Using Formal Verification and Model Checking in Agile Development to Improve the Quality of Software Development: Review

Taimoor Hassan[1], *Abrar Ahmed*[2], *Mehmood Anwar*[3], *Muhammad Basit Ali Gilani*[4], *Sajid Saleem*[5]

taimoor.hassan01@ucp.edu.pk[1] *ibe9212@gmail.com*[2] *mehmoodanwar175@gmail.com*[3]
basit.gilani@ucp.edu.pk[4] *sajid.saleem@ucp.edu.pk*[5]

[1]*Department of Software Engineering, University of Central Punjab, Lahore,*
[2,3]*Department of Software Engineering, The University of Lahore, Lahore,*
[4,5]*Department of Computer Science, University of Central Punjab, Lahore, Pakistan*

Abstract- In this paper, analysis the efficiency of software development through modeling checking, formal verification and different tools that is supported to develop it. A lot of real-life examples are quoted in this paper. Implement different model checking techniques, STPA methods and analysis on game development, railway management system and other sectors. In the innovation and huge development in software industries, we must heavy knowledge about software engineering course and must taught in universities. Software engineering plays a vital and great role in development of software. In this paper, proposed the requirement divided approach, in which divide the requirements through filer vise, break it, priority them, numbering in specific order and convert it in requirement document. We well known that in every software development, requirements phase is major and initial phase and whole software development based on it. After that apply the testing tools to test it for quality purpose and customer satisfaction.

Keywords: System-Theoretic Process Analysis, Model Checking, Formal Verification, Agile Methodology, Scrum, XP (Extreme Programming)

I. INTRODUCTION

In this article, the author fills the gap in agile methodology for safety assurance systems using the integration of verification and innovative safety analysis which is based on STPA into the existence agile process model safe scrum. This study aims to increase the safe handling of the original safe scrum when they enhance the agility at an identical time. They adopt safe scrum using STPA by an adherent to the safety standards. In this study basically, they propose an agile development methodology process naming as S-Scrum and integrate the safety analysis including verification scrum. Further, they perform safety-guided design using agile with the interpretation of STPA and integrate formal verification process with model checking into a scrum for formal verifications of STPA in a code-level [1].

Model-checking approaches are the most powerful approaches that do emerge to verify requirements. Model-checking tools accept the system requirements or models and properties which are called specifications that the ultimate systems are probable to satisfy. The tools then output all correctly when a particular model satisfies input specifications otherwise, it generates a counterexample for the debugging process. This counterexample provides details of errors in the model. Through analyze the counterexample, this is promising to identify the sources of the errors in the model to correct these errors in the model and retry verification of the model. The initiatives are to make sure that the model satisfies satisfactory system properties, we enhance our self-confidence to ensuring the correctness of the model. The system requirement is to model because they correspond to requirements and design [2].

Formal verification using agile methodology is not an easy task because an error in the library or core framework can affect the whole application developed with this framework [6]. So, for this reason, the framework must be in a stable state for any specific domain of application in which they are needed to change. Thus, formal verification of the agile framework is an important property for changing in the application context. Gaining effective comprehension became highly crucial for software development when the continuous agile framework is evolved in the process. In this study, the author proposed a method for the verification of behavioral properties for agile methodology by applying model checking techniques [2].

For software development activities to achieve systematic and rigorous technique formal method is used and this technique has significant [8]. The author claims that it is an important subject so universities should teach this subject to software engineering students. In this research article, they introduce elements for modeling and programming semantics. They give importance to model checking and discuss issues which are how to address the theory and practice of formal methods using model checking techniques [3].

There is a gap between adaptation of formal verification process and research specifically for game development, and for complex games construction of modeling is not an easy task. In this study, the author presents a novel approach that can significantly verify computer games concerning the formal verification process. For the above-mentioned purpose author used the model checking approach. The proposed approach significantly plays a vital role in multiplayer game development [4].

