

# Architecting software monitors for control-flow anomaly detection through large language models and conformance checking

Francesco Vitale<sup>a</sup>, Francesco Flammini<sup>b,c</sup>, Mauro Caporuscio<sup>d</sup>, Nicola Mazzocca<sup>a</sup>

<sup>a</sup>*University of Naples Federico II, Via Claudio, 21, Naples, 80125, Italy*

<sup>b</sup>*University of Applied Sciences and Arts of Southern Switzerland, Via la Santa 1, Lugano, 6962, Switzerland*

<sup>c</sup>*University of Florence, Viale Morgagni, 67, Florence, 50134, Italy*

<sup>d</sup>*Linnaeus University, Universitetsplatsen, 1, Växjö, 35252, Sweden*

## Abstract

**Context:** Ensuring high levels of dependability in modern computer-based systems has become increasingly challenging due to their complexity. Although systems are validated at design time, their behavior can be different at run-time, possibly showing control-flow anomalies due to “unknown unknowns”.

**Objective:** We aim to detect control-flow anomalies through software monitoring, which verifies run-time behavior by logging software execution and detecting deviations from expected control flow.

**Methods:** We propose a methodology to develop software monitors for control-flow anomaly detection through Large Language Models (LLMs) and conformance checking. The methodology builds on existing software development practices to maintain traditional V&V while providing an additional level of robustness and trustworthiness. It leverages LLMs to link design-time models and implementation code, automating source-code instrumentation. The resulting event logs are analyzed via conformance checking, an explainable and effective technique for control-flow anomaly detection.

**Results:** We test the methodology on a case-study scenario from the European Railway Traffic Management System / European Train Control System (ERTMS/ETCS), which is a railway standard for modern interoperable railways. The results obtained from the ERTMS/ETCS case study demonstrate that LLM-based source-code instrumentation can achieve up to 84.775% control-flow coverage of the reference design-time process model, while the subsequent conformance checking-based anomaly detection reaches a peak performance of 96.610% F1-score and 93.515% AUC.

**Conclusion:** Incorporating domain-specific knowledge to guide LLMs in source-code instrumentation significantly allowed obtaining reliable and quality software logs and enabled effective control-flow anomaly detection through conformance checking.

**Keywords:** Conformance checking, software monitoring, fuzzy run-time verification, cyber-physical systems, resilience, railways

## 1. Introduction

The complexity of modern computer-based systems increases their exposure to several types of threats, including software defects, hardware faults, and malicious attacks [25, 27]. The usage of model-based verification and formal methods can significantly help in fault avoidance and detection [44, 4, 6]; however, practical limitations in test coverage and scalability of formal methods, as well as changes and uncertainties in the system and its environments, make verification and validation extremely challenging. These limitations pose risks to computer-based systems’ dependability [36, 34]. We aim to demonstrate that a higher level of dependability can be achieved by software monitoring, which involves logging the software execution and detecting any deviations from the expected behavior [13, 8, 22]. Specifically, we focus on *control-flow anomaly detection*, which deals with the identification of misalignments between the expected flow of activities and their actual sequencing [45].

Software monitoring has been implemented through run-time verification of declarative specifications and run-time model

checking [49, 51, 28, 11]. Run-time verification is closely aligned with formal software specifications and can accurately identify errors that violate those specifications, although its effectiveness depends on the completeness and correctness of the underlying models. This challenge is particularly pronounced in modern software systems, where maintaining strict consistency between system models and their implementations is difficult due to system complexity and multi-developer settings [47, 43]. Moreover, increasingly complex systems introduce incompleteness and uncertainty, including so-called “unknown unknowns”, anomalies that cannot be anticipated due to the lack of prior knowledge of their existence. Such emergent unwanted behavior can have multiple causes, such as system integration of different, possibly commercial-off-the-shelf components or lack of resources to evaluate all the possible fault scenarios of the system [42, 37].

In this paper, we address the limitations of existing run-time verification by conformance checking, an effective and explainable method for control-flow anomaly detection that provides fuzzy control-flow diagnoses that check the adherence of actual executions with prescriptive behavioral models [45]. However,

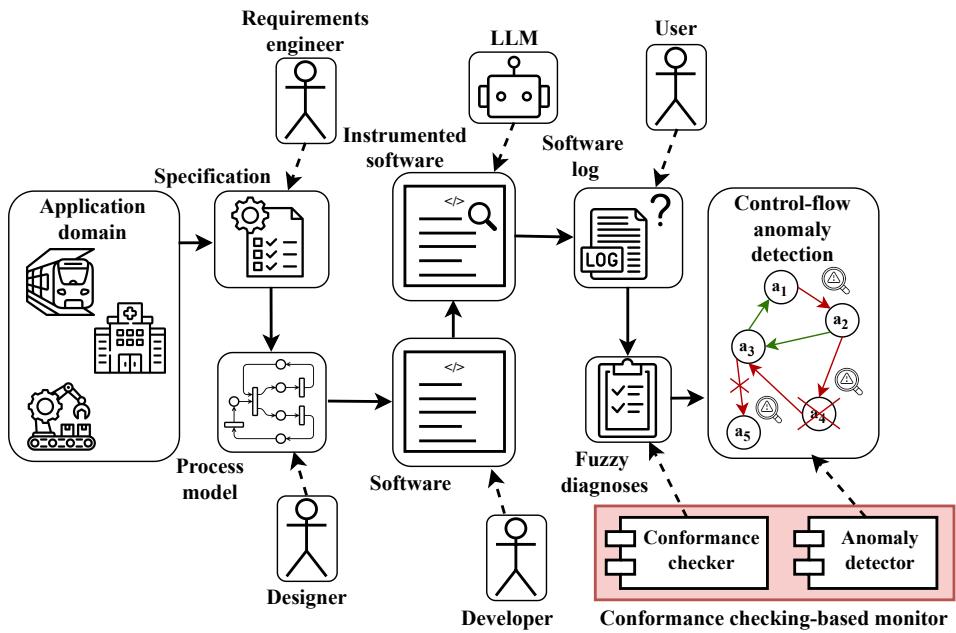


Figure 1: High-level view of the methodology and the conformance checking-based monitor.

obtaining high-quality software logs is difficult as software usually lacks structured source-code instrumentation [9]. This reflects on the quality of the diagnoses provided by conformance checking [32, 52, 31]. We aim to address this issue by integrating Large Language Models (LLMs) into software monitoring. LLMs are advanced neural networks trained on vast amounts of code and textual data, enabling them to understand software structure and control flow [24]. By leveraging these capabilities, LLMs can automatically generate instrumentation code that logs program execution at run-time.

Combining LLMs and conformance checking, we formulate the following two Research Questions (RQs):

- **RQ1 (Source-code instrumentation):** How can LLMs be leveraged to bridge high-level design models and software implementations and generate high-quality logs for subsequent monitoring through conformance checking?
- **RQ2 (Control-flow anomaly detection):** How effective is conformance checking-based control-flow anomaly detection in identifying software anomalies using LLM-enabled software instrumentation?

To address these RQs, we propose a methodology enabling the development of conformance checking-based monitors, whose high-level view is shown in Figure 1. Based on the application domain, a requirements engineer develops a specification. This is used to drive the design of a prescriptive process model and the development of the software. The software is instrumented by an LLM, which bridges the high-level design with the low-level structure and control-flow of the software. The software log is generated when users interact with the system and compared with the process model through a conformance checker.

This results in fuzzy diagnoses that an anomaly detector processes to find any control-flow anomalies.

We test the methodology and the conformance checking-based monitor on a case-study scenario from the European Rail Traffic Management System / European Train Control System (ERTMS/ETCS), a railway standard setting the specification for software development and testing of modern interoperable railways [29]. The ERTMS/ETCS requirements specification document, SUBSET-026, prescribes the behavior of train components in all reference operational scenarios<sup>1</sup>. The results obtained from the ERTMS/ETCS case study demonstrate that LLM-based source-code instrumentation can achieve up to 84.755% control-flow coverage, while the subsequent conformance checking-based anomaly detection reaches a peak performance of 96.610% F1-score and 93.515% AUC.

In summary, the novel contributions of this paper are:

- A fuzzy and explainable conformance checking-based run-time monitor capable of detecting control-flow anomalies from software logs generated by LLM-instrumented code.
- A methodology to guide LLM-enabled source-code instrumentation and development of the fuzzy and explainable conformance checking-based run-time monitor for software monitoring of computer-based systems.
- The application of the methodology and the evaluation of the monitor capabilities referencing the ERTMS/ETCS

<sup>1</sup><https://www.era.europa.eu/era-folder/1-ccs-tsi-appendix-mandatory-specifications-etcs-b4-r1-rmr-gsm-r-b1-mr1-frmcs-b0-ato-b1>

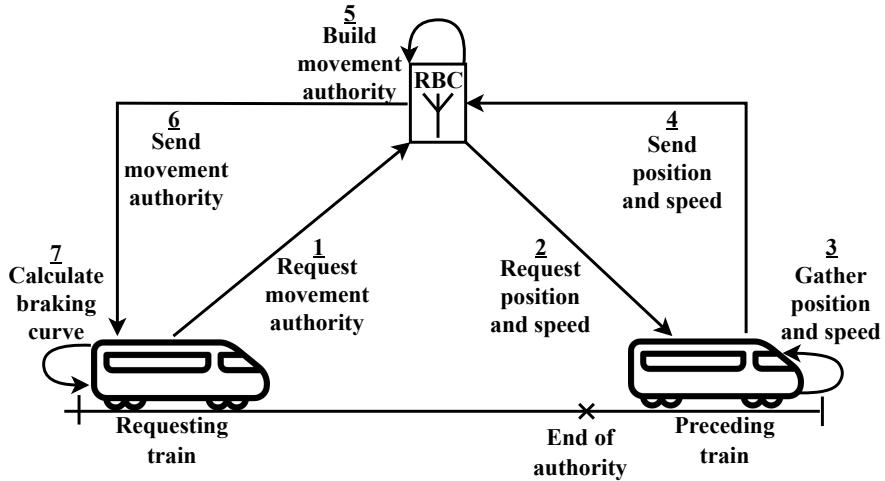


Figure 2: Request of the movement authority and calculation of the braking curve by a train in ERTMS/ETCS systems.

standard, a real-world case study documenting the specification of European railways.

The rest of the paper is organized as follows. Section 2 motivates the research work through a detailed description of ERTMS/ETCS systems. Section 3 describes the conformance checking-based monitor architecture. Section 4 describes the methodology driving the engineering and use of conformance checking-based software monitoring. Section 5 describes the case-study scenario from the ERTMS/ETCS standard, the techniques employed for control-flow anomaly detection, and the experimental factors and metrics. Section 6 presents the results. Section 7 discusses the results as responses to the research questions, and presents the threats to validity. Section 8 presents the related work on software logging and anomaly detection. Section 9 concludes and hints about future research directions.

