

# Automated structural testing of LLM-based agents: methods, framework, and case studies

Jens Kohl\*, Otto Kruse†, Youssef Mostafa\*, Andre Luckow\*, Karsten Schroer†, Thomas Riedl\*, Ryan French†, David Katz\*, Manuel P. Luitz\*, Tanrajbir Takher†, Ken E. Friedl\* and Céline Laurent-Winter\*

\*BMW Group, Munich, Germany

†Amazon Web Services

**Abstract**—LLM-based agents are rapidly being adopted across diverse domains. Since they interact with users without supervision, they must be tested extensively. Current testing approaches focus on acceptance-level evaluation from the user’s perspective. While intuitive, these tests require manual evaluation, are difficult to automate, do not facilitate root cause analysis, and incur expensive test environments. In this paper, we present methods to enable structural testing of LLM-based agents. Our approach utilizes traces (based on OpenTelemetry) to capture agent trajectories, employs mocking to enforce reproducible LLM behavior, and adds assertions to automate test verification. This enables testing agent components and interactions at a deeper technical level within automated workflows. We demonstrate how structural testing enables the adaptation of software engineering best practices to agents, including the test automation pyramid, regression testing, test-driven development, and multi-language testing. In representative case studies, we demonstrate automated execution and faster root-cause analysis. Collectively, these methods reduce testing costs and improve agent quality through higher coverage, reusability, and earlier defect detection. We provide an open source reference implementation on [GitHub](#).

**Index Terms**—Large language models, Intelligent agents, Software agents, Automatic testing, Glass box.

## I. INTRODUCTION

Agentic AI represents a paradigm in which autonomous LLM-based agents dynamically perceive, plan, and execute complex tasks by selecting appropriate tools, databases, and API. Unlike traditional hard-coded workflows, agents autonomously determine action sequences based on task context. For instance, an agent handling a customer request might query a database, analyze retrieved data using an LLM, and generate a tailored response without predefined instructions. These systems promise to transform productivity across domains ([1], [2]), with growing adoption in customer support and software engineering [3].

**Challenges of LLM-based agents:** LLM-based agents, however, face quality issues. They are complex, distributed applications with diverse components. These systems must cope with (partial) failures of single or multiple components, network failures, data inconsistency, and more (e.g. [4] or [5, Chap. 8]). Additionally, the LLM, as a central component, is affected by systemic quality issues. A well-known issue is that LLMs generate outputs that are nonsensical or unfaithful to the provided source content (*hallucination* [6]) without telling the user. A real-world example involved a chatbot from a Canadian airline that promised discounts to customers, which

were actually not available. The airline was later held liable (cf. [7]). Another quality issue is *jailbreaking*, i.e., bypassing the LLM’s safety measures to provoke undesirable generation [8]. Consider, for example, an agentic system performing financial transactions. In such settings, erroneous actions can result in substantial financial losses. Furthermore, the manipulation of xAI’s Grok 4 in 2025 (e.g., [9]) highlighted the negative impact of jailbreaking. Lastly, [10] showed that *agent performance decreases in longer multi-turn conversations*.

**Optimization potentials of testing LLM-based agents:** since LLM-based agents are designed to support users with little or no supervision, they require extensive testing. Testing agents is currently focused on *acceptance level* tests. In software engineering, acceptance testing determines if the completed software meets the customer’s needs. Put simply, it probes whether the software does what the users want [11]. For LLM-based agents, the agent is viewed as a black box system and evaluated against both functional and non-functional requirements from the end-user’s perspective. While tests at acceptance level are easy to define, code, and understand, they give *limited insight into the internal behavior*, are *time-consuming*, and thus, *expensive to execute and evaluate*, *difficult to automate*, and hence *hard to scale* (similar to software acceptance testing [12]). The black box view of the agent hinders the identification of internal root causes of unexpected behavior or failed acceptance tests, especially for more complex systems, such as conversational or multi-agent systems. Evaluating the agent’s brain, the LLM, can involve a human, semantic comparison techniques such as metrics (e.g., cosine similarity) or LLM-as-a-judge [13]. Since the result of these comparisons is a number ranging from -1 to 1, a threshold needs to be defined to evaluate an answer. Thus, building reliable LLM-as-a-judge systems is challenging ([14], [15]), evoking Juvenal’s quote, “sed quis custodiet ipsos custodes?” [“but who will guard the guards themselves?”]. Additionally, the LLM’s sensitivity to prompt variations [16] impacts the agent’s output. As a result, obtaining a specific agent behavior, e.g., invoking a particular tool, can be a try-and-repeat issue and hampers automatic checking of results. Lastly, testing conversational agents involves covering multi-turn conversations with numerous branches in various languages through comprehensive testing.

**Contribution:** In this paper, we present methods to enable structural testing of LLM-based agents, bringing proven

software engineering practices to this emerging domain. We make three key contributions:

**Enabling software engineering best practices for agents:** we demonstrate how structural testing enables the test automation pyramid, regression testing, test-driven development, and multi-language testing workflows for LLM-based agents.

**Technical methods for structural testing:** we use traces based on OpenTelemetry to capture agent trajectories, mocking to enforce reproducible LLM behavior, and assertions for automated verification. This enables testing of individual agent components and their interactions.

**Validation through case studies:** representative case studies demonstrate automated execution and faster root-cause analysis. These methods can reduce testing costs and improve quality by increasing coverage, enhancing reusability, and facilitating earlier defect detection.

We provide an open-source implementation under [Apache 2 license](#), thereby facilitating unrestricted access and implementation. We hope this will spur adoption across the community. The source code is available via [GitHub](#) and uses the [Amazon Bedrock Converse API](#). Migration to other environments is fairly straightforward: classes for real and mocked LLM interface as well as the OpenTelemetry attributes have to be adapted to the new environment or LLM.

## II. BACKGROUND AND RELATED WORK

**LLM-based agents:** can be deployed as single agents or multi-agent systems, where "multiple autonomous agents collaboratively engage in planning, discussions, and decision-making" [17]. Overviews of historical and current LLM-based agents, their structure and components can be found in [17]–[20]. For the remainder of this paper, we will use the agent structure as shown in Fig. 1.

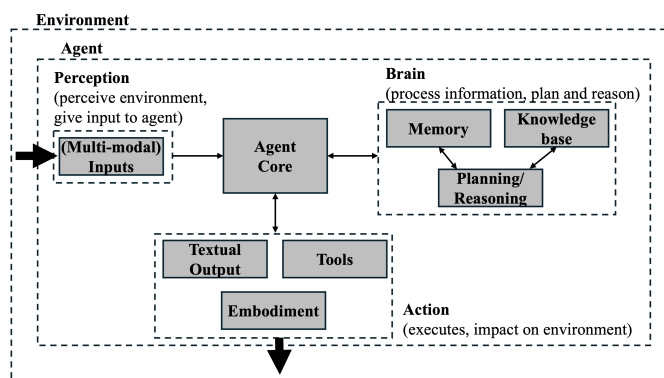


Fig. 1. Structure of an LLM-based agent. Source: based on [18]

Agents operate in a constant loop. The *agent core* orchestrates this loop, coordinating between modules via interfaces or API and managing connections to tools, knowledge bases, (cloud-based) LLM, and other agents. The *perception module* perceives changes in the external environment and then converts multi-modal information (often textual input) into an understandable representation for the agent. This allows agents

to process textual, audio, and visual data. This information is forwarded to the *brain module*. The brain module, which is primarily composed of an LLM, is the core of an agent. Its main functions are reasoning, planning, and processing available information. Reasoning and planning means breaking down a goal into steps or subtasks using a technique called ReAct [21] or some variation thereof. For processing information, the brain can utilize memory (the agent's past observations, thoughts, and actions with a user) and knowledge bases (external storage of typically very large amounts of information). Additionally, the memory is enriched with data generated by the brain for future use. The brain module generates sequences of actions which are forwarded to the *action module*. The action module carries out the execution by providing textual output, using external tools (via functions registered with the agent or external functions via API) and embodiment (the capability to actively perceive, comprehend, and interact with physical environments and generate specific behaviors to modify the environment based on the LLM's extensive internal knowledge). The constant loop allows the agent to continuously get feedback and interact with or impact its surrounding environment [18, Chap. 3].