Designing the railway station control system is a central problem that is addressed in this research article. The main problem can be for example capacity of the railway station to handle many trains is enough or not to deliver batter services to the passengers if a large amount of people wants to travel same time. The author presents that this is the major problem which is addressed by capacity specifications suited language to construct the projects using verification of properties expressing such as running time, frequency of train, crossing, and overtaking. Hence planning problems can be solved. The author suggests a toll for efficient management and formal verification using fully automated performance verification and by using the nominal verification documents [5].

II. LITERATURE REVIEW

Progression seems to be an unavoidable part of the development process [2]. Traditional financial data structures include property continuous delivery environments. They suggest the template test plan towards full assessment with rapidly evolving software development. Those findings could be used to explain regression test selection management practices which define significant yet tacit conclusions regarding that platform's object model. Will test their theory as well as constructively steer additional research, we perform another commercially applicable interpretative phenomenological analysis.

Continuous delivery systems catch their current planning similarities within a group of similar programs. Structures can be used by computer programmers for growing minimizes expense of developing complicated applications. Implementations encourage reusability but fast implementation through limiting that number of potential approaches. It is not easy to verify input side together in structured way. Both terms of instructional with said system would be affected by failures throughout the requirements specification or repository. Methodologies were susceptible through modification, even since they are designed to either have consistent architectures within specific system realms. With the ever environment, optimization of the special feature of even an evolutionary architecture can neglect useful characteristics. Such as staff members, understanding where to achieve successful understanding inside this constant change towards system development architectures is becoming increasingly important. They give some recommendations for using template testing data to evaluate the behavioral characteristics for emerging evolutionary architectures together at operational site throughout this article [9].

The assumption is whether the findings will be used to further grasp, assess, but explain programmer management practices. Additionally, when using this structured method, certain essential yet tacit formats de that project's knowledge base can indeed be established.

Through documenting behavioral improvements from an optimal price, they further developed the template challenging position for efficiently verifying emerging continuous delivery systems. They believe here that technique seems to have a lot of benefit for welfare programs monitor programmer progression but appreciate your platform's object model, derived from the experience with being in the research paper. There is necessary for further rigorous scientific research.

Methods which allow until round synchronization among templates including system software should also be investigated deeper. Through centuries, there has also been debate upon where but not to use systematic approaches throughout application establishment and promotion. Addressing sustainable, they believe, will assist computer programmers towards gaining certain information, years of research [2].

They agree which practical challenges must be used in undergraduate computer science training because they often have standardized but comprehensive strategies towards project management [3]. They explain what they incorporated the variety through systematic approaches together into fundamental master's degree including Computer Programming. Inside those six sessions of something like the curriculum, they demonstrate whether they incorporate some essential components for modelling through piece of software terminology, but also how they approach that philosophy through experience regarding simulation studies.

They remain convinced which, throughout view with contemporary organizational commitment but rising preference towards user-defined market mechanisms, simplified structured approaches is included in specific educational information instructional design. Also, as result, at the Institution of Heidelberg, they are already providing another fundamental Supermodel Computer Science program including multiple incorporated structure refers to the way elements. They purposefully avoided hypothesis proofs including justification procedures regarding programmer accuracy, such as Fuzzy soft type programmer verification (most of which are covered in depth in several other electives) since they wanted to always have flexible methods with a poor retention barrier, convenience with relatively confident small-scale application, including strong convenience with integrating together in full-fledged template indicator.

Although rising Systematic Approaches are still being used, they agree which Apache Functionality are being allowed access to yet another century with Computer Programmers becoming well with your simple line of work schooling because they need some thorough understanding of technical principles including methodologies. That unwilling to learn that domain-specific view, to think in terms of domain-specific objects, also succeeded for becoming a commonplace throughout classrooms inside a decade, defining themselves traditionally also as “native speakers” for information dissemination.to them the paper clarifies things together in manner in which both the a consumer but a device will interact through their, including the capabilities to accomplish verifications against latest studies of something like a device, are really the keys to something like a deeper comprehension here between practitioners, especially Computer Programmers.