## 2. Motivation

Modern computer systems will run within increasingly variable and unpredictable environments. A running example are railway systems, which are characterized by many sources of uncertainty, such as environmental conditions, railway traffic, and connection issues between on-board and trackside equipment [19]. In this paper, we target the safety-critical ERTMS/ETCS railway systems, which control the operation of trans-European railway traffic.

An ERTMS/ETCS railway system involves the digital elaboration of data generated by trackside and on-board equipment [3]. Essential on-board components are the Driver Machine Interface (DMI), European Vital Computer (EVC), Balise Transmission Module (BTM), and the Radio Transmission Module (RTM): the DMI enables the driver to engage with ERTMS/ETCS procedures and control the train; the EVC implements the needed logic for safely managing data flow within the on-board subsystem and between on-track and on-board communications; the

BTM reads information through Eurobalises; and the RTM handles all the needed train-to-infrastructure communication logic. On the trackside, the RBC supervises trains in its area and handles several functionalities through the interlocking system to ensure efficient and safe train operation. The type of processing depends on the level of operation, from level 1 to level 3, which defines the degree of automation and the needed trackside and on-board equipment. At level 1, the system uses active Eurobalises to transmit signals to the train, providing discontinuous signalling. Level 2 introduces continuous radio communication between the train and trackside equipment, enabling more efficient operation. Level 3 adds moving block signalling and train integrity check equipment for even higher capacity. Let us consider an example ERTMS/ETCS critical task: the acquisition of the movement authority by a train. The movement authority provides information about the distance from other trains to the EVC of a train. The EVC must calculate the braking curve based on such information and on the static speed profiles to ensure the safety of the passengers and infrastructure. Figure 2 shows the acquisition of the movement authority in ERTMS/ETCS level 2 and level 3, which enables the calculation of the braking curve of the requesting train by letting the RBC collect the train positions wirelessly.

The case-study ERTMS/ETCS scenario that we target in our experiments is the Start of Mission (SoM) procedure. This procedure is rather complex and critical, as its goal regards obtaining a movement authority at the start of a journey. The procedure includes: validating the driver's identity; registering to the closest RBC for train supervision; reporting the train position; obtaining railway traffic information; and obtaining the movement authority.

Although SoM is described in the ERTMS/ETCS system requirements specification, it is mostly specified in natural language and can be subject to interpretation ambiguity among different manufacturers of system components. In fact, extensive field integration testing involving different companies is usually required, which however cannot exclude interaction anomalies

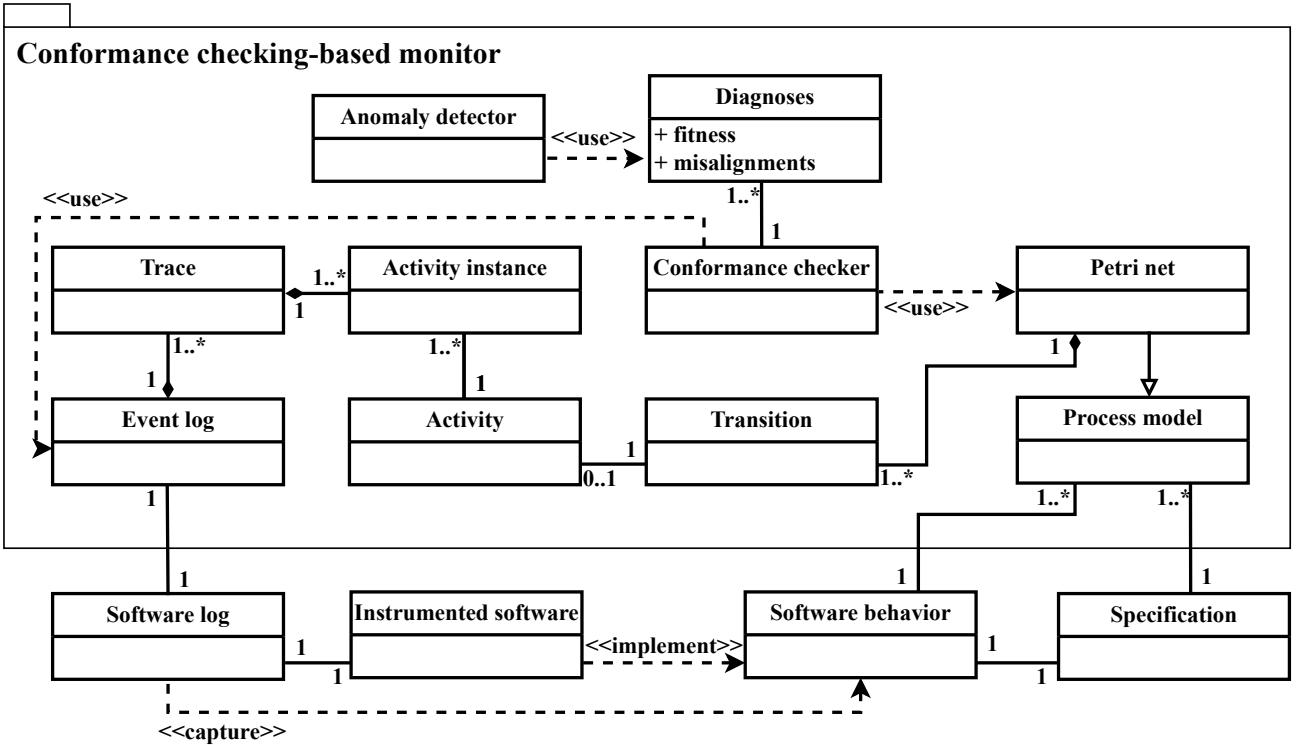


Figure 3: Conceptual UML class diagram of the conformance checking-based monitor and other related methodological artifacts.

in unspecified situations and edge cases. Software monitoring can identify these anomalies by tracing and checking key information regarding software executions such as resource usage [14] and procedure calls [9]. We aim to implement software monitoring through conformance checking to perform control-flow analysis of software behavior and identify any deviations from the expected software execution, i.e., control-flow anomaly detection [30, 35, 45]. In the following, we present the proposed monitor architecture and overall methodology for software control-flow anomaly detection.

### 3. The conformance checking-based monitor architecture

The conformance checking-based monitor connects well-known concepts of the process mining community and software artifacts produced in traditional software development processes. On the one hand, process mining includes the concepts of process models and event logs, the two fundamental inputs to conformance checking. On the other hand, the software artifacts allow generating these inputs, hence their presence is pivotal to the application of conformance checking. Figure 3 shows a conceptual UML class diagram of the overall architecture. In this section, we are interested in describing the monitor architecture. The other concepts will be explored in detail in Section 4.

The main goal of the monitor is to generate diagnoses through the **conformance checker** and use these diagnoses to detect control-flow anomalies through the **anomaly detector**.

#### 3.1. Event log

Conformance checking algorithms use event logs, which are structured data that collect uniquely identified activity instances of a reference process [1]. In this paper, we focus on sequences of activity instances, i.e., traces; thus, we consider the following definition:

**Definition 3.1** (Event log). *Let  $\mathcal{A}$  denote the universe of activities. Let  $\mathcal{A}^*$  denote the universe of traces. An example trace is  $\langle \sigma_1, \sigma_2, \dots, \sigma_n \rangle$ . Let  $\mathcal{B}(\mathcal{A}^*)$  indicate the set of multi-sets of traces. An event log is an element of  $\mathcal{B}(\mathcal{A}^*)$ , i.e.,  $L \in \mathcal{B}(\mathcal{A}^*)$ . An example event log is*

$$L = [\langle \sigma_1, \dots, \sigma_\alpha \rangle^a, \langle \sigma_1, \dots, \sigma_\beta \rangle^b, \langle \sigma_1, \dots, \sigma_\gamma \rangle^c],$$

where  $\sigma_\alpha, \sigma_\beta, \sigma_\gamma$  indicate the last activity instance within the corresponding trace, and  $a, b, c$  indicate the number of times the three traces appear in the event log.

The event log is associated with a software log recorded from the execution of the software instrumented through LLMs. The criticality lies in maintaining a reliable association between the activities of the event log and the process model. This will be explored in more detail in the instrumentation phase of the methodology detailed in Section 4.

#### 3.2. Process model

Event logs are checked against a process model, which is a behavioral model that captures control-flow relationships between activities. The most common formalism employed by

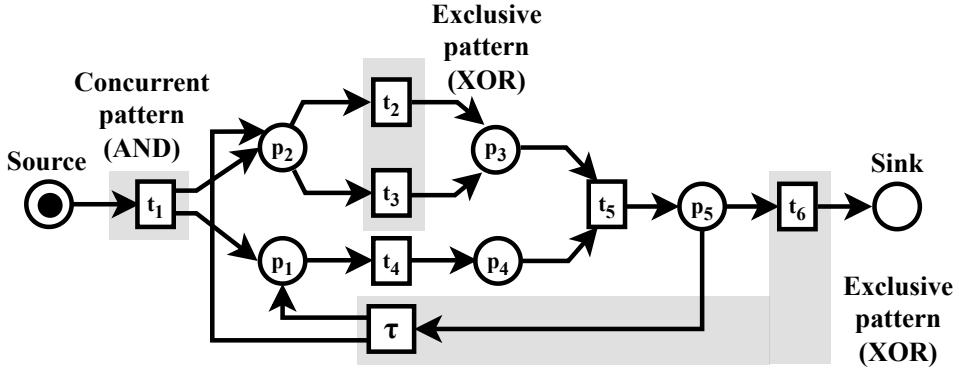


Figure 4: Petri net with grey-highlighted control-flow patterns.

process mining is the Petri net, and, in particular, we focus on the labeled accepting Petri net variant [1].

**Definition 3.2** (Labeled accepting Petri net). *Let  $P$  and  $Tr$  be two sets of nodes of a bipartite graph such that  $P \cap Tr = \emptyset$ , and  $F \subseteq (P \times Tr) \cup (Tr \times P)$  a set of directed arcs. A Petri net is the triple  $(P, Tr, F)$ . Its marking  $M \in \mathcal{B}(P)$  is a multiset of tokens and encodes the current state. Petri nets that have an initial marking  $M_0$  and a final marking  $M_f$ , i.e., an initial and final state, are called accepting Petri nets. Furthermore, let  $A \subseteq \mathcal{A}$  be a set of activities and  $l_{Tr} : Tr \rightarrow A \cup \{\tau\}$  a function that associates to elements of  $Tr$  either an activity of  $A$  or the “silent” label  $\tau$ , which represent unobservable activities that add legitimate behaviors not directly visible. A labeled accepting Petri net is the tuple  $(P, Tr, F, M_0, M_f, A, l_{Tr})$ .  $N$  denotes the universe of all labeled accepting Petri nets, hereafter referred to as Petri nets.*

The formal semantics of Petri nets include the ability to *fire* a transition. Given the number of incoming arcs of a transition, if the current marking is such that there is at least a token in each place connected to the transition, it can fire, i.e., the transition consumes one token from each incoming place and generates one token for each outgoing arc. This firing dynamic enables the Petri net to evolve its state, allowing for the above-mentioned conformance checking and simulation. In addition, it is worth noting that there is a special class of Petri nets, namely workflow Petri nets, which have two specific places: a source place and a sink place. In these Petri nets,  $M_0$  assigns a token to the source place. Any complete firing sequence moves the Petri net state from  $M_0$  to  $M_f$ , which consists of at least a token in the sink place.