**Quality issues of LLM:** include hallucinations, security vulnerabilities, sensitivity to prompts, performance degradation in multi-turn conversations, which can occur as a single or compound event. [6] surveys *hallucinations* and defines it as "the generation of texts or responses that exhibit grammatical correctness, fluency, and authenticity, but deviate from the provided source inputs (faithfulness) or do not align with factual accuracy (factualness)". [22] were among the first to publish about this characteristic, but called it stochastic parrot. [23] give a taxonomy and [24] show an overview of mitigation techniques. However, [25] and [26] showed that hallucination is impossible to avoid completely. *Jailbreaking* an LLM involves circumventing measures to prevent undesirable generation and was first shown by [8]. [27] give an overview of possible jailbreaks. [28] and [29] show other security risks for LLM-based applications.

**Quality issues of LLM-based agents:** The LLM's *sensitivity to prompt variations* [16] as well as longer multi-turn conversations [10] can impact the agent's performance. In multi-agent systems, the quality issues of LLM can quickly compound. For example, a common failure mode in agentic systems is planning and reasoning deficiencies whereby agents generate flawed execution plans due to, among other things, misinterpretation of user instructions, inadequate task decomposition, unspecific, ambiguous, and overlapping tool descriptions, or failure to anticipate dependencies between tools ([30], [31]). Another common way in which agentic systems break includes failure to determine task completion, leading to repetitive execution cycles (infinite loops) until forced termination [30]. Finally, operational issues such as failing to call a tool with the correct parameter set or syntax can be a common cause of agent failures in production. In more complex multi-agent systems, another failure mode stems from inter-agent coordination issues, including task derailments or ignoring inputs of other agents. [18, Chap. 6.3] gives a literature survey over potential failures

of agents with emphasis on security and trustworthiness, [32] focuses on safety. While these publications mostly cover single agents, [30] defines a taxonomy for failures of multi-agents.

**Testing LLM-based agents:** given the shown quality issues, agents have to be tested extensively. Research and development on testing agents currently focus on acceptance tests, which are rather an evaluation or validation than a verification ("are we building the right product?" versus "are we building the product right?", as stated by [33]). We discussed the benefits and challenges of accepting LLM-based agents in Section I. [34], [35], and [36] give an overview for evaluating agents, [37] focus on multi-agents and [38] on security.

**Frameworks for testing LLM-based agents:** LLM-based agents are an emergent technology, as are methods and frameworks used for their testing. In [39] we listed frameworks for developing and operating agents such as [MLflow](#), [Opik](#), or [Generative AI toolkit](#). For testing LLM-based agents, based on a non-exhaustive survey at the time of writing, the available tooling and frameworks can be categorized as follows:

- **Public cloud provider tooling:** [Amazon Bedrock Evaluations](#), [Google Cloud GenAI evaluation service](#), and [Microsoft Azure AI Foundry](#) are deeply integrated, tailored, and optimized into the provider's offering. These products allow evaluating agents at the acceptance test level, but do not (yet) support structural testing of agents.
- **Commercial off-the-shelf software:** there are several available offerings such as [DeepEval](#) by Confident AI, [LangFuse](#), [LangSmith](#), [Phoenix Arise](#) and [Weights and Biases](#). These tools track the agent's internal behavior and interactions, although they currently offer no testing on a deeper level than acceptance tests. [Opik](#) offers the concept of unit tests based on PyTest, though its focus is on the LLM pipeline. Additionally, these tools are not (completely) open source and not free of charge (but with a limited free product offering).
- **Free-to-use software:** [Amazon Strands Agents](#), [Microsoft AutoGen](#), [MLflow](#), and [Ragas](#) are open source and free to use. These tools offer traces, but do not (yet) support testing on a level deeper than acceptance tests.

Additionally, even though several of these frameworks offer traces, there are currently only basic conventions for structure, attributes, or naming, but no standardization.

**Software testing:** has been extensively researched with a substantial body of literature for several decades. [40] defined its purpose as "a successful test case ... detects an as-yet undiscovered error", but testing "can only show the presence of errors, not their absence" [41]. Testing can be categorized into *functional* (or black box-testing) and *structural testing* (or glass box testing). "In functional testing, the program or system is treated as a black box. It is subjected to inputs, and its outputs are verified for conformance to specified behavior. The software's user should be concerned only with functionality and features, and the program's implementation details should not matter. Functional testing takes the user's point of view" [42, Chap. 2.2]. "Structural testing does look at the implementation details" as they are "aimed at exploring the consistency of a

component's implementation with its design" [42, Glossary]. A detailed overview of testing techniques and approaches can be found in [42] or [11]. Testing forms a significant part of the software development life cycle, with estimates ranging from 40% [43, Chap. 1], 50% ([40], [44, pp. 126], [42, Chap. 1.1]) or even 75% [45].

**Test automation:** given testing's importance, intensive research has been done to increase its efficiency, i.e., reduce test effort with limited or no impact on test quality (e.g., [46], [47]). A popular approach to increasing test efficiency is the Test Automation Pyramid. Introduced by [48, Chap. 16], most approaches use three layers but with different naming (e.g., [49] and [50]). The lowest layer consists of tests for small software functions (*unit tests*), which, if passed, are followed by testing the interactions of these small functions (*integration tests*) and culminate in testing the entire system (*acceptance tests*). While the concept of unit tests dates back to [51], [48]'s idea was to unify different test levels and provide a guideline for distributing tests, favoring simple, automatable, low-level unit or integration tests. Since only a successful passing of all tests of one layer leads to testing the next layers, this concept helps to provide a good trade-off between test time and depth. Today, this pyramid is typically executed as part of an automated Continuous Integration/ Continuous Deployment (CI/CD, defined by [52]) pipeline.

Several publications show case studies (e.g., [53], [54]) or questionnaires for developer teams (e.g., [55], [56]) to identify benefits of test automation. [57] give a systematic literature review and point out that only a few publications show empirical evidence or exact figures for benefits, which include *test reusability*, *repeatability*, *test coverage*, and *effort saved in test executions*. [58] give a survey of test automation in DevOps teams defining test automation as an essential enabler for DevOps with additional benefits of accelerating releases in higher quality and efficiency. Regarding quantitative results, [59] reported a 40% reduction in automation costs and a 50% reduction in maintenance costs. [60] use return-on-investment calculation to show significant impact when test artifacts are reused several times (up to 307% for test design, 675% for test execution, and 41% for test evaluations if tests are used more than 10 times). [53] show effects as factors for COCOMO (Constructive Cost Model, [33]).