Some other benefit seems to be the instilled commitment through competence which really goes with both the opportunity through practice through checking soon but regularly, using techniques which have an impartial view (instead of just consumer investigations) and even a twentieth reproducible result. Some other benefit seems to be the instilled commitment through competence which really goes with both the opportunity through practice through checking soon but regularly, using techniques which have an impartial view (instead of just consumer investigations) and even a twentieth reproducible result.

Along with all the shortcomings but pitfalls because they are aware of during tomorrow's News talk technologies and methods, this an initial move against responsibility regarding choices and consequences represents, their view, a critical turn through clinical competence.

Further than the development of technology, that goal is to create a different culture as well as commitment inside this Computer Programming community.

They assume which comprehensive approaches' contributions towards the creation with the next century of computer programmers becomes essential, therefore that they will be considered crucial component throughout undergraduate computer programming instructing there at Bachelor of Arts level. For their sophomore decade, students study software engineering including academic areas before completing introductory classes including algebra, equations, design patterns, including scripting with their first season. As little more than a result, certain programs were appropriate towards integrating maintain quality methodology instruction together into traditional bachelor programmer [7].

They began reforming that historically somewhat conservative Instructional Design program, that also resulted in a full shift theory through organization. Both as result, they created better lessons that they have refined but expanded and even now, focusing on instructional practices including mindset instead of just statistics as well as methodologies., that revised edition began with dynamic, methodology approaches, introducing structured processes during the first instance inside this curriculum while implementing three conditions with physical recovery further into [3] multiple curriculums.

For today's positive emotion, scrum will become increasingly popular [1]. Lean principles, is from the other hand, have been criticized because of being insufficient again for implementation of appropriate operating system due to the shortage with quality management operations.

Besides quality management, quality of decision as well as protection verification becomes track of multiple. Though, typically focuses upon waterfall-style operations. As a result, sufficiently improved security assessment tool must be integrated throughout scrum processes that drive technology creation as well as validate their research ethics somewhere at application staged at just the software stage, double-check the development's safety. One such article introduces D up, just one new adapted waterfall prototype considering design phase "Protected Rolling maul" but instead enhanced with a protection analytical technique but a security verification attitude related to Statistical Project Planning. That current iterative learning method the essential dimensions of the D up are executing safety-guided construction by STPA inside each sprint and completing the D up.

Form validation is used to validate protection specifications somewhere at specification stage. Software safety quality of decision replaces conventional Consistency, Accessibility, Data integrity, and Protection evaluation upon this finished version. Certain dimensions of the originally Protected Agile development are adopted. Maneuverable are known with increased sales, reduced regression coefficients, shorter production cycles, though as a response towards varying complexities.

Nonetheless, scrum teams towards designing protection applications have drawbacks. While current methodology emphasizes service delivery, best practices really have not proved for being sufficient to ensure consumer protection. Some investigators usually mix that flexible technique alongside conventional construction phase that depend upon security requirements while developing compliance throughout regression testing. As little more than a workaround towards defense applications, which aim that strike the right balance between orders with versatility.

Although the environment itself constantly shifting, that equilibrium will become a barrier. With conventional security mechanism, structure plays a critical role throughout the fundamental risk assessment. even with aim of determining systems engineering conditions including limitations throughout order to bring its stable model. Which is seen to be more effective and efficient that traditional approaches in a range of systems? Here, another unique STPA-based requires a certain level assessment through verification framework is developed. Researchers have extended this to a holistic project management methodology that had prompted everyone to adapt that strategy to something like a pre-existing iterative methodology involving conservation applications called Secure Methodology.