Figure 4 depicts an example Petri net made of places source, sink and  $p_1, \dots, p_6$ , and transitions  $t_1 \dots t_6$  and  $\tau$ . The figure highlights in grey the control-flow patterns that the Petri net captures, such as the concurrent pattern (i.e., the AND pattern) linked to  $t_1$ ,  $p_2$  and  $p_3$ . This pattern allows the concurrent execution of transition  $t_4$  and either transition  $t_2$  or  $t_3$ . A desirable property of Petri nets is ensuring that the final marking is always reachable and that no transitions or places become dead. This property, met by the example Petri net, guarantees a complete

and token-free traversal of the net, ensuring every transition has a viable path from start to finish.

The Petri net is obtained through a design-time description of the software behavior according to the application’s specification. As mentioned earlier, the high-level control-flow patterns and names assigned to the Petri net must be linked to the event log entries. Otherwise, the subsequent phase cannot be carried out due to the mismatching level of abstraction between the event log and the Petri net.

### 3.3. Conformance checking and anomaly detection

As the event log and Petri net are well-defined, the conformance checker can now implement a conformance checking technique to verify whether the traces of an event log follow the control-flow patterns prescribed by a reference Petri net. Such verification leads to a series of conformance-checking **diagnoses** that record two types of global and local information: the fitness and misalignments. These can be computed through alignment-based conformance checking, which first evaluates the alignments between traces and event logs.

**Definition 3.3** (Alignment and moves). *Let us denote  $\gg$  as the “skipped” activity. Let  $N \in N$  be a Petri net and  $\sigma \in \mathcal{F}^*$  a trace.  $\sigma_L = \langle a_1, \dots, a_o \rangle \in (\mathcal{A} \cup \{\gg\})^*$  is a (finite) sequence of log moves related to  $\sigma$  if and only if  $\sigma_L \setminus \{\gg\} = \sigma$ . Then,  $\sigma_N = \langle b_1, \dots, b_o \rangle \in (\mathcal{A} \cup \{\tau\} \cup \{\gg\})^*$  is a (finite) sequence of model moves if and only if  $\sigma_N \setminus \{\gg\}$  is a firing sequence of  $N$ , i.e. an allowed control flow. An alignment  $\gamma_{\sigma, N}$  is the two-row matrix*

$$\gamma_{\sigma, N} = \begin{array}{c|c|c|c|c} a_1 & a_2 & \cdots & a_o \\ \hline b_1 & b_2 & \cdots & b_o \end{array},$$

*if for all  $1 \leq i \leq o$ ,  $(a_i, b_i) \neq (\gg, \gg)$ , where  $(a_i, b_i)$  is a move. The upper row is the sequence of log moves (log sequence) and the bottom row is the sequence of model moves (model sequence). We define  $|\gamma_{\sigma, N}|$  the alignment length, i.e., the number of moves of the alignment.*

Alignment-based conformance checking attempts to find the closest (best) alignment between the model and a trace. Figure

	$\sigma_1: \{t_1, t_5, t_4, t_2, t_6\}$	$\sigma_2: \{t_2, t_4, t_5, t_6\}$	$\sigma_3: \{t_3, t_5, t_4, t_6\}$	$\sigma_4: \{t_5, t_3, t_4, t_6\}$
Log sequence	$t_1   t_5   t_4   t_2   \gg   t_6$	$\gg   t_2   t_4   t_5   t_6$	$\gg   t_3   t_5   t_4   \gg   t_6$	$\gg   t_5   t_3   t_4   \gg   t_6$
Model sequence	$t_1   \gg   t_4   t_2   t_5   t_6$	$t_1   t_2   t_4   t_5   t_6$	$t_1   t_3   \gg   t_4   t_5   t_6$	$t_1   \gg   t_3   t_4   t_5   t_6$
	Wrongly-ordered activities ( $t_4 \rightarrow t_5, t_2 \rightarrow t_5$ )	Skipped activity ( $t_1 \rightarrow t_2, t_1 \rightarrow t_4$ )	Skipped activity ( $t_1 \rightarrow t_3, t_1 \rightarrow t_4$ )	Skipped activities ( $t_1 \rightarrow t_3, t_1 \rightarrow t_4$ )
			Wrongly-ordered activity ( $t_4 \rightarrow t_5$ )	Wrongly-ordered activities ( $t_4 \rightarrow t_5, t_3 \rightarrow t_5$ )

Figure 5: The best alignments associated with four faulty traces against the Petri net in Figure 4. The red-highlighted alignment parts indicate mismatches between the trace and the Petri net..

5 shows the four best alignments against the Petri net in Figure 4 linked to four faulty traces  $\sigma_{1,\dots,4}$ . The red-highlighted alignment parts indicate mismatches between the trace and the Petri net due to violating some control-flow constraints. For example,  $\sigma_1$  (leftmost trace) has wrongly-ordered activities, as  $t_5$  precedes  $t_4$  and  $t_2$  instead of being executed after their appearance. This violation leads to the red-highlighted model-log sequence pairs, which can be recorded as additional diagnoses to use in the methodology’s further steps. Once the best alignments are found, the fitness can be computed.

**Definition 3.4** (Fitness). *Let us denote  $\Gamma_{\sigma,N}$  as the set of all alignments between a trace  $\sigma \in \mathcal{A}^*$  and a Petri net  $N \in \mathcal{N}$ . Let  $\delta$  be the unitary cost function for a pair of moves or an alignment. Finally, let  $\gamma_{\sigma,N}^w \in \Gamma_{\sigma,N}$  be the worst-case alignment and  $\gamma_{\sigma,N}^* \in \Gamma_{\sigma,N}$  the best-case alignment, i.e., the alignments with the least and most costs according to  $\delta$ , respectively. The alignment-based fitness for  $\sigma$  is defined as*

$$F_{\sigma,N} = 1 - \frac{\delta(\gamma_{\sigma,N}^*)}{\delta(\gamma_{\sigma,N}^w)}.$$

Let  $L \in \mathcal{B}(\mathcal{A}^*)$  be an event log. The alignment-based fitness for  $L$  is defined as

$$F_{L,N} = \frac{\sum_{\sigma \in L} F_{\sigma,N}}{|L|}.$$

The misalignments are counters associated with each transition  $tr \in Tr$  of the reference Petri net that record the number of mismatches between the log sequences and model sequences involving  $tr$ . For example, Figure 5 outlines that there are 2  $t_5$  mismatches in the best alignment of  $\sigma_1$ . A detailed description of how to calculate misalignments can be found in [45]. The misalignments and fitness constitute the diagnoses.

**Definition 3.5** (Diagnoses). *Let  $\mathcal{A}_\alpha \subseteq \mathcal{A}$  be the number of activities of the target software and  $L \in \mathcal{B}(\mathcal{A}_\alpha^*)$  be an event log of  $k$  traces and  $N \in \mathcal{N}$  a Petri net. The conformance checker collects the diagnoses  $D \in \mathbb{R}^{k \times (\alpha+1)}$  as in Table 1 by alignment-based conformance checking of each trace  $\sigma \in L$  against  $N$ .*

These can be used by an anomaly detector to verify whether a trace is anomalous based on both its number of misalignments and the fitness value. Control-flow anomaly detection is performed by classifying each trace of the diagnoses.

Table 1: Alignment-based conformance checking diagnoses obtained from replaying the traces  $\sigma_1 \dots \sigma_{|L_o|}$  of event log  $L_o$  against a reference Petri net  $N$ .

Trace	$a_1$	$a_2$	...	$a_{\alpha-1}$	$a_\alpha$	$F_\sigma$
$\sigma_1$	$u_{a_1,\sigma_1}$	$u_{a_2,\sigma_1}$	...	$u_{a_{\alpha-1},\sigma_1}$	$u_{a_\alpha,\sigma_1}$	$F_{\sigma_1}$
$\sigma_2$	$u_{a_1,\sigma_2}$	$u_{a_2,\sigma_2}$	...	$u_{a_{\alpha-1},\sigma_2}$	$u_{a_\alpha,\sigma_2}$	$F_{\sigma_2}$
...	...	...	...	...	...	...
$\sigma_k$	$u_{a_1,\sigma_k}$	$u_{a_2,\sigma_k}$	...	$u_{a_{\alpha-1},\sigma_k}$	$u_{a_\alpha,\sigma_k}$	$F_{\sigma_k}$

**Definition 3.6** (Control-flow anomaly). *Let  $D \in \mathbb{R}^{k \times (\alpha+1)}$  be the diagnoses collected by the conformance checker. Let  $d_\sigma \in D$  be the diagnoses associated with a trace  $\sigma$ .  $\sigma$  exhibits an control-flow anomaly if the anomaly detector classifies  $d_\sigma$  as anomalous.*

Given the structure of diagnoses, any unsupervised anomaly detection algorithm can be used [7]. This class of algorithms identifies patterns or deviations without requiring labeled data, making them suitable for scenarios where normal and abnormal behaviors are not explicitly defined. In this context, the algorithm interprets the diagnosis metrics, such as misalignment counts, fitness scores, and other derived features—as indicators of behavioral conformity. By modeling the distribution of these indicators across multiple traces, it can flag outliers that significantly deviate from the expected process behavior, thereby signaling potential anomalies in the system execution. The training of the anomaly detector will be detailed in the following section.

## 4. The methodology for LLM-enabled software control-flow anomaly detection

This section delves into the methodology that we devised to enable the use of the conformance checking-based monitor defined in Section 3. The methodology is depicted in Figure 6 and split into three phases: **software development**, **software monitoring design** and **software anomaly detection**. These are described in the following.

