasikala Nitin Kumar Jayasheelan Palanisamy "A Pragmatic Research Approach On Artificial Intelligence In Content Delivery Through SDS Technologies", 2024/11,Nanotechnology Perceptions, Volume20, Issue14,Pages2235-2249.

[5] He, Z., & Zhao, M. (2020). Evaluating active distribution networks as part of CPS. Journal of Cyber-Physical Systems, 9(4), 56-73.

[6] Hussain, A., & Shah, Z. (2021). Optimization and reliability modeling for CPSs in hazardous environments. IEEE Industrial Informatics, 17(2), 112-129.

[7] Kang, J., & Lin, Z. (2019). Simulation-based testing for autonomous CPSs. IEEE Control Systems, 38(1), 45-58.

[8] Kim, D., & Lee, H. (2021). Advanced fault detection for smart grids within CPSs. IEEE Transactions on Smart Grid, 12(3), 1456-1469.

[9] Liu, F., & Tan, Y. (2020). A quantitative reliability model for CPS communications. International Journal of Cyber-Physical Systems Engineering, 5(2), 98-120.
[10] Ma, X., & Zhang, J. (2018). Cross-domain analysis of reliability in power CPSs. SSRN Journal on Cyber Networks, 24(2), 201-215.
[11] Mei, H., & Zhao, S. (2022). Reliability testing framework for industrial CPSs in Industry 4.0. Springer Manufacturing Science, 18(4), 289-302.
[12] Nakamura, T., & Yamashita, A. (2019). Fault injection testing for CPS safety analysis. Safety Science, 121, 12-24.
[13] Park, J., & Kim, C. (2023). Techniques for evaluating software reliability in CPS. Journal of Software Engineering, 31(1), 67-79.
[14] Qian, Y., & He, L. (2021). Performance-based reliability metrics for smart CPS devices. Journal of Embedded Systems, 42(2), 34-49.
[15] Ren, W., & Wang, X. (2020). Reliability modeling and optimization in distributed CPSs. Journal of Network and Computer Applications, 164, 102-119.
[16] Santos, P., & Costa, R. (2018). Real-time fault management in CPS. IEEE Internet of Things Journal, 5(6), 4823-4834.
[17] Smith, J., & Green, K. (2019). Balancing redundancy and reliability in CPS design. Journal of System Architecture, 25(2), 66-78.
[18] Tang, J., & Wang, F. (2023). CPS resilience strategies using predictive maintenance. Reliability Engineering and System Safety, 230, 108913.
[19] Varga, P., & Török, M. (2022). Exploring CPS reliability through empirical testing. Springer Internet Technologies, 7(1), 88-103.
[20] Wang, H., & Zhou, L. (2021). Temperature-constrained reliability optimization for CPSs. IEEE Transactions on Industrial Electronics, 68(5), 4412-4424.
[21] Xu, L., & Guo, F. (2020). Techniques for enhancing CPS robustness. IEEE Transactions on Cybernetics, 51(3), 1586-1598.
[22] Yang, C., & Zhao, P. (2018). A framework for CPS vulnerability testing. International Journal of Critical Infrastructure Protection, 23, 100-110.
[23] Yu, D., & Kim, H. (2023). Adaptive testing strategies for complex CPSs. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 54(3), 321-332.
[24] Zhang, Y., & Sun, L. (2022). Metrics for measuring CPS reliability in heterogeneous systems. Springer Cyber-Physical Engineering Journal, 4(2), 99-120.
[25] Zhou, X., & Chen, Y. (2023). A comparative study of CPS reliability methodologies. IEEE Transactions on Network and Service Management, 19(3), 117-129.