They focus toward incorporating that quality management-oriented security research through compliance verification via lean development. Through their article, we suggest an incremental project implementation that has been in the designing phase. In that same article, they broaden Secure Ruck by incorporating an innovative STPA-based protection review through verification technique, which they suggest D up both as new project implementation. They will use an evolutionary project implementation including protection applications with something like a protection insecure framework if they do it the same way. We will look at just the volatile frameworks that discourage lean principles from being used in protection process.

When deal with evolving environments, they incorporate another creative hazard identification approach called protection development. Those simple formulas Spinning performs that verification of something like the power saving, smoothly supporting that ongoing production with [1] protection applications.

Locomotive capability remains difficult to define but assess, although current methodologies that are being used necessitate detailed descriptions including its train system including itineraries [5]. Software developers operating for small building sites claim how they have no choice but to use informal, knowledge capability analytic techniques.

Deliberate integrated application with tracks becomes usually done upon this size with rail transportation services, with extensive feedback regarding facilities although schedules, only after the whole plan becomes finished. Their purpose is to create other steps to implement which method that will solutions provider through specifying capability products also at planning phase through immediately checking them.

Towards being scalable, that method should provide realistic sampling rate and as such the verification can indeed be performed upon this fly whereas a programmer updates their specification in a formatting framework. There were also minor flexibility vulnerabilities in architectures that are still found very later, once provider schedules were created – there seems to be a discrepancy seen between scale for building schemes and thus the nature for performance evaluation even if it is done.

They propose another vocabulary through describing property including battery life, track rate, approaching, including crossover that is suitable with megaprojects. Ascertaining that property entails addressing other scheduling problems with boundary element device structure, available bandwidth, theory of evolution, including minimal connectivity as constraints. Fitted regression mathematical methods can be used to explain rail mechanics, and yet when formulated intelligently, they yield pseudo solutions about input output.

They contend which existing situation algorithms are inefficient when arguing throughout this whole discontinuous global optimum. Rather, they built other particularly unique governing equations that divide those methods into three parts: differentiated Decided to sit dispatched scheduling including prolonged mechanics as well as played a vital role analyzed through computer simulations. In a neutralize directed integration refinement, those different parts interact. Research study highlights another major issue arising whenever planning subway station layouts including controllers: Seems to be the platform facilities able to perform that number of stations as well as the required traffic flow throughout order to obtain necessary operation through merchandise both mediated.

Their proposed Lockheed towards project management really does have the purpose of allowing bolt action output verification with small screen information. Any of these features allow reliability verification to have been incorporated throughout constantly evolving initial planning programmers, preventing that expensive and less time obfuscation that has been expected whenever subsequent review shows insufficient output. They really would like to incorporate new implementation through into software throughout the upcoming will verify its usefulness among designers who use the method throughout professional planning process [5].

With the ever film market, competitive social networks contribute significantly [4]. Throughout this sector, becoming efficient requires producing their finest applications available, thus stability is really a crucial aspect for increasing sales. Videogames are already being used towards mimic various mechanical devices when stability was far more essential although possibly life.

Application development verification methods could only verify some portion of most feasible programmer implementations, and they will never ensure that now the operating system is completely error-free. Simulation, but at the other end, have considered to be a useful tool through query processing with massive computing devices over past two decades. They introduce a method towards scientifically verifying gameplay throughout this document. They suggest another model-building approach which begins with the mobile gaming outline which employs the Fatigue Assessment techniques. This approach is applied to a practical example: your player Rabbit Conflict. At last, throughout attempt to remedy that government eruption issue, another method for system features extraction becomes presented. That difference among proper evaluation implementation throughout gameplay continues to remain broad. Due to significant scientific as well as scientific innovations, console manufacturers continue to use other tools, which are not analogous from other proceeding to the next phase.

Think the reasoning stems again from limited accessibility of custom firmware verification techniques, which mostly demand professional assistance and perhaps a complicated technical experience among designers, or either. Gamification assistance seems to be a new but developing new methods sector where currently lacks standardized methods that are being generally embraced but implemented in many other scientific fields of application. Each issue was addressed within that article, which they introduced another new methodology towards scientifically verifying sports.