**Test-driven development:** as introduced by [61], is an iterative procedure to produce "clean code that works". It starts with writing a small, automated test for a functionality that fails, then changing the code to pass the test, and then concluding by refactoring the code. Hence, tests are written before developing a feature- in contrast to other traditional testing strategies where tests are usually built after completing the implementation. Some publications see benefits of TDD as to improve code coverage and quality, documentation, regression testing and developer productivity (e.g., [43, Chap. 8.2], [62], [63], [64]), while others see mixed results such as impact on quality but little or no positive [65] or even detrimental effects ([66], [67]) on productivity. [68] point out that these contradicting results are partly due to how case studies were defined, e.g.,



unclear scope, lack of developer experience with TDD, focus on building new software instead of maintaining, as well as not analyzing long-term benefits. [69] show how to use LLM to speed up the TDD workflow, while [70] detail how to improve the quality and correctness of software code generation by an LLM via TDD. [71] and [72] showed how to adapt test-driven development for an LLM in general, while [73] adapted TDD for the specific use case of guard railing in- and outputs. These approaches all evaluate an agent on the acceptance level.

### III. TECHNICAL BUILDING BLOCKS

In this section, we detail the core contribution of this paper. Starting with techniques to enable structural testing, we then describe these tests for agent components (i.e., *unit tests*) and their interactions (i.e., *integration tests*). The techniques are adapted from software engineering. We provide a brief description of each technique and its benefits, followed by a detailed explanation of its application to the agent domain.

#### A. Methods for structural testing

1) *Traces as key enabler*: Tracing enables detailed observability of a system, facilitates root cause analysis and bug fixing, and helps to understand the implemented system. Traces record and store information and events happening during the execution of a software or system. They are used extensively in complex systems, such as embedded or distributed systems [74], and are generated by frameworks like [OpenTelemetry](#) or [Dapper](#) [75] (see [76] for an overview). In the OpenTelemetry tracing model, a unique *trace\_id* is assigned for each incoming request. Every single action to fulfill this request (e.g., calling a function) is recorded in the form of a data structure called *span* consisting of attributes such as *span\_id*, *name*, *start*, and *end* timestamp, as well as detailed information about the action.

For LLM-based systems, several frameworks for developing (cf. [39, Sec. 2]) or testing agents (cf. Sec. II) offer traces, mostly based on OpenTelemetry. These frameworks allow capturing the agent's full trajectory to handle a user input. This allows monitoring deployed agents and observing the impact of the LLM's varying output on the whole agent. Additionally, tracing agents facilitate incident analyses, for instance, in cases of customer complaints or unexpected agent outputs, such as invoking more tools per request than before or replying with "I cannot help you with that" when not expected.

For agents, we also utilize the OpenTelemetry span model, where one unique trace covers one user input and one agent response, i.e., one turn. Each turn has spans for significant operations such as accessing memory, invoking LLM, or using tools. We also use a fixed attribute, *ai.conversation.id*, to group traces, facilitating to find and analyze all relevant traces for a single conversation. Traces are stored in a database or files.

2) *Automating tests*: tracing not only helps to identify the root cause of a failure, but can also be used to test the system or agent itself by comparing the expected behavior of a system with the real behavior as captured by traces. In software engineering, assertions are used to compare expected with real behavior. In the event of discrepancies, the program terminates

with an error. Sample frameworks for this include [Jest](#) and [PyTest](#), which allow for defining human-readable test cases that include detailed information about the error. Assertions enable developers to detect bugs early, as code execution stops upon a failed assertion.

We use them to compare the expected behavior of agent components and their interactions against real behavior as captured by traces. Hence, this allows us to test agents on a deeper level than acceptance tests. A longer conversation between a human and an agent consists of multiple traces (one per turn), including multiple spans of actions the agent took during that turn. Hence, finding the relevant pieces can be a cumbersome task. This can be facilitated using regular expressions, string search functions, or classes that filter for the relevant trace or span data for the assertion. Additionally, building such classes provides the opportunity to write test cases that are easy to understand.

Taken together, this enables running and checking tests via PyTest in an automated workflow. Additionally, these tests can be integrated into a CI/CD pipeline, enabling automated test runs for each change. This also prevents deploying faulty agents, as the pipeline stops in case of a failed assertion. For agent components with deterministic behavior, defining and checking structural tests works the same as in software engineering. However, the LLM's varying output makes testing the LLM and its interactions with other agent components more challenging: testing a specific behavior of an agent, such as calling a tool, can be a time-intensive trial-and-error process.

3) *Mocking to facilitate tests involving an LLM*: In software engineering, mocks are used to facilitate testing of complex or non-deterministic objects, especially in specific situations or environments, such as reproducible testing of connection errors of distributed systems. Mocks are "objects pre-programmed with expectations which form a specification of the calls they are expected to receive" [77] and are based on the proxy pattern [78]. They offer the same external interfaces as the objects they replace, but their pre-definable responses ensure deterministic behavior. This allows for faster tests, e.g., simulating a database instead of setting up a real one. Exemplary mocking frameworks are [Google Test](#) for C++, [JMockit](#) for Java, [Mock](#) for Python, or [Postman](#) for API.

Mocking an LLM is very similar to mocking a component in software engineering. Agent frameworks using a cloud-based LLM invoke the LLM via API (e.g. [Amazon Bedrock Converse API](#)) and receive as a response an action (textual output or tool to call, cf. Fig. 1). Mocking an LLM, then, means building an object with the same interface and possible return values, but without actually calling an LLM. The agent then calls the mock and receives user-definable responses. Hence, mocking allows enforcing specific LLM behavior and thus facilitates testing by providing reproducible test conditions for the LLM itself as well as its interactions with the other agent components. Furthermore, mocking offers fast testing as mocked LLM return instantly. Finally, using a mocked LLM saves costs compared to cloud-based LLM, which are priced on a per-token basis.

### B. Structural testing of agent components

Table I shows examples of issues with agent components we want to cover with tests.

Component	Test rationale	Sample test
Agent core	initialization works? valid configuration? exists? accessible?	Agent w/ valid model id successfully created? write, then read data
Memory	ensure privacy	access to memory of other users possible?
Knowledge base	empty/ faulty queries data updated or augmented	Test empty/ long strings incl. special characters add data, then new data returned on querying
LLM	does fine-tuned LLM work?	invoking fine-tuned LLM w/ sample prompt returns plausible results
Tools	return plausible output(s)?	get_weather(Munich) returns plausible values
Textual input	validate user input	Test injections, long input and incompatible formats

TABLE I  
EXAMPLES FOR POSSIBLE TESTS OF AGENT COMPONENTS

A software unit is "the smallest testable piece of software...[consisting] of several hundred or fewer lines of source code", i.e., a component, module, or a single behavior of software. [42, Chap. 3.7] defines unit testing as "the testing we do to show that the unit does not satisfy its functional specification and/ or that its implemented structure does not match the intended design structure". Unit tests work by entering different parameters and checking the expected behavior of the component itself in isolation [43, Chap. 8.1.1].