### 4.1. Software development

#### 4.1.1. Requirements engineering and software design

In the **requirements engineering step**, a requirements engineer analyzes the software system requirements and generates a System Requirements Specification (SRS) document re-

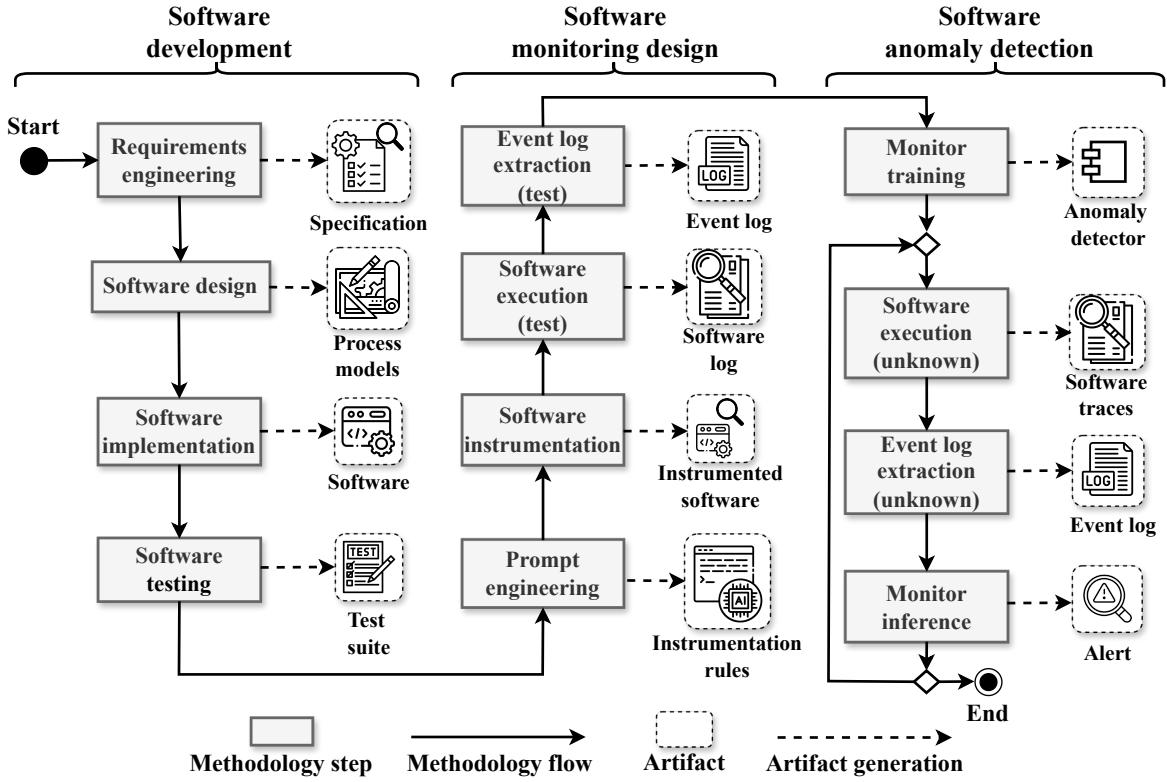


Figure 6: The methodology for LLM-enabled software control-flow anomaly detection. The methodology is split into the software development, software monitoring design, and software anomaly detection phases. LLMs are used in the software monitoring design phase to link process models with the software for run-time control-flow anomaly detection through conformance checking.

porting the software system's functional and non-functional aspects. The functional aspects regard the use cases that the software must implement, whereas non-functional aspects regard performance and dependability metrics. For example, the developers of the ERTMS/ETCS standard produced the ERTMS/ETCS SRS document (SUBSET-026). The dynamic aspects of the standard procedures are described in the document's chapter 5 (SUBSET-026-5), including the SoM scenario.

As will be shown in Section 5, the SRS is mostly written in natural language and can be subject to interpretation ambiguity. This ambiguity can initially be solved with the development of formal models in the subsequent **software design** step. The SRS is used to drive this step and design of the software architecture, which is captured by several diagrams describing static and dynamic aspects. Static aspects involve the description of components' responsibilities and their interconnection. Dynamic aspects involve the procedures that components execute and how the procedures relate to each other. In this paper, we are exclusively concerned with dynamic diagrams, as they capture the control-flow relationships that the conformance checking-based monitor uses to evaluate the presence of control-flow anomalies. Although semi-formal languages can be used, such as UML activity diagrams, they lack the structure and semantics needed to perform run-time verification through conformance checking. Hence, our target formalism is the Petri net, which has seen widespread use in the process mining com-

munity.

Notably, some transformation rules can also be applied to map semi-formal models to formal models. Figure 7 shows a trace-equivalent UML activity diagram of the Petri net in Figure 4. The XOR and AND patterns are explicitly encoded by graphic elements of the UML notation. The UML activity diagram is trace-equivalent since any trace of the Petri net is also allowed on the UML diagram. For example, the trace  $\langle t_1, t_2, t_4, t_5, t_3, t_4, t_5, t_6 \rangle$  can be executed on the UML activity diagram as follows:  $t_1$  initiates two concurrent flows, with the upper path implementing an XOR choice that allows  $t_2$  to execute, followed by  $t_4$ , and then  $t_5$  after synchronization at the AND join. After this, the XOR split cycles back to the concurrent flow, where  $t_3$  and  $t_4$  execute, synchronize, and allow  $t_5$  again, before the process concludes with  $t_6$ . This illustrates how the UML diagram faithfully represents both concurrency and exclusive choices encoded in the Petri net.

#### 4.1.2. Software implementation and testing

Once the software has been thoroughly documented and its behavior, structure, and interactions have been described through process models, the next step is **software implementation**. At this stage, developers translate conceptual representations into executable code. However, maintaining strict consistency between the software implementation and the design-time models presents a significant challenge [47, 26]. As the soft-

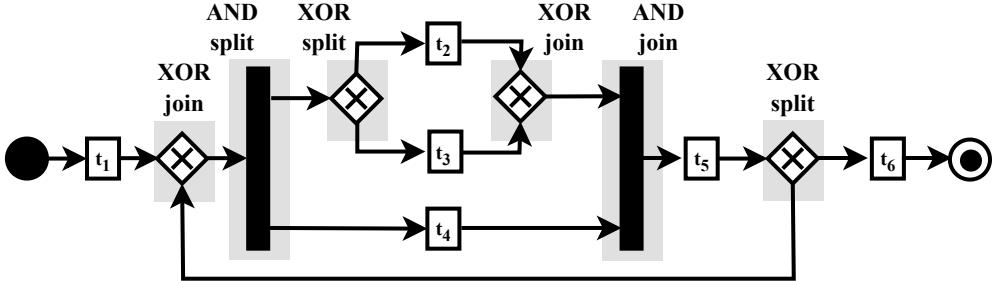


Figure 7: The trace-equivalent UML activity diagram of the Petri net in Figure 4.

ware evolves, deviations between the implemented system and its original models tend to emerge. Ensuring that both remain aligned requires disciplined configuration management, continuous verification, and systematic model updates. Even within model-driven engineering environments, where code generation and model synchronization are supported by automation, achieving complete consistency is more an aspiration than a guarantee. The complexity of real-world systems, combined with human intervention and evolving requirements, makes this alignment an ongoing and essential part of the software engineering process.

Additionally, the events logged by the software may not be related to the behavior captured by the process models, or their mapping to high-level events may not be straightforward. Although this issue can be addressed through log abstraction, which transforms low-level data into high-level information, there is no one-size-fits-all solution [16]. Hence, we deem quality software instrumentation the preferred way to accurately link low-level behavior with the prescriptive design-time models.

The verification and validation (V&V) processes employ both white-box and black-box testing to ensure that the developed software conforms to its specifications and fulfills intended requirements. These processes are particularly critical for safety-critical software, where certification depends not only on demonstrating thorough and systematic testing but also on compliance with development processes, safety analyses, and traceability requirements defined by relevant standards such as EN 50128, IEC 61508, or ISO 26262. Comprehensive V&V provides the evidence needed to support safety claims and regulatory approval.

However, no matter how thorough the V&V process is, run-time conditions may give rise to so-called “unknown unknowns”, which are situations that were not anticipated during design or testing. Detecting such conditions is important for maintaining system safety and reliability. One effective approach is to employ a run-time monitor that tracks software behavior as it unfolds, enabling the system to respond to unexpected or unpredictable conditions [13]. While run-time monitoring is not the only possible mitigation, it provides a practical and proactive mechanism to identify and manage behaviors that elude traditional V&V.

Nonetheless, the test suite developed during **software test-**

**ing** can be used to stimulate the system and collect software logs while the system operates under correct conditions.

#### 4.2. Software monitoring design

##### 4.2.1. Prompt engineering and software instrumentation

In our methodology, we aim to characterize software behavior by software instrumentation. Among the different types of instrumentation techniques, source-code instrumentation is particularly promising, as it enables collecting semantically meaningful events tied to the software’s structural representation. For example, Cinque et al. [9] present a “rule-based” approach to logging instrumentation of source code (i.e., using design-time artifacts to place logging statements).

However, since software implementations often deviate significantly from high-level descriptions, bridging low-level software constructs with design-time models remains challenging. To address this, we propose using LLMs to assist in source-code instrumentation, leveraging their ability to 1) encode domain knowledge and 2) infer semantic structure from code.

While LLMs are powerful tools, it is widely acknowledged that their output is strongly dependent on the prompts used. This gave rise to **prompt engineering**, an activity concerned with designing prompt structures that effectively guide the model toward producing accurate, relevant, and contextually appropriate responses. The following is the logging prompt that we will use to instrument the code.

#### Software instrumentation prompt

**Role:** You are a software developer responsible for instrumenting an existing software system.

**Context:** You are instrumenting the software of a complex, standards-based procedure involving multiple control flows and decision points. The system’s behavior follows a reference process model that defines the interactions, activities, and transitions between components.

**Action:** Instrument the source code according to the following guidelines:

1. Modify the system’s initialization method so that it accepts an external logging handle.
2. Preserve the original program logic and functional behavior.
3. Insert instrumentation points that correspond to

the activities and control flows described in the reference process model.

4. Ensure that all logged data is recorded persistently in a structured text file.

**Output:** The instrumented version of the software system.

The prompt assigns a role to the LLM, provides the context, specifies point-to-point actions, and establishes the output type. Thus, in the **software instrumentation** step, the LLM is provided with the logging prompt, the reference process model, and the software. By acknowledging the dynamics described in the process model and mapping them to the software constructs, the LLM is capable of bridging the high-level model with the low-level implementation, providing an instrumented software that generates quality software logs.

#### 4.2.2. Software execution and event log extraction (test)

The test suite generated during software development can be used to stimulate the **software execution** and extract a software log. In fact, while the tests have already ensured the correctness of the software, they did not capture its behavior. Specifically, we consider black-box tests, which force different inputs to the software and verify an expected output. With the instrumented code, black-box tests also yield the events triggered throughout the software execution.