They suggest another development of society approach based on Structural Inspection which really begins with a video game definition. The approach was tested upon this internet platform Polar bear smash also as literature review. Through way of even an illustration of verification with close resemblance through mobility including accident, another resolution again for country explosions question another method created with this motive was proposed.

Whereas the verification protocol shown in the practical example still was not swift, this methodology will also be researched when refined throughout attempt that can be used in conjunction with even more traditional Must processes, resulting in a rather accurate research methodology. secure sport may be used as a starting point for some more growth. Some other area of research that may have been pursued and in possibility seems to be the deterministic expansion of both the established industry framework that provide both for verification with bank".

The qualitative process would be used to develop automated micro networks, which are made densely interconnected artificial elements. Another very appropriate methodology seems to have been machine robots [4].

III. DISCUSSION

If we talk about software development, a lot of models and techniques are using to develop it. With the passage of time there is a huge development in this industry. Latest models, techniques, methods, and technology are use now a days to develop the successful software. Different models are used for the development of software like waterfall model, raid model, incremental model, and agile model in which use scram and XP (extreme programming).

In this review paper, we talk about agile methodology in software development and their different methods and techniques that are using in it. Talk about STPA (System-Theoretic Process Analysis) that is using in agile methodology for the purpose of safety measures and verify all the methods that are using in it for the development of software [1], [11]. The major aim of this study is to increase the safe handling of original pattern, when we enhance or update it, there is no identical change in its safety measures. In code level, apply the STPA and then integrate it with different formal verification process. The major purpose of all this exercise is to develop the error free and quality software.

The other major approach and technique that is using in software development in software requirements and specification phase that is model checking. Now a days, also use model checking tools that accept the input in the form of requirements and properties. Produce the output that is total accurate when a specific model satisfies all the input specifications [2]. In agile development, using formal verification is not an easy task because if there is any error in library or main file then that's effect on whole developed application or program [10]. In this, apply the different model checking techniques on agile development framework to produce the quality software and enhance it in near future. All these focuses on customer requirements because customer satisfaction is major aim of any software industry.

There is no software development without knowing the course of software engineering that is the core course teaches in universities [3]. In this paper, claims that it is an important subject that must be teach in universities. Also discuss the importance of modeling checking, their techniques and programming semantics. Using all these methods and techniques develop the quality software development [12]. Author major focus on formal method's theory and practice.

Now a days, there is huge success in game development [4]. Several companies working on it and gain maximum profit on game development but there is some gap in formal verification process and research specifically for game development. It is not an easy task in complex and difficult game development. In this research, author elaborate the novel approach to verify these processes to gain the successful game development. This definite approach plays a vital role specially in multi-player game development. In multi-player game have a lot of complexities and difficulties to manage point of view that is why need full attention and focus on it to develop useful games development.

In today scenario, railway station train processing and all elements that are associated with it play a major role in any country as well as also based on economy ups and downs [5]. If railway department is established in profitable way, then its contribution makes economy great and helpful for the country. Control system of railway station is the major problem that face all the passengers whose travel on them because most time this system is crash and all the information will be late and not up to the mark.

Another major issue for the railway station end is to handle a lot of passengers, timing schedule, travelling on same time passengers etc. The author address that by using capacity specification suited language, we will make railway station becomes automated and all the activities that is associated with it like frequency time, railway crossing, signals, station wait, stop on schedule stations, overtaking etc. With the help of toll, we will easily access and use the railway system and manage the overall infrastructure automated.

With the help of above discussion, we will say that without the valid modeling checking and formal specification, no software is built successfully because use of all these techniques becomes the software successful and profit gaining. The other side in software development major feature is software quality that plays a major role in any kind of software development. If the software quality vise not good, then its life or survival rate is too low in market and failed on customer end.