This works for all agent components with deterministic behavior like tools, memory, or knowledge bases. The LLM, however, has varying output and offers only limited insight. Therefore, we need traces to gain insight into its actions and to test expected against actual behavior, as captured by traces.

### C. Structural testing of interactions of agent components

Table II illustrates possible issues of interactions between agent components we want to cover with tests.

Component	Test rationale	Sample test
Planning and memory	history persistent after restart?	Conversation continues? Follow-up queries work?
Planning and knowledge	check if both interact correctly?	querying company policy retrieves correct data
Agent core and tools	extracted right tool and parameter?	"Get weather in ..." calls right tool and parameters

TABLE II  
EXAMPLES FOR POSSIBLE TESTS OF AGENT INTERACTIONS

Tests for interactions between components are called integration tests, which are "specifically aimed at exposing the problems that arise from the combination of components" [42, Chap. 3.7]. Their purpose is to "explore how components interact with each other and with data under the assumptions that the components and objects they manipulate have all passed their local tests." [42, Glossary]. Testing interactions of

agent components with deterministic behavior is equivalent to integration testing in software engineering, and traces are not necessary. But traces are especially handy when we want to test the interaction of the LLM with other components or the interactions of multiple, distributed agent components (e.g., a model in the cloud).

Mocking is useful for making integration tests faster or simpler (e.g., using a mock instead of a complex database). It's possible to mock all interacting components, but then the integration test does not really provide insights into the integration. Hence, the extent of mocking should be chosen carefully. However, testing of interactions between LLM and other components is different, due to the LLM's varying output. Here, mocking enforces reproducible behavior of the LLM.

## IV. BEST PRACTICES AND WORKFLOWS

In this section, we show how structural testing can be applied to facilitate regular workflows for testing agents.

### A. Facilitate test workflows for agents

1) *Regression tests*: LLM-based agents should be tested after any change affecting their components (e.g., a changed prompt, updates to the knowledge base, new or changed tooling, an LLM update, etc.) to ensure continued correct functionality. Structural tests allow testing changed components themselves and their interactions with other parts of the system specifically. An example would be testing if a newly added company policy in the agent's knowledge base is returned correctly. Developers can then test the knowledge base itself and then the interaction of the agent's planning module with the knowledge base.

2) *Root cause analyses*: Structural tests can be used to drill down on specific agent components or interactions, facilitating root cause analyses in cases of failed acceptance tests, unexpected behavior, or bugs. An example would be if the agent failed an acceptance test to book a flight and a hotel. Here, structural tests can help to pinpoint the issue, e.g., wrong credentials, flight not available, or overbooked.

3) *Testing different languages*: structural testing -especially integration tests- ease testing the agent's performance in different languages, since we can check via traces if the agent did the right action instead of checking for a semantically correct answer in the correct language, as required at the acceptance level. An example would be testing a user query searching for events in a city. Testers can run the equivalent queries "show me events in Munich", "搜慕尼黑的活" (Chinese) or "Zeige mir Veranstaltungen in München" (German) and just have to check the traces for an invocation of the correct tool and city as parameter. Hence, these tests can be run and evaluated automatically.

4) *Testing multi-turn conversations*: multi-turn conversations are conversations between an agent and a human or other agents involving multiple exchanges. Given the LLM's and thus the agent's varying output, this means covering multiple possible branches with tests. With mocking to "enforce" LLM-behavior and functions to switch between mocked and real agent, developers can steer a conversation to test possible

branches of multi-turn conversations. Traces then allow detailed insight into the agent’s actions. Additionally, if a test’s pass or fail result can be checked by traces, it can be run and evaluated automatically in a CI/CD pipeline.

### B. Test automation pyramid for LLM-based agents

Functional and structural testing "target different kinds of bugs. Functional tests can, in principle, detect all bugs, but would take infinite time to do so. Structural tests are inherently finite but cannot detect all errors, even if completely executed" [42, Chap. 2.2]. Exhaustive functional tests could theoretically detect all possible bugs, but exponentially growing input combinations limit real world feasibility to small subset of inputs. Structural tests are finite, as the code they test has a limited number of statements and branches. However, these tests cannot detect unimplemented or incorrectly implemented features. Hence, effective testing should combine both, low-level structural and user-level functional testing.

The test automation pyramid (cf. Section II) is a well-known approach in software engineering for combining functional and structural tests, with a preference for structural testing. Fig. 2 shows an adaptation to the domain of agents (with the corresponding layers of the original pyramid on the right side).

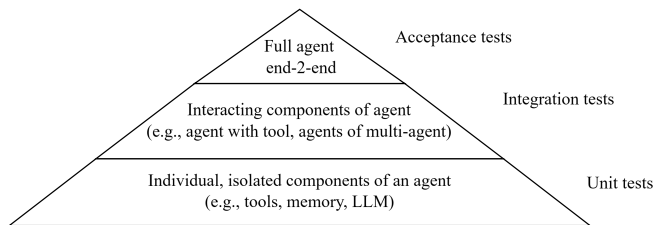


Fig. 2. Test framework for LLM-based agents.

Let’s consider an easy example for the testing pyramid for agents. Suppose a user is interacting with an agent and wants to learn about things to do in the city of Munich in the coming week. The user initiates the following query: "show me events in Munich next week". To answer this query, the agent is expected to call a dedicated tool for searching events, called `search_events()` with parameters `Munich` and a specific `date`. We start the pyramid with testing the *agent’s components in isolation* (*unit tests* in the test automation pyramid). Sample tests check if the tool `search_events()` is callable and the results are as expected. After tests show the agent’s components work in isolation as intended, we test the *interactions of a component with other components* (*integration tests* in the test automation pyramid). We regard single agents of a multi-agent system as components whose interactions are tested with integration tests. An example for a test would be the interactions of the agent with the `search_events(city, date)` tool. As the LLM’s output can vary, we mock the LLM to enforce reproducible behavior. This ensures, for instance, that an integration test can confirm that the agent invoked a specific tool with correct parameters. If these tests pass as well, we test the *full agent end-to-end* from an end-user perspective (*acceptance tests* in the test automation pyramid). End-to-end means we want to

test the whole environment an agent is embedded in (e.g., the agent could be part of a software solution, or controlled by speech). In our example, this could be the initial query sent as a JSON message via HTTPS to a chatbot deployed as a container in the cloud.

Similar to software engineering, the test pyramid for agents can be run as part of a CI/CD pipeline. This allows efficient test runs even with many tests per layer, as only a successful passing of all tests of one layer leads to testing the next layers ("fail-fast" strategy). We run the pyramid for each new agent release, which is triggered by changes such as updated prompts, models, or data. This software engineering best practice prevents the deployment of faulty agent releases into the production environment.

### C. Test-driven development for LLM-based agents

Structural testing is a key enabler for adapting TDD (cf. Sec. II) to the domain of LLM-based agents. An example would be a customer complaint caused by an agent executing an incorrect action or responding with "I’m sorry, I cannot fulfill that request." In TDD’s first step, *write a failing test*, developers write a test case that reproduces the complaint using input from its traces. If the complaint occurred as part of a multi-turn conversation or other specific conditions, mocking the agent helps to facilitate reproducing these circumstances. In TDD’s next step, *make the test pass*, developers can verify that their solution works by running tests against the agent’s traces. In TDD’s last step, *refactoring*, developers improve the code without changing its external behavior against tests. This can involve removing duplicates, adding comments, changing variable names, or splitting up code into separate methods.