The software log contains the different events logged according to the instrumentation rules. However, while the LLM has used high-level descriptions of design-time models, the software log may still have spurious information that is not relevant to the high-level reference process model. On account of this, we filter the spurious information and only retain the sequence of activities mapped to the process model transitions.

#### 4.3. Software anomaly detection

##### 4.3.1. Monitor training

The event log extracted during software monitoring design is used in the **monitor training** step to train the anomaly detector to classify control-flow anomalies.

**Definition 4.1** (Monitor training). *Let  $\Delta$  denote the universe of binary classifiers. Let  $L \in \mathcal{B}(\mathcal{H}_a^*)$  be an event log of  $k$  traces obtained from executing  $k$  tests against the instrumented software. Let  $N \in N$  be a Petri net described during the software development phase. Let  $D \in \mathbb{R}^{k \times (a+1)}$  be the diagnoses obtained by the conformance checker by aligning the traces of  $L$  against  $N$ . Monitor training is the function  $\eta : \mathbb{R}^{k \times o} \rightarrow \Delta$ , such that  $\eta(D) = \delta$ , where  $\delta$  is the anomaly detector.*

Through the anomaly detector, the conformance checking-based monitor is capable of classifying a new piece of data as either anomalous or normal. Many unsupervised machine learning algorithms can implement  $\eta$  and build a monitor. Two common approaches are clustering and dimensionality reduction [53]. Clustering involves grouping similar data points using a distance metric, such as the Euclidean distance. A threshold on the distance from the closest cluster can be set so that any

new piece of data exceeding such distance is deemed anomalous. Dimensionality reduction involves building a new lower-dimensional reference system on which data are projected. Reconstructing data from the lower-dimensional reference system to the original one leads to reconstruction error. A threshold on the reconstruction error can be set so that any new piece of data exceeding such error is deemed anomalous.

#### 4.3.2. Software execution, event log extraction, and monitor inference

When unknown software executions occur as the users interact with the software, new traces are collected using the event log extraction prompt above. To verify whether the software executed as intended, **monitor inference** handles the traces through conformance checking and evaluates whether it exhibits a control-flow anomaly according to Definition 3.6.

### 5. Case study

In this section, we demonstrate the application of the proposed methodology in Figure 6 to the SoM procedure of the ERTMS/ETCS standard.

#### 5.1. Software development

The ERTMS/ETCS SRS is mostly written in natural language and can be subject to interpretation ambiguity between different manufacturers of system components. In fact, extensive field integration testing involving different companies is usually required, which, however, cannot exclude interaction anomalies in unspecified situations and edge cases, and that can introduce additional uncertainties, which can be possibly managed using the approach described in this paper.

The following are a few excerpts from SUBSET-025-5:

#### Excerpts from SUBSET-026-5, §5.4.2

##### Status of data stored in the ERTMS/ETCS on-board equipment

**§5.4.2.1:** At the beginning of the Start of Mission procedure, the data required may be in one of three states:

- a) **Valid** — the stored value is known to be correct.
- b) **Invalid** — the stored value may be wrong.
- c) **Unknown** — no stored value is available.

**§5.4.2.2:** This refers to the following data: Driver ID, ERTMS/ETCS level, RBC contact information, Train Data, Train Running Number, Train Position (see §3.6.1.3).

**§5.4.2.3:** Note 1: The status of data in relation to the previous and the actual mode is described in chapter 4, section “What happens to stored information when entering a mode”.

**§5.4.2.4:** Note 2: The change of status of data in course of the procedure is shown in the table in §5.4.3.3.

Although these informal descriptions of the requirements are quite structured and are attached with detailed tables and,

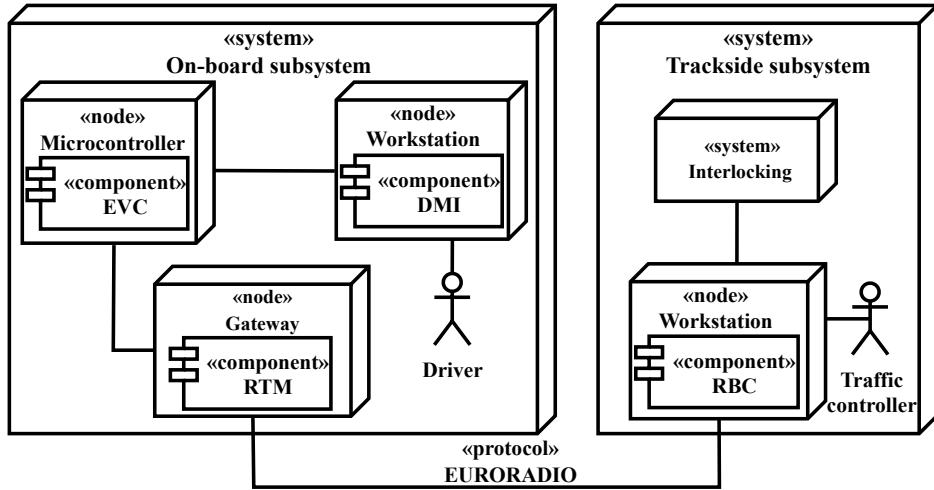


Figure 8: Deployment diagram of ERTMS/ETCS railway systems, split into the on-board subsystem and trackside subsystem.

at times, state diagrams, they still need to be translated into artifacts that document the progressive refinement of natural language into more rigorous and possibly formal models.

We have designed two UML diagrams representing simplified views of the essential static and dynamic aspects of ERTMS/ETCS railway systems. Figure 8 illustrates the core components of the on-board and trackside subsystems. This diagram captures the deployment of ERTMS/ETCS components—EVC, DMI, RTM, RBC, and interlocking—as specified in SUBSET-026-2, and depicts the interconnection of the on-board and trackside subsystems through the EURORADIO protocol.

Building on this structure and interpreting the requirements of SUBSET-026-5, §5.4, we have developed a UML activity diagram representing the high-level Start of Mission (SoM) control flow, shown in Figure 9. The activity diagram abstracts implementation details such as specific message exchanges, data structures, and state-machine transitions, focusing instead on the logical sequencing of activities and decision points.

To provide clarity, the UML activities have been organized into four categories, corresponding to the essential phases of SoM: 1) initial data entry and validation; 2) RBC connection and position report; 3) driver intervention and train data; and 4) final mode assignment. Each activity is labeled using a repeatable and interpretable naming scheme: som\_<action\_name>\_<component>, where <component> corresponds to one of the components depicted in Figure 8, and <action\_name> describes the specific action performed. This systematic labeling ensures repeatability and facilitates understanding across the SoM workflow.

As explained in the previous sections, transformation rules can be applied to obtain a trace-equivalent Petri net from the UML activity diagram. This is noteworthy since conformance checking algorithms are typically suited for the Petri net formalism.

The specification and the diagrams have guided the implementation of an SoM prototype in Python, which adds more

```

def _phase_1_get_initial_data(self):
    if not (self.current_mode == Mode.STAND_BY
            and self.desk_open):
        return None

    state = self._procedure_s1_driver_id_entry()
    if state == 'D2':
        state = self.
            ↪ _procedure_d2_check_pos_level()

    if state == 'S2':
        state = self._procedure_s2_level_entry()

    if state == 'D3':
        state = self.
            ↪ _procedure_d3_check_level_valid()
        if state == 'D7':
            return 'S3'

    return state

def _procedure_s1_driver_id_entry(self):
    if self.driver_id_status == DataStatus.
        ↪ UNKNOWN:
        self.driver_id = self.
            ↪ _simulate_driver_action("Please enter
            ↪ Driver ID:")
    elif self.driver_id_status == DataStatus.
        ↪ INVALID:
        self.driver_id = self.
            ↪ _simulate_driver_action("Please
            ↪ revalidate/re-enter Driver ID:")
    self.driver_id_status = DataStatus.VALID
    return 'D2'

```

Listing 1: Code snippet of the prototype software implementing phase 1 of the SoM procedure.

details than the essential behavior of the high-level diagrams shown earlier. Listing 1 shows a code snippet of the prototype