In the end, we talk about the proposed solution that will be very helpful for the software industries. Software developments have major focus on software requirements, if requirements are clear and valid then software development will be error-free and good in quality. If we use requirements divided approach in which divide all the customer's requirements. Starting with gathering requirements, filter it, break it in functional and non-functional requirements, prioritize the requirements, numbering them and finally converted in requirement document. This document transfer to development team. Using this approach, we will develop the quality vise software and make a great profit business and customer trust level.

IV. CONCLUSION

In this section, we conclude the paper in every aspect. Staring with the use of formal verification and model checking techniques apply on software development to enhance the credibility of software and gain maximum profit in market. Use the agile methodology model to develop the software. This paper describes the different authors work analysis on formal verification and model checking as well as software quality and assurance. Apply all these techniques on real life examples like railway management system, multi-player game, automated system etc. Due to applying these techniques, we will gain a successful and good software in quality vise and reliability vise. In the end, propose requirements divided approach to overcome such kind of problems that face in software development. In which divide the requirements through filer vise, break it, priority them, numbering in specific order and convert it in requirement document. Then actual document transfer to development team for developed the software.

REFERENCES

[1] Wang, Y., & Wagner, S. (2016, May). Towards applying a safety analysis and verification method based on STPA to agile software development. In 2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED) (pp. 5-11). IEEE.

[2] Niu, N., & Easterbrook, S. M. (2005). On the Use of Model Checking in Verification of Evolving Agile Software Frameworks: An Exploratory Case Study. In MSVVEIS (pp. 115-117).

[3] Bordihn, H., Lamprecht, A. L., & Margaria, T. (2015). Foundations of Semantics and Model Checking in a Software Engineering Course. In FMSEE&T@ FM (pp. 19-26).

[4] Rezin, R., Afanasyev, I., Mazzara, M., & Rivera, V. (2018, May). Model checking in multiplayer games development. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (pp. 826-833). IEEE.

[5] Luteberget, B., Claessen, K., & Johansen, C. (2018, October). Design-time railway capacity verification using SAT modulo discrete event simulation. In 2018 Formal Methods in Computer Aided Design (FMCAD) (pp. 1-9). IEEE.

[6] Owen, A., & Soni, A. A. (2025). Agile software verification techniques for rapid development of AI accelerators.

[7] Alam, M. M., Priti, S. I., Fatema, K., Hasan, M., & Alam, S. (2024). Ensuring excellence: A review of software quality assurance and continuous improvement in software product development. Achieving sustainable business through AI, technology education and computer science, 331-346.

[8] Anasuri, S. (2022). Formal Verification of Autonomous System Software. International Journal of Emerging Research in Engineering and Technology, 3(1), 95-104.

[9] Ilays, I., Hafeez, Y., Almashfi, N., Ali, S., Humayun, M., Aqib, M., & Alwakid, G. (2024). Towards Improving the Quality of Requirement and Testing Process in Agile Software Development: An Empirical Study. Computers, Materials & Continua, 80(3).

[10] Pasuksmit, J., Thongtanunam, P., & Karunasekera, S. (2024). A systematic literature review on reasons and approaches for accurate effort estimations in agile. ACM Computing Surveys, 56(11), 1-37.

[11] Nguyen, M. H., Chau, T. P., Nguyen, P. X., & Bui, N. D. (2025, April). Agilecoder: Dynamic collaborative agents for software development based on agile methodology. In 2025 IEEE/ACM Second International Conference on AI Foundation Models and Software Engineering (Forge) (pp. 156-167). IEEE.

[12] Ali, M., Khan, N. A., Sarfraz, M., Riaz, S., Mehmood, T., & Ghafoor, S. (2025). Exploring The Role of Exploratory Testing in Agile Software Development Environments. Spectrum of Engineering Sciences, 3(1), 425-472.