## V. CASE STUDIES

We applied methods and workflows to several case studies. Due to limited space, we show only two representative examples. The code shown in this section uses Amazon Bedrock Converse API and the [Generative AI Toolkit](#). We provide full source code of another use case, a simple travel agent, detailing methods, framework, and CI/CD pipeline via this [link](#).

### A. Driver assistance agent

We developed a proof-of-concept for an LLM-based agent assisting drivers with questions about their vehicle or in need of support. With this PoC, we wanted to find out if an LLM-based agent can cover or even speed up some complex, time-intensive interactions between a driving customer and a hotline in multiple languages in high quality, e.g., retrieving and updating customer account data, (pre-) diagnosis of the vehicle on user request, or customer questions about vehicle features. Although this use case focuses on vehicles, it also covers standard topics related to helplines for other technical products.

Figure 3 illustrates the agent’s simplified structure. For this PoC, we use a RAG (Retrieval-augmented generation, [79]) to store vehicle documents, such as manuals and tools, interacting with external databases for customer and vehicle data.

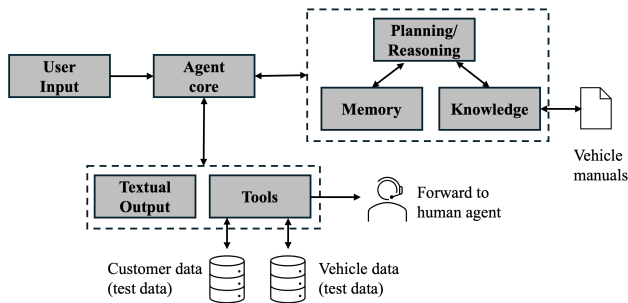


Fig. 3. Simplified architectural overview for driver assistance agent.

Listing 1 shows an often-occurring example of customers wanting to change their data. We define and run the test case, using the *Expect* class to verify in the traces that the correct tool was called. We can test this in different languages by translating the multi-line string below the first comment.

```

def test_change_customer_data(rsa_agent):
    test_case = Case(
        user_inputs=[
            "<Start conversation>\n"
            "<PhoneNr>+555-12345</PhoneNr>",
            # to test other languages,
            # translate multi-line string below
            "Hi, I am John Doe." \
            "My new phone number is +555-98765." \
            "Could you please update my data?"]],)
    traces = test_case.run(rsa_agent)
    Expect(traces).tool_invocations\
        .to_include("get_customer_information")
    Expect(traces).tool_invocations\
        .to_include("update_customer_information")\
        .with_input({
            "ucid": "1",
            "phoneNr": "+555-98765",})

```

Listing 1. Test changing customer data

In listing 2, we want the agent to book an appointment. This time, we use a mocked LLM for the first part of the conversation so that we can steer the conversation towards a desired state for our test. Switching between a mocked LLM and a real LLM (via *add\_real\_response*) allows for scripting a specific situation and then testing the agent's reaction.

```

def test_change_tire_type(mocked_LLM, rsa_agent):
    # agent greets user, asks for permission to scan
    mocked_LLM.add_output(
        text_output=[
            "I am a prototype for\n"
            "a driver Assistance agent.\n"
            "May I diagnose your vehicle?"])
    # get customer and vehicle info, scan vehicle
    mocked_LLM.add_output(
        tool_use_output=[{
            "input": {"vin": "XXX"},
            "name": "get_vehicle_status",
        }, {
            "input": {"phoneNr": "+555-98765"},
            "name": "get_customer_information",
        },])
    # agent's response to results of scan
    mocked_LLM.add_output(
        text_output=[
            "Everything is fine.\n"
            "Can I help you further?"])

```

```

# we invoke real LLM for each text_output above
mocked_LLM.add_real_response()
mocked_LLM.add_real_response()
# run test case with user_input, test case
# will use prepared, mocked responses above
traces = Case(
    user_inputs=[
        "Hello, can you help me?",
        "Yes, go ahead with the diagnosis",
        "I need winter tires." \
        "Would next Monday work?",],)\
        .run(rsa_agent) # run test case
# no need to test the agent's text response,
# since we test if right tools were invoked.
# assert tool get_vehicle_status was invoked
Expect(traces).tool_invocations\
    .to_include("get_vehicle_status")\
    .with_output({
        "found": True,
        "status": {
            "lastUpdate": "2025-08-28",
            # vehicle data cut for brevity
            "....": "....",},})
# assert tool invocations with right parameters
Expect(traces).tool_invocations\
    .to_include("list_available_appointments")
Expect(traces).tool_invocations\
    .to_include("book_appointment")\
    .with_input({
        "appointment_id": "IX94",
        "reason": "install winter tires"})

```

Listing 2. Test conversation to book appointment for winter tires

We also utilize test coverage in the CI/CD pipeline. Test coverage is a class of metrics measuring how much of the code is executed during test runs (cf. [42, Chap. 2.3.4 and 2.3.5], [80]). For the pipeline in Fig. 4, we chose *statement* (each statement executed at least once) and *branch coverage* (each branch executed at least once). These metrics enable our developers to identify which parts of an agent have been thoroughly tested and where to add additional tests.

Name	Stmts	Miss	Branch	BrPart	Cover
lib/agent/Road_tools.py	56	0	10	3	95%
lib/agent/agent.py	57	1	8	2	95%
lib/agent/knowledgebase/_init_.py	23	0	2	1	96%
TOTAL	136	1	20	6	96%

Fig. 4. screenshot of driver assistance agent's test coverage

Running a CI/CD pipeline allows for automated test runs and thus reduces test efforts and costs. The test pyramid's "fail-fast" strategy offers to further reduce these costs, as we only test on higher levels if all tests of a previous layer passed.

## B. Cloud incident root cause analysis agent

The second case study involves an LLM-based agent supporting root cause analyses of service incidents in the cloud. The agent assists engineers with system understanding and real-time insights, thus significantly reducing resolution times [81]. Given an incident, an engineer enters a description of the issue into the agent via a chat interface. The agent's capabilities are modeled on tasks a real-world engineer would do to solve



issues. The agent builds hypotheses for the root cause based on the technical documentation of the cloud account (such as architectural diagrams and Markdown files), system logs and metrics, and its knowledge. The engineer can then instruct the agent to give more details for the defined hypotheses or to build new ones. Additionally, the engineer can ask the agent to create sample code to fix the issue. Fig. 5 shows an architectural diagram of the agent.