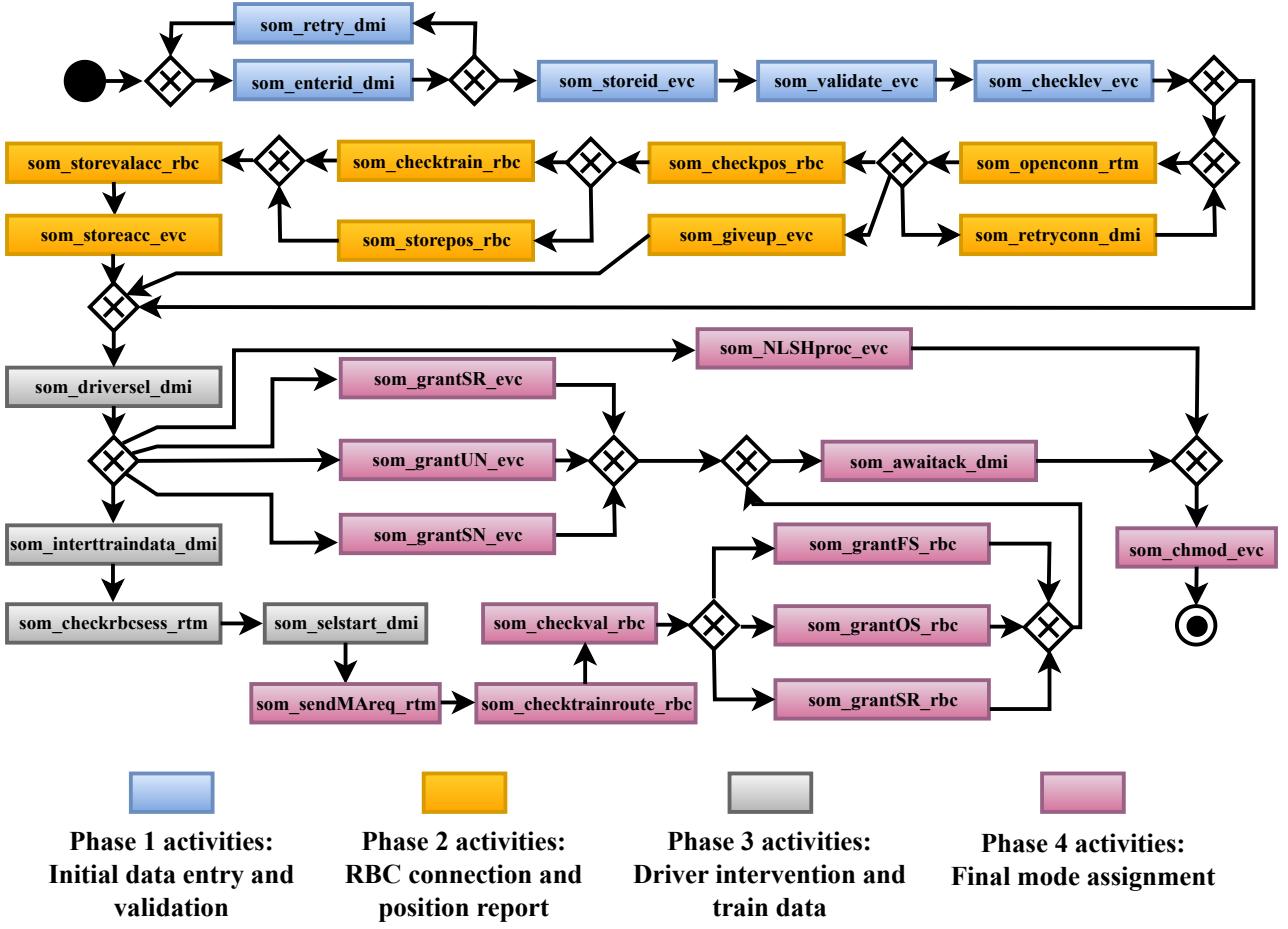


Figure 9: High-level UML activity diagram describing the SoM procedure, split into four phases: initial data entry and validation; RBC connection and position report; driver intervention and train data; and final mode assignment.

```

def test_path_12_success_grant_fs(setup_test_logger):
    script = [
        "DRIVER_007", '2', True, "session_open",
        "validate_position",
        'TD', "DATA", "TRN", "ack", "Start", "ma_fs"
    ]
    sim = ERTMSOnBoardSystem(logger=
        setup_test_logger, controller=MockController
        (script))
    sim.run_start_of_mission()
    assert sim.current_mode == Mode.
        FULL_SUPERVISION
    
```

Listing 2: Code snippet of the test to obtain full supervision.

software implementing phase 1 of the SoM procedure, including the subroutine that handles the acquisition of the driver ID from the DMI.

Next, we developed a comprehensive test suite that instantiated 50 control-flow paths by stimulating the prototype with

different inputs. The test suite must cover a wide range of possibilities, as the SoM procedure may instantiate many different control flows. Listing 2 shows one of the tests in the test suite aimed at forcing the software to provide full supervision to the train.

### 5.2. Software monitoring design

Having developed both the software and its test suite, the instrumentation can now be performed through an LLM. Specifically, we have used the software instrumentation prompt seen in Section 4 and provided LLMs with both the prototype software and the process model in XML format. With both domain-specific knowledge and full access to the code internals, LLMs are able to interpret code structure and place logging instructions where they identify the best fit. For example, Listing 3 shows the instrumentation of one of the phase 1 procedures shown in Listing 1 by Gemini Pro 2.5, one of the LLMs we used in our experiments. The LLM has successfully identified the correct code locations where the `som_enterid_dmi`, `som_retry_dmi`, `som_storeid_evc`, and `som_validate_evc` activities had to be logged.

```

def _procedure_s1_driver_id_entry(self):
    if self.driver_id_status == DataStatus.UNKNOWN:
        self.logger.info("som_enterid_dmi")
        self.driver_id = self.
        ↪ _simulate_driver_action("Please enter
        ↪ Driver ID:")
    elif self.driver_id_status == DataStatus.
    ↪ INVALID:
        self.logger.info("som_retry_dmi")
        self.driver_id = self.
        ↪ _simulate_driver_action("Please
        ↪ revalidate/re-enter Driver ID:")

    self.logger.info("som_storeid_evc")
    self.driver_id_status = DataStatus.VALID

    self.logger.info("som_validate_evc")
    return 'D2'

```

Listing 3: Code snippet of the `_procedure_s1_driver_id_entry` function instrumented by Gemini Pro 2.5.

### 5.3. Software anomaly detection

The event log resulting from the software execution with the test suite can now be used for monitor training. This is necessary because although LLMs allow obtaining quality event logs, they may introduce some noise, such as missing or duplicated activities. While these discrepancies may indicate anomalies, they can be treated as source-code instrumentation noise. Thus, by allowing some degree of noise, the monitor can become more effective at finding true positives while reducing the amount of false positives thanks to this tolerance.

Since the only available traces are those obtained through the test suite, the event log only contains normal traces. After performing conformance checking against the reference Petri net, unsupervised, one-class algorithms can be used to learn how to characterize normal behavior from the diagnoses of Definition 3.5. In the next section, we will show the application of several unsupervised, one-class machine learning techniques to the diagnoses generated through our methodology.

## 6. Evaluation

The evaluation aims to substantiate the answers to the research questions with metrics that quantify source-code instrumentation quality (RQ1) and control-flow anomaly detection effectiveness (RQ2). The software for the experiments is implemented using Python and was run on a Windows 11 machine with an Intel® Core™ i9-11900K CPU @ 3.50GHz and 32GB of RAM. The software uses machine learning and process mining libraries, such as `scikit-learn` and `pm4py`. In addition, it uses the APIs of several LLMs to query the models with the prompts shown in Section 4. The software is available online on GitHub<sup>2</sup>.

<sup>2</sup>[https://github.com/francescovitale/pm\\_software\\_monitor](https://github.com/francescovitale/pm_software_monitor)

### 6.1. RQ1: Source-code instrumentation

We considered several state-of-the-art LLMs that have shown considerable performance in code-related tasks. In particular, we have chosen Gemini 2.5 Pro (gemini-2.5-pro) and Gemini 2.5 Flash (gemini-2.5-flash) [21], and Claude Sonnet 4.5 (clause-sonnet-4.5) [2]. Each of these models represents a distinct approach to large-scale code modeling. The Gemini family, developed by Google DeepMind, integrates multimodal reasoning capabilities and has been optimized for efficiency and responsiveness in code-intensive workflows. Finally, the Claude Sonnet series, developed by Anthropic, is known for its strong contextual reasoning and safety-aligned design, which enhances its ability to perform complex refactoring and documentation-related tasks.

The aforementioned three LLMs are used for source-code instrumentation, whose quality is evaluated using the following metrics. By comparing the event log obtained from the software execution using the test suite with the reference Petri net, we obtain the fitness. The higher the fitness, the higher the adherence of the control flow to the design-time description. Regarding event log-specific metrics, we consider the average trace length and the number of trace variants. Finally, we consider a key metric: the coverage. Let  $L$  and  $N$  be the event log resulting from the execution of the test suite and  $N$  the reference Petri net, we define the control-flow coverage as follows:

$$\text{Coverage} = 1 - \frac{\#\text{misalignments}}{\sum_{\sigma \in L} |\gamma_{\sigma,N}^*|}.$$

The coverage indicates how aligned the source-code instrumentation is to the Petri net.

Table 2 reports the results obtained for each LLM. The two best-performing LLMs with respect to the coverage metric are gemini-2.5-pro and claude-sonnet-4.5, which achieve 84.775% and 78.101% coverage while maintaining high fitness values (0.881 and 0.822). This indicates that the models provided a high-quality instrumentation that aligns with the model (see Definition 3.4) and covers most of its control-flow paths. The remaining LLM, gemini-2.5-flash, could not achieve the same performance, dropping fitness and coverage down to 65.248% and 60.387%.

Figure 10 shows the fitness values distributions (top) of the traces of the event logs linked to the LLMs. The best fitness distribution is achieved by gemini-2.5.pro, for which 37.5% of traces achieve a fitness of up to  $\approx 1$ . This can also be visualized in the bar plots below, which show the top-5 misaligned activities by counting their misalignments (see Definition 3.3). The number of misalignments for each activity increases as the fitness distribution gets lower, highlighting the correlation between the global indicator and the local diagnoses. It is worth noting that the best-performing LLMs, claude-sonnet-4.5 and gemini-2.5-pro, have the same first three most misaligned activities, which also suggests that there may be some systematic errors in the implementation of the source code.

### 6.2. RQ2: Control-flow anomaly detection

To evaluate the capability of the LLM-enabled conformance checking-based monitor, we have built some datasets that in-

Table 2: The fitness, number of variants, average trace length and coverage related to the source-code instrumentation performed by each LLM. The bold values indicate the best-performing LLM according to the control-flow coverage percentage.

Model	Fitness	Coverage	Trace Length	Variants
<b>gemini-2.5-pro</b>	<b><math>88.06\% \pm 11.311\%</math></b>	<b><math>84.775\% \pm 14.127\%</math></b>	$13 \pm 4$	23
claude-sonnet-4.5	$82.213\% \pm 12.813\%$	$78.101\% \pm 15.309\%$	$13 \pm 4$	24
gemini-2.5-flash	$65.248\% \pm 10.255\%$	$60.387\% \pm 11.852\%$	$15 \pm 5$	23

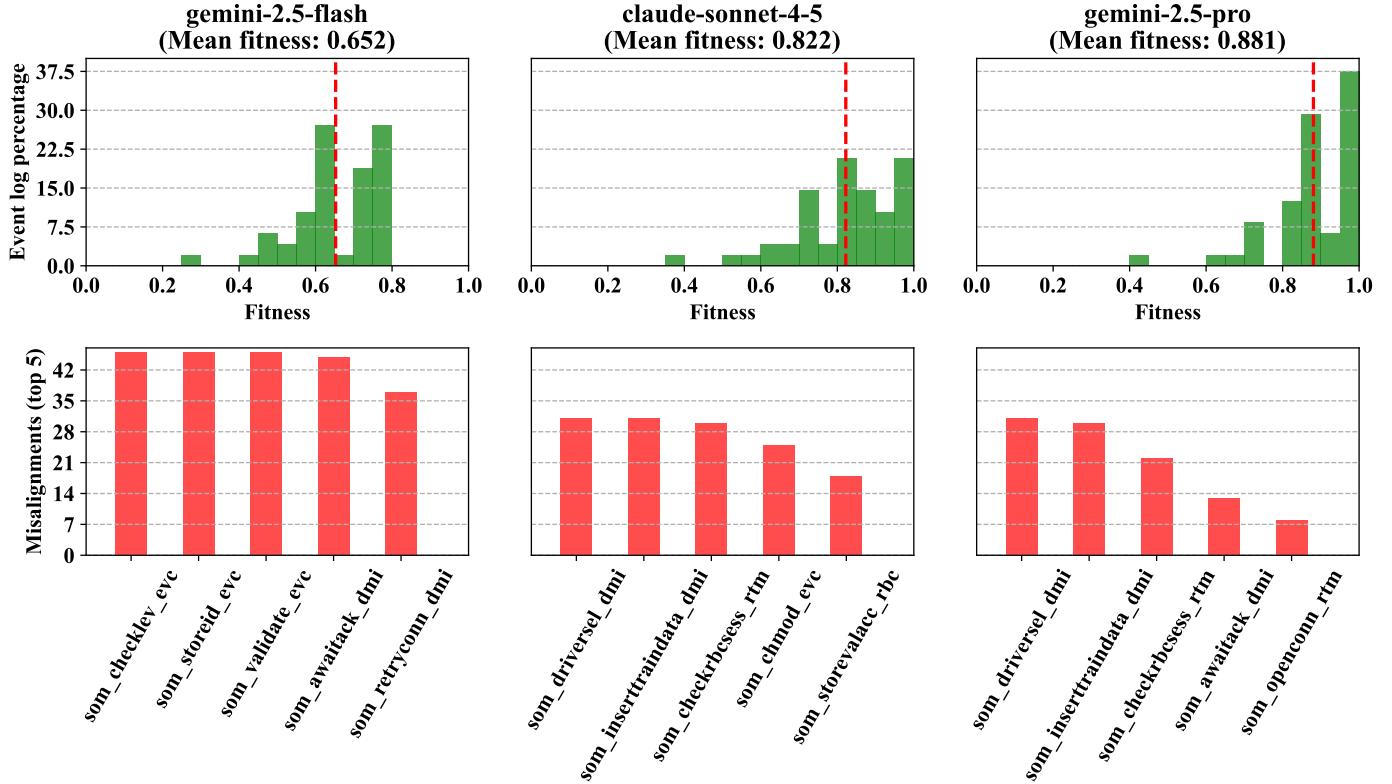


Figure 10: The fitness value distributions of the event logs obtained for each LLM, and the corresponding per-activity misalignments.