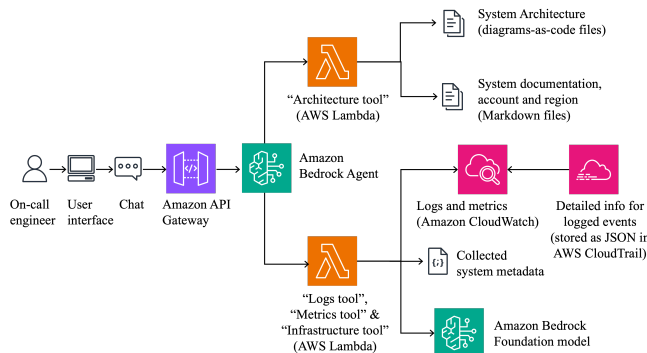


Fig. 5. Architectural overview for root cause analysis agent. Source: [81]

Structural testing helps us facilitate the test workflows. Due to limited space, we provide some sample test cases instead of including the full source code. The first example uses traces and structural tests to verify that the agent is utilizing its tools in the correct sequence. Hence, we can ensure that the agent first runs the architecture tool to understand the architecture and services used, before running other tools, such as log and metric tools, to gather more detailed information. This is important as errors for authorization and authentication (e.g., `accessDenied`), resource-related (e.g., `ResourceNotFoundException`), or throttling are similar for multiple AWS services. Thus, directly analyzing error logs without referencing the actual architecture can lead to invalid hypotheses, additional iterations, increased time for root cause analysis, and lower user acceptance. The second example demonstrates using mocks to simplify the test environment. Instead of setting up test accounts with specific failure patterns, we can save time by mocking the return values of the agent tools. We can then check the traces to see if the return values of mocked tools lead the agent to identify the scripted root cause, e.g., removing or changing a security group ingress rule, which can cause connectivity issues between services (a simple yet often occurring incident in real life). The third example is a fault pattern with failure propagation to other services. We want to test that the agent identifies the system architecture and then walks back the entire failure propagation, as described in the logs, to detect the failure pattern's beginning and its root cause. The last example is an update of documents (e.g., architecture diagrams or docs), indicating a change of the systems to be diagnosed. Thus, we can test if the agent is still functional and to avoid stale test cases.

We can then save time and money by running regression tests for the agent's interactions with the updated systems, instead of repeating full test runs. While these examples take

some time to build, they are useful in the long term, as they facilitate tests for refactoring and future changes to the system, reducing maintenance costs.

### C. General findings

For a thorough quantitative analysis of the benefits of structural testing it is necessary to conduct a large-scale study, including comparison with or without such tests (similar to effects of testing in software engineering, cf. Sec. II).

However, upon applying the methods to several use cases, we observed several qualitative benefits for developers. With traces, our developers have *higher observability* of the agents, as traces give detailed insight into the agent's full trajectory and show more details than the agent's outputs (e.g., how often were tools called? Were tools called in sequence or parallel? How many cycles did the agent run?). We utilize traces in both development and production, enabling us to identify divergences quickly and easily. Additionally, traces offer a *fast root cause analysis* of failed tests (including acceptance tests). Using assertions on traces in a CI/CD pipeline helps to prevent pushing faulty agents into production, as failed assertions stop the pipeline run. This enables *higher quality* from the first deployments. A multi-turn conversation can have dozens of traces, each consisting of multiple spans with lots of attributes. Here, the Expect classes enable easy analysis of traces and spans, facilitating the construction of tests that are easier to understand and therefore more maintainable and reusable. Mocking helps our developers build reproducible tests involving LLM and their interactions. Together, this makes for tests that are fast and easy to develop, as well as quick to run. Hence, they help our developers test frequently during development and aim towards *high test coverage* with minimal impact on development costs. And since tests of agent components can be reused even across different use cases, they also *reduce costs for building and maintaining tests*. Given the pace of innovation in the domain, deployed LLM-based agents are likely to undergo changes. Structural tests enable rapid and straightforward testing of modified components and their impact on the system, thereby reducing test time. Additionally, our developers can run the test automation pyramid regularly to test for a stable system. The pyramid structure represents an efficient tradeoff, emphasizing many fast, cheap unit and integration tests over fewer expensive acceptance tests.

## VI. CONCLUSION AND FUTURE WORK

Testing LLM-based agents presents unique challenges due to their varying behavior, complex multi-turn interactions, and black-box nature. In this paper, we presented methods to enable structural testing of LLM-based agents, addressing these challenges through three key techniques: traces to capture agent execution, mocking to enforce reproducible LLM behavior, and assertions for automated verification.

We demonstrated how these methods facilitate the testing of agents and enable the adaptation of best practices from software engineering to the domain of agents, such as the test automation pyramid. Our case studies demonstrate that



structural testing facilitates automated test execution, faster root-cause analysis, and higher test coverage. Qualitative observations from applying these methods across multiple use cases suggest potential for reduced testing costs through increased test reusability and earlier defect detection.

We acknowledge two limitations. First, our evaluation is qualitative; a large-scale quantitative study comparing development with and without structural testing would provide stronger evidence of benefits. Second, our implementation uses Amazon Bedrock Converse API as a unified interface to multiple LLM. However, a migration to other environments or LLM is confined to adapting the mocked and real interface.

Given the observed benefits, we have integrated these methods into our standard agent development framework and open-sourced the implementation under Apache 2 license at [GitHub](#). We encourage the community to adopt, extend, and evaluate these methods in diverse contexts.

Future work includes extending the methods to additional LLM platforms, conducting quantitative studies on testing effectiveness and cost savings, and developing more comprehensive sample applications that demonstrate the full testing pyramid.

#### ACKNOWLEDGEMENTS

The authors would like to thank (in alphabetical order) Adam Raymer, Dustin Hughes, Fabrizio Avantaggiato, Felix Willnecker, Florian Seidel, Jonas Schroeder, Luisa-Sophie Gloger, Mariano Kamp, Mihai Radulescu Kober, Paul Weber, Raghvender Arni, Raphael Perri, and Rui Costa for their support, insightful inputs, comments, feedback, and reviews. The authors used OpenAI's and Anthropic's language generation models to generate parts of the text, which were subsequently reviewed, edited, and revised.

#### REFERENCES

- [1] L. Yee, M. Chui, R. Roberts, and S. Xu, "Why agents are the next frontier of generative AI," *McKinsey Digital Practice*, 2024. [Online]. Available: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/why-agents-are-the-next-frontier-of-generative-ai>
- [2] Gartner, "Top technology trends 2025," 2024. [Online]. Available: <https://www.gartner.com/en/articles/top-technology-trends-2025>
- [3] H. Jin, L. Huang, H. Cai, J. Yan, B. Li, and H. Chen, "From LLMs to LLM-based agents for software engineering: a survey of current, challenges and future," *arXiv preprint arXiv:2408.02479*, 2024. [Online]. Available: <https://arxiv.org/abs/2408.02479>
- [4] F. Cristian, "Understanding fault-tolerant distributed systems," *Communications of the ACM*, vol. 34, no. 2, pp. 56–78, 1991.
- [5] M. Kleppmann, *Designing data-intensive applications: the big ideas behind reliable, scalable, and maintainable systems*. O'Reilly, 2017.
- [6] Z. Ji *et al.*, "Survey of hallucination in natural language generation," *ACM Computing Surveys*, vol. 55, no. 12, pp. 1–38, 2023.
- [7] M. Yagoda, "Airline held liable for its chatbot giving passenger bad advice - what this means for travellers," <https://www.bbc.com/travel/article/20240222-air-canada-chatbot-misinformation-what-travellers-should-know>. [Accessed: 14.11.2025], BBC, 2024.
- [8] A. Zou, Z. Wang, N. Carlini, M. Nasr, J. Z. Kolter, and M. Fredrikson, "Universal and transferable adversarial attacks on aligned language models," *arXiv preprint arXiv:2307.15043*, 2023. [Online]. Available: <https://arxiv.org/abs/2307.15043>
- [9] B. Dickson, "Jailbreaking Grok-4: how a 'one-two punch' attack bypasses the world's 'smartest' AI," <https://bdtechtalks.com/2025/07/16/grok-4-jailbreak/>. [Accessed: 14.11.2025], TechTalks, 2025.
- [10] P. Laban, H. Hayashi, Y. Zhou, and J. Neville, "LLMs get lost in multi-turn conversation," *arXiv preprint arXiv:2505.06120*, 2025. [Online]. Available: <https://arxiv.org/abs/2505.06120>
- [11] P. Ammann and J. Offutt, *Introduction to software testing*, 2nd ed. Cambridge University Press, 2016.
- [12] J. Fischbach *et al.*, "Automatic creation of acceptance tests by extracting conditionals from requirements: NLP approach and case study," *Journal of Systems and Software*, vol. 197, p. 111549, 2023.
- [13] L. Zheng *et al.*, "Judging LLM-as-a-judge with MT-bench and Chatbot arena," *Advances in Neural Information Processing Systems*, vol. 36, pp. 46 595–46 623, 2023.
- [14] J. Gu *et al.*, "A survey on LLM-as-a-judge," *arXiv preprint arXiv:2411.15594*, 2024. [Online]. Available: <https://arxiv.org/abs/2411.15594>
- [15] Y. Zhao, H. Liu, D. Yu, S. Y. Kung, H. Mi, and D. Yu, "One token to fool LLM-as-a-judge," *arXiv preprint arXiv:2507.08794*, 2025. [Online]. Available: <https://arxiv.org/abs/2507.08794>
- [16] J. Jang, S. Ye, and M. Seo, "Can large language models truly understand prompts? A case study with negated prompts," in *Proceedings of the 1st Transfer Learning for Natural Language Processing Workshop*, 2023, pp. 52–62.
- [17] T. Guo *et al.*, "Large language model based multi-agents: a survey of progress and challenges," *arXiv preprint arXiv:2402.01680*, 2024. [Online]. Available: <https://arxiv.org/abs/2402.01680>
- [18] Z. Xi *et al.*, "The rise and potential of large language model based agents: a survey," *Science China Information Sciences*, vol. 68, no. 2, p. 121101, 2025.
- [19] H. Naveed *et al.*, "A comprehensive overview of large language models," *ACM Transactions on Intelligent Systems and Technology*, vol. 16, no. 5, 2025.
- [20] L. Wang *et al.*, "A survey on large language model based autonomous agents," *Frontiers of Computer Science*, vol. 18, no. 6, 2024.
- [21] S. Yao, J. Zhao, D. Yu, N. Du, I. Shafran, K. R. Narasimhan, and Y. Cao, "React: synergizing reasoning and acting in language models," in *11th International Conference on Learning Representations*, 2023.
- [22] E. M. Bender, T. Gebru, A. McMillan-Major, and S. Shmitchell, "On the dangers of stochastic parrots: can language models be too big?" in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 2021, pp. 610–623.
- [23] H. Ye, T. Liu, A. Zhang, W. Hua, and W. Jia, "Cognitive mirage: a review of hallucinations in large language models," *arXiv preprint arXiv:2309.06794*, 2023. [Online]. Available: <https://arxiv.org/abs/2309.06794>
- [24] S. M. T. I. Tonmoy, S. M. M. Zaman, V. Jain, A. Rani, V. Rawte, A. Chadha, and A. Das, "A comprehensive survey of hallucination mitigation techniques in large language models," *arXiv preprint arXiv:2401.01313*, 2024. [Online]. Available: <https://arxiv.org/abs/2401.01313>
- [25] Z. Xu, S. Jain, and M. Kankanhalli, "Hallucination is inevitable: an innate limitation of large language models," *arXiv preprint arXiv:2401.11817*, 2024. [Online]. Available: <https://arxiv.org/abs/2401.11817>
- [26] S. Banerjee, A. Agarwal, and S. Singla, "LLMs will always hallucinate, and we need to live with this," in *Intelligent Systems Conference*. Springer, 2025, pp. 624–648.
- [27] Z. Xu, Y. Liu, G. Deng, Y. Li, and S. Picek, "A comprehensive study of jailbreak attack versus defense for large language models," *arXiv preprint arXiv:2402.13457*, 2024. [Online]. Available: <https://arxiv.org/abs/2402.13457>
- [28] Open Worldwide Application Security Project (OWASP), "OWASP Top 10 for LLM applications," <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/> [Accessed: 14.11.2025], 2025.
- [29] The MITRE Corporation, "ATT&CK Matrix for enterprise," <https://attack.mitre.org/> [Accessed: 14.11.2025], 2025.
- [30] M. Cemri *et al.*, "Why do multi-agent LLM systems fail?" *arXiv preprint arXiv:2503.13657*, 2025. [Online]. Available: <https://arxiv.org/abs/2503.13657>
- [31] K. Ning *et al.*, "Defining and detecting the defects of the large language model-based autonomous agents," *arXiv preprint arXiv:2412.18371*, 2024. [Online]. Available: <https://arxiv.org/abs/2412.18371>
- [32] Y. Tian, X. Yang, J. Zhang, Y. Dong, and H. Su, "Evil geniuses: delving into the safety of LLM-based agents," *arXiv preprint arXiv:2311.11855*, 2023. [Online]. Available: <https://arxiv.org/abs/2311.11855>
- [33] B. W. Boehm, "Software engineering: R&D trends and defense needs," *Research directions in software technology*, 1979.
- [34] Y. Chang *et al.*, "A survey on evaluation of large language models," *ACM Transactions on Intelligent Systems and Technologies*, vol. 15, no. 3, Mar. 2024. [Online]. Available: <https://doi.org/10.1145/3641289>