clude both the normal traces of the previous experiment and new anomalous traces generated by simulating the control-flow of Figure 9 and injecting three types of control-flow anomalies:

- Missing Activities (MA): The control flow is corrupted by removing an activity from the trace.
- Unknown Activities (UA): The control flow adds activities that were not included in the model.
- Wrongly-Ordered Activities (WOA): The control flow swaps the order of activities, opposed to the model prescriptions.

These three anomalies can be linked to the software fault injection taxonomy of Duraes and Madeira [15]. Specifically, the MA anomaly type corresponds directly to their “Missing construct” category, which the authors identified as the “dominant type of software bug”. Similarly, the UA anomaly type maps to their “extraneous construct” category, representing “surplus” code. Finally, the WOA anomaly type is a clear example of their “Wrong construct” category, which includes defects where the code is “wrongly coded or ill-formed”.

The injection process is as follows. Given an event log  $L \in \mathcal{B}(\mathcal{A}_\alpha^*)$  generated by simulating the model in Figure 9, we inject control-flow anomalies according to a Poissonian mechanism governed by a rate parameter  $\lambda > 0$ . For each trace  $\sigma \in L$ , the number of injected anomalies  $K$  is drawn from a Poisson distribution  $K \sim \text{Poisson}(\lambda)$ , so that  $P(K = k) = \frac{e^{-\lambda}\lambda^k}{k!}$ ,  $k = 0, 1, 2, \dots$ . The value of  $K$  determines how many modifications are applied to trace  $\sigma$ . Let  $AT \in \{\text{MA}, \text{WOA}, \text{UA}\}$  denote the anomaly type, for which MA involves randomly deleting  $K$  activities from  $\sigma$ , WOA involves random  $K$  swaps between pairs of activities in  $\sigma$ , and UA involves randomly inserting  $K$  new activities drawn uniformly from an unknown pool of activities at random positions in  $\sigma$ .  $\sigma$  is transformed into an anomalous version  $\tilde{\sigma}$  by applying the corresponding number and type of modifications:  $\tilde{\sigma} = f(\sigma, AT, K)$ , where  $f(\cdot)$  denotes the stochastic transformation induced by the selected anomaly mechanism. In this way, the Poisson parameter  $\lambda$  controls the expected number of anomalies per trace, providing a flexible and statistically grounded mechanism for simulating heterogeneous anomalous behavior in event logs.

Table 3: The anomaly detection metrics associated with each technique and anomaly type using the software logs generated through Gemini 2.5 pro. The bold figures indicate the best-performing technique for the selected metric per anomaly type.

Anomaly	Technique	Accuracy (%)	Recall (%)	Precision (%)	F1-score (%)	AUC (%)
MA	FT	44.052 ± 9.445	27.600 ± 14.935	84.517 ± 3.722	39.372 ± 18.105	62.232 ± 4.541
	DBSCAN	78.549 ± 2.669	<b>98.800 ± 2.400</b>	77.840 ± 2.979	87.001 ± 1.277	73.648 ± 5.058
	AE	<b>91.001 ± 2.856</b>	94.000 ± 4.561	<b>93.824 ± 3.165</b>	<b>93.788 ± 2.014</b>	<b>91.558 ± 2.424</b>
WOA	FT	79.972 ± 7.425	77.200 ± 11.703	94.447 ± 2.615	84.331 ± 6.967	88.507 ± 3.206
	DBSCAN	86.426 ± 7.008	<b>96.400 ± 2.939</b>	87.337 ± 8.294	91.339 ± 4.065	91.818 ± 4.355
	AE	<b>93.047 ± 2.480</b>	96.000 ± 3.347	<b>94.731 ± 3.773</b>	<b>95.252 ± 1.644</b>	<b>96.617 ± 2.336</b>
UA	FT	36.128 ± 5.656	17.000 ± 9.434	69.583 ± 13.353	26.504 ± 14.082	53.611 ± 5.389
	DBSCAN	81.464 ± 3.719	<b>96.400 ± 7.200</b>	82.106 ± 5.584	88.265 ± 2.276	83.592 ± 6.641
	AE	<b>93.337 ± 2.349</b>	96.000 ± 2.191	<b>94.931 ± 2.462</b>	<b>95.432 ± 1.609</b>	<b>95.961 ± 1.161</b>
ALL	FT	44.846 ± 10.198	39.467 ± 12.092	96.324 ± 1.368	54.813 ± 12.629	68.454 ± 3.499
	DBSCAN	91.242 ± 1.085	<b>99.600 ± 0.800</b>	91.352 ± 1.439	95.286 ± 0.539	84.232 ± 4.959
	AE	<b>94.081 ± 1.762</b>	95.467 ± 2.778	<b>97.855 ± 1.189</b>	<b>96.610 ± 1.050</b>	<b>93.515 ± 1.059</b>

The procedure above is applied three times against the traces of an event log  $L$  of 50 traces generated from the model in Figure 9. The first application of  $f$  injects MA anomalies in the traces of  $L$ , resulting in  $L_{MA}$ . Similarly, the second and third applications result in  $L_{WOA}$  and  $L_{UA}$ . In all three cases, we set  $\lambda = 3$ , i.e., on average, each individual trace has three instances of the selected anomaly. Finally, we consider  $L_{ALL} = L_{MA} \cup L_{WOA} \cup L_{UA}$ .

The selected conformance checking-based techniques are trained according to the framework in [45], where the normal event log is split into three sublogs: the training, validation and test event logs. Diagnoses are extracted for each event log. The training diagnoses are used to train two unsupervised machine learning techniques: the density-based spatial clustering of applications with noise (DBSCAN), which deals with noisy, high-dimensional and arbitrarily distributed data [39], and the autoencoder (AE), which is a neural network-based approach for dimensionality reduction that involves encoding and decoding the input data with the aim of minimizing the reconstruction error [38]. The validation diagnoses are used in two slightly different ways. For DBSCAN, a threshold is computed based on the distances of the validation data from the training clusters, whereas for AE, a threshold is built on the reconstruction error of validation data. The anomalous event logs are handled similarly and classified according to the threshold used. Please note that we only consider the normal event log generated by gemini-2.5-pro, as it is the highest quality log as highlighted in Table 2 and Figure 10.

We also consider the baseline Fitness Thresholding (FT) technique, which is solely based on setting a threshold on the fitness metric. This is the most intuitive approach for conformance checking-based anomaly detection, although it is not as effective, as the results will show.

As for the metrics, we use the widely recognized precision, recall, and F1-score metrics commonly employed by the anomaly detection community. In particular, given negative and positive traces, the traces flagged as, respectively, normal and anomalous, the aforementioned metrics are calculated through the true positives (TP), true negatives (TN), false positives (FP)

and false negatives (FN) classified by the technique:

$$\begin{aligned} \text{Accuracy} &= \frac{TP + TN}{TN + TP + FP + FN}, \\ \text{Precision} &= \frac{TP}{TP + FP}, \\ \text{Recall} &= \frac{TP}{TP + FN}, \\ \text{F1-score} &= 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}. \end{aligned}$$

In addition, we also use the Area Under the Receiving Operating Curve (AUC). The ROC curve plots the *True Positive Rate* (TPR) against the *False Positive Rate* (FPR), defined respectively as:

$$\begin{aligned} \text{TPR} &= \frac{TP}{TP + FN}, \\ \text{FPR} &= \frac{FP}{FP + TN}. \end{aligned}$$

The AUC is then computed as the integral of the ROC curve:

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR}) d(\text{FPR}),$$

and can be interpreted as the probability that the model assigns a higher anomaly score to a randomly chosen anomalous trace than to a randomly chosen normal one.

Table 3 reports the results achieved for each conformance checking-based technique. The best-performing techniques are always either DBSCAN or AE, i.e., those that integrate unsupervised machine learning on top of conformance checking. They significantly outperform the baseline FT technique for the MA and UA anomalies, whereas the WOA anomaly is well discriminated by FT as well. This indicates that while fitness allows finding wrongly-ordered anomalies, it fails at identifying missing and unknown anomalies, for which an extension using other machine learning techniques is required. Considering the

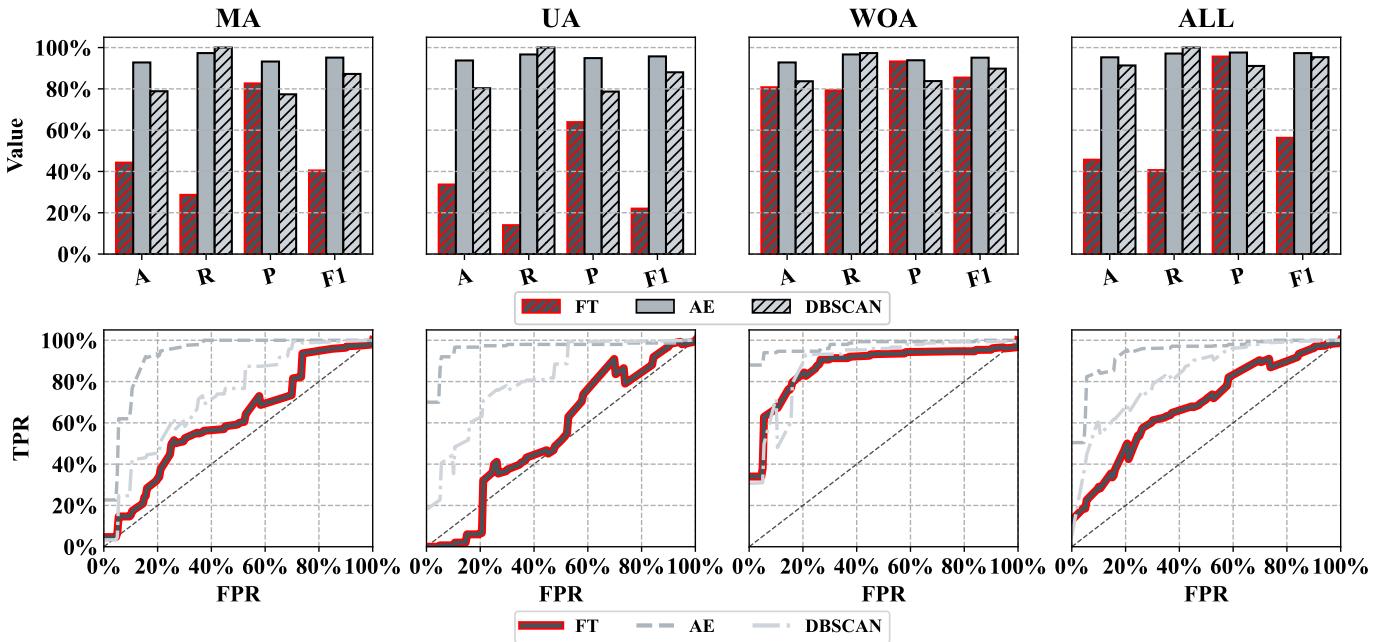


Figure 11: Bar plots of the accuracy (A), recall (R), precision (P), and F1-score (F1), and ROC curves associated with each technique and anomaly type.

overall performance across all the anomalies, the AE is able to top the other two techniques, achieving up to 96.610% F1-score and 93.515% AUC.

Figure 11 visually compares the metrics through bar plots and shows the corresponding ROC curves from which AUC is computed. The bar plots especially outline the superiority of the DBSCAN and AE techniques for all the anomaly types, especially for the accuracy, recall, and F1 metrics. The ROC curves at the bottom confirm this observation, and also show that the AE is the most stable across a wide variety of reconstruction error thresholds, i.e., its AUC is higher.

## 7. Discussion

### 7.1. RQ1: Source-code instrumentation

Obtaining quality software logs is pivotal to assessing the correctness of the computer-based system’s execution. The main challenge in instrumenting code regards the adequate placement of log instructions and the connection of software traces to high-level models to ensure correct operation. We addressed this challenge by the systematic incorporation of LLMs in the engineering process of high-stakes systems. Our approach demonstrated satisfying results, with gemini-2.5-pro achieving up to 84.8% coverage of the reference process model used to develop the prototype of SoM, the case-study ERTMS/ETCS scenario. However, the correct prompting and choice of the LLM are needed, as deepseek-V3.2 and gemini-2.5-flash showed significantly inferior performance compared to the aforementioned gemini-2.5-pro and claude-sonnet-4.5.

### 7.2. RQ2: Control-flow anomaly detection

The ability to identify control-flow anomalies through the proposed conformance checking-based monitor has been eval-

uated with well-established anomaly detection metrics and different techniques. We have used the normal traces generated by the best-performing LLM model to carry out our evaluations. The approach has proven successful, as different types of control-flow anomalies that can be linked to well-known software defects could be identified by the combination of alignment-based conformance checking and the AE with 96.610% F1 and 93.515% AUC. This finding also outlines the suitability of LLM-based source-code instrumentation for subsequent conformance checking-based control-flow anomaly detection.

In addition, it is worth noting that using the AE does not invalidate the explainability of the proposed approach, as feature-based explanations can be provided through post-hoc explainability tools, such as SHAP, to identify the misaligned activities that caused the highest reconstruction errors [45].

### 7.3. Threats to validity

Following common guidelines for empirical studies in software engineering [48], we discuss potential threats to construct, internal, and external validity.

#### 7.3.1. Construct validity

Construct validity concerns whether the employed evaluation metrics adequately capture the intended phenomena.

We used a wide variety of metrics to evaluate both the instrumentation quality of LLMs and the ability of conformance checking to leverage LLM-based instrumentation for control-flow anomaly detection. While we believe that the quality of anomaly detection was comprehensively evaluated, our coverage metric focuses exclusively on the degree to which control-flow paths of the reference process model are exercised. Hence, it is worth mentioning that there are other, more traditional

ways of assessing instrumentation quality, such as measuring *code coverage* (e.g., statement, branch, or path coverage), *instrumentation overhead* (i.e., the runtime and memory impact introduced by instrumentation), and *trace completeness* (the proportion of relevant execution events successfully captured).

### 7.3.2. Internal validity

Internal validity addresses the extent to which observed results can be attributed to the studied factors rather than to uncontrolled variables.

Our experiments revealed that different LLMs, despite being instructed with the same prompt, produced varying results in terms of fitness, control-flow coverage, average trace length, and number of variants. While these differences can be partly attributed to the intrinsic architectural and training complexities of the selected LLMs, other factors may have contributed to the observed variability. For instance, aspects such as prompt formatting, context length handling, or differences in the pretraining and fine-tuning data should be further explored.

Regarding the anomaly detection experiments, although we employed both clustering-based and reconstruction-based techniques on top of conformance checking diagnoses, their performance might still be affected by other experimental factors. These include the specific fine-tuning procedures applied, the choice of hyperparameter configurations, and the stochastic nature of optimization processes.

### 7.3.3. External validity

External validity concerns the extent to which the findings can be generalized beyond the specific context of the study.

While we explored the industry-relevant ERTMS/ETCS standard and specifically targeted the research questions that we formulated, the generalizability of the results regarding process model quality and anomaly detection effectiveness should be further validated by, e.g., referencing case studies implementing real software instrumented following our methodological approach.

## 8. Related work

This section provides an overview of the existing work regarding software monitoring, which we split into software logging and software anomaly detection.

### 8.1. Software logging

Briand et al. [5] proposed the instrumentation of Java programs to record objects' interactions and log the sequences of messages exchanged. Their objective was to reverse engineer the program and automatically obtain a sequence diagram to enhance the understanding of the software's internals. Cinque et al. [9] proposed the rule-based source-code instrumentation technique, which involves placing logging instructions in specific places in the program according to a system representation developed at design time. This allows for the collection of high-quality logs linked to the entities of the system and their interactions. The authors extended their work in [8] and compared

their technique to other logging approaches, such as assertion-checking and event logging. Their results indicate that different logging approaches can be combined to improve failure coverage. Zhang et al. [50] proposed a declarative approach to tag the structures of Java programs and insert logging instructions corresponding to those structures. The approach requires querying the program and specifying instrumentation commands, which can include logging instructions.

In addition to source-code instrumentation, the literature has proposed many binary-code instrumentation frameworks. Nethercote and Seward [33] presented Valgrind, a binary-code instrumentation framework that allows instrumenting the binary code at read/write instructions to registers and memory, system calls, and heap allocations. Engelke and Schulz [18] presented Instrew, which is similar to Valgrind, but optimizes instrumentation intrusiveness by leveraging the LLVM compiler infrastructure. While binary-code instrumentation is very flexible and can be optimized to reduce its overhead regarding software execution time and program size, source-code instrumentation typically leads to more interpretable and higher-quality logs. This is pivotal to obtaining meaningful descriptions of software executions.

In this paper, we focus on the source-code instrumentation. This technique places logging rules to record specific events occurring in a program and facilitates the connection of high-level models with the low-level implementation. We enhance this ability by integrating LLMs in the software development flow, which automates source-code instrumentation while leveraging their ability of understanding code structure.

### 8.2. Software anomaly detection

Traditional software anomaly detection approaches involve run-time verification of declarative specifications. Zee et al. [49] presented a run-time checker for Java able to verify whether safety specifications are met during software execution. The safety properties refer to the current and past states of the program at a specific point in time, where the state is represented by the variables' value. Zhao et al. [51] and Kejstová et al. [28] extended the idea of run-time verification by proposing run-time model-checking frameworks. The frameworks involve collecting the software state during its execution to restrict the state space of the reference software model. In this way, model-checking of declarative specifications becomes feasible at run-time due to the reduced time needed to check the specification properties.

Although run-time verification and model-checking are effective for verifying software behavior, they require accurate software specifications and models. Hence, the literature put forward several data-driven solutions for software anomaly detection. For example, Singh et al. [40] proposed a rule-based framework for anomaly detection that involves the selection of an optimized set of software features and the extraction of fuzzy rules that discriminate correct behaviors from anomalous ones. Denaro et al. [14] proposed a neural network-based unsupervised anomaly detection framework. The solution employs deep autoencoders trained using software key performance indicators to discriminate whether the software execution is cor-

rect. Data-driven methods using textual logs have also been proposed, although they usually target business process anomaly detection. These methods mostly aim to capture the relationships between the events of business process logs through neural network-based models, such as long-short term memory networks and autoencoders [46, 23, 45].

Although data-driven approaches have proven effective, they require laborious feature extraction through ad-hoc selection of software metrics and/or trace encodings [41]. In addition, the limited trustworthiness and explainability of advanced machine learning limits its use [17]. A promising area of research that addresses these issues is process mining, which combines traditional model-based analyses with data-driven insights. Cinque et al. [10] evaluated the capability of process mining to discover the normal behavior of the Apache web server as Petri nets with several algorithms, including the  $\alpha$ -miner, inductive miner, and integer linear programming-based miner. Subsequently, the authors performed a sensitivity analysis for the threshold to assign to the fitness metric for discriminating normal and anomalous behavior. Similarly, Pecchia et al. [35] evaluated the anomaly detection capability of process mining. The sensitivity analysis related to thresholding fitness assessed that higher fitness values lead to improved detection performance. However, the authors also remark that the quality of the model being discovered is critical to quality detection performance. In fact, they correlated noise in event logs handled by process discovery with negative effects on performance. In particular, as noise increases in event logs, there is a higher chance of false negatives, i.e., more misclassification of anomalies.

In this paper, we focus on extending the fitness thresholding approach above by including additional diagnoses in the control-flow anomaly detection process. Specifically, we integrate unsupervised machine learning on account of its anomaly detection capabilities in one-class classification settings.

## 9. Conclusions

In this paper, we took on the problem of run-time monitoring of complex computer-based systems to detect control-flow anomalies due to unexpected changes in the system, the environment, or other “unknown unknowns”. Given the limitations of run-time verification of declarative specifications in terms of strict consistency with prescriptive specifications and flexibility, we proposed a methodology to architect software monitors by combining LLMs with conformance checking to enable quality source-code instrumentation and fuzzy run-time control-flow analysis. We tested the methodology on a case-study scenario from ERTMS/