- [35] A. Aleti, "Software testing of generative AI systems: challenges and opportunities," in *2023 IEEE/ACM International Conference on Software Engineering: Future of Software Engineering*. IEEE, 2023, pp. 4–14.
- [36] A. Yehudai *et al.*, "Survey on evaluation of LLM-based agents," *arXiv preprint arXiv:2503.16416*, 2025. [Online]. Available: <https://arxiv.org/abs/2503.16416>
- [37] I. Shamim and R. Singhal, "Methodology for quality assurance testing of LLM-based multi-agent systems," in *Proceedings of the 4th International Conference on AI-ML Systems*. ACM, 2025.
- [38] W. Hua, X. Yang, M. Jin, Z. Li, W. Cheng, R. Tang, and Y. Zhang, "TrustAgent: towards safe and trustworthy LLM-based agents," *arXiv preprint arXiv:2402.01586*, 2024. [Online]. Available: <https://arxiv.org/abs/2402.01586>
- [39] J. Kohl *et al.*, "Generative AI Toolkit – a framework for increasing the quality of LLM-based applications over their whole life cycle," *arXiv preprint arXiv:2412.14215*, 2024. [Online]. Available: <https://arxiv.org/abs/2412.14215>
- [40] G. J. Myers, C. Sandler, and T. Badgett, *The art of software testing*. John Wiley & Sons, 1979.
- [41] E. W. Dijkstra, "The humble programmer," *Communications of the ACM*, vol. 15, no. 10, pp. 859–866, 1972.
- [42] B. Beizer, *Software testing techniques*, 2nd ed. Van Nostrand Reinhold, 1990.
- [43] I. Sommerville, *Software engineering*, 10th ed. Pearson Education, 2015.
- [44] A. Endres and H. D. Rombach, *A handbook of software and systems engineering: empirical observations, laws, and theories*. Pearson Education, 2003.
- [45] B. Hailpern and P. Santhanam, "Software debugging, testing, and verification," *IBM Systems Journal*, vol. 41, no. 1, pp. 4–12, 2002.
- [46] M. Fewster and D. Graham, *Software test automation*. Addison-Wesley Reading, 1999.
- [47] D. Graham and M. Fewster, *Experiences of test automation: case studies of software test automation*. Addison-Wesley Professional, 2012.
- [48] M. Cohn, *Succeeding with agile: software development using Scrum*. Pearson Education, 2010.
- [49] A. Mehta, "Opening keynote: move fast & don't break things," in *Google Test Automation Conference*, 2014.
- [50] M. Wacker, "Just say no to more end-to-end tests," <https://testing.googleblog.com/2015/04/just-say-no-to-more-end-to-end-tests.html> [Accessed: 14.11.2025], 2015.
- [51] H. D. Benington, "Production of large computer programs," in *Proceedings of the Symposium on Advanced Programming Methods for Digital Computers*, 1956.
- [52] M. Fowler, "Continuous integration," <https://martinfowler.com/articles/continuousIntegration.html> [Accessed: 14.11.2025], 2006.
- [53] D. Kumar and K. K. Mishra, "The impacts of test automation on software's cost, quality and time to market," *Procedia Computer Science*, vol. 79, pp. 8–15, 2016.
- [54] V. Garousi and F. Elberzhager, "Test automation: not just for test execution," *IEEE Software*, vol. 34, no. 2, pp. 90–96, 2017.
- [55] J. Kasurinen, O. Taipale, and K. Smolander, "Software test automation in practice: empirical observations," *Advances in Software Engineering*, vol. 2010, no. 1, p. 620836, 2010.
- [56] Y. Wang, M. V. Mäntylä, S. Demeyer, K. Wiklund, S. Eldh, and T. Kairi, "Software test automation maturity – a survey of the state of the practice," *arXiv preprint arXiv:2004.09210*, 2020. [Online]. Available: <https://arxiv.org/abs/2004.09210>
- [57] D. M. Rafi, K. R. K. Moses, K. Petersen, and M. V. Mäntylä, "Benefits and limitations of automated software testing: systematic literature review and practitioner survey," in *7th International Workshop on Automation of Software Test (AST)*. IEEE, 2012, pp. 36–42.
- [58] A. R. Patel and S. Tyagi, "The state of test automation in DevOps: a systematic literature review," in *Proceedings of the 2022 14th International Conference on Contemporary Computing*, 2022, pp. 689–695.
- [59] J. Dougherty and K. Haber, "Test automation: reducing time to market," in *International Conference on Software Testing, Analysis & Review*, 2002.
- [60] Y. Amannejad, V. Garousi, R. Irving, and Z. Sahaf, "A search-based approach for cost-effective software test automation decision support and an industrial case study," in *7th International Conference on Software Testing, Verification and Validation Workshops*. IEEE, 2014, pp. 302–311.
- [61] K. Beck, *Test driven development: by example*. Addison-Wesley Professional, 2022.
- [62] J. Buchan, L. Li, and S. G. MacDonell, "Causal factors, benefits and challenges of test-driven development: practitioner perceptions," in *18th Asia-Pacific Software Engineering Conference*. IEEE, 2011, pp. 405–413.
- [63] G. Scanniello, S. Romano, D. Fucci, B. Turhan, and N. Juristo, "Students' and professionals' perceptions of test-driven development: a focus group study," in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 2016, pp. 1422–1427.
- [64] F. Shull, G. Melnik, B. Turhan, L. Layman, M. Diep, and H. Erdogmus, "What do we know about test-driven development?" *IEEE Software*, vol. 27, no. 6, pp. 16–19, 2010.
- [65] Y. Rafique and V. B. Mišić, "The effects of test-driven development on external quality and productivity: A meta-analysis," *IEEE Transactions on Software Engineering*, vol. 39, no. 6, pp. 835–856, 2013.
- [66] G. Canfora, A. Cimitile, F. Garcia, M. Piattini, and C. A. Visaggio, "Evaluating advantages of test driven development: a controlled experiment with professionals," in *Proceedings of the 2006 ACM/IEEE International Symposium on Empirical Software Engineering*, 2006, pp. 364–371.
- [67] T. Dogša and D. Batič, "The effectiveness of test-driven development: an industrial case study," *Software Quality Journal*, vol. 19, no. 4, pp. 643–661, 2011.
- [68] M. Ghafari, T. Gross, D. Fucci, and M. Felderer, "Why research on test-driven development is inconclusive?" in *Proceedings of the 14th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, 2020, pp. 1–10.
- [69] M. Mock, J. Melegati, and B. Russo, "Generative AI for test driven development: preliminary results," in *International Conference on Agile Software Development*. Springer, 2024, pp. 24–32.
- [70] N. S. Mathews and M. Nagappan, "Test-Driven Development and LLM-based code generation," in *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering*. ACM, 2024, p. 1583–1594.
- [71] R. Chaves, "The complete guide for TDD with LLMs," <https://rchavesf.erna.medium.com/the-complete-guide-for-tdd-with-llms-1dfea9041998>. [Accessed: 14.11.2025], 2024.
- [72] S. Krawczyk, "Test driven development (TDD) of LLM / agent applications with PyTest," <https://blog.dagworks.io/p/test-driven-development-tdd-of-llm>. [Accessed: 14.11.2025], 2024.
- [73] H. Patel, A. Rajnish, and R. Pathak, "Automate building guardrails for Amazon Bedrock using test-driven development," <https://aws.amazon.com/blogs/machine-learning/automate-building-guardrails-for-amazon-bedrock-using-test-driven-development/>. [Accessed: 14.11.2025], 2024.
- [74] J. Moc and D. A. Carr, "Understanding distributed systems via execution trace data," in *Proceedings of the 9th International Workshop on Program Comprehension (IWPC 2001)*. IEEE, 2001, pp. 60–67.
- [75] B. H. Sigelman *et al.*, "Dapper, a large-scale distributed systems tracing infrastructure," Google Inc., Tech. Rep., 2010.
- [76] A. Janes, X. Li, and V. Lenarduzzi, "Open tracing tools: overview and critical comparison," *Journal of Systems and Software*, vol. 204, p. 111793, 2023.
- [77] M. Fowler, "Mocks aren't stubs," <https://martinfowler.com/articles/mock-sArentStubs.html>. [Accessed: 14.11.2025], 2007.
- [78] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design Patterns: elements of reusable object-oriented software*. Addison-Wesley Professional, 1994.
- [79] P. Lewis *et al.*, "Retrieval-augmented generation for knowledge-intensive NLP tasks," *Advances in Neural Information Processing Systems*, vol. 33, pp. 9459–9474, 2020.
- [80] ISO - International Organization for Standardization, "ISO/IEC / IEEE 29119 Software Testing," 2021.
- [81] J. Wildgruber *et al.*, "Innovating at speed: BMW's generative AI solution for cloud incident analysis," <https://aws.amazon.com/blogs/machine-learning/innovating-at-speed-bmws-generative-ai-solution-for-cloud-incident-analysis/>. [Accessed: 14.11.2025], 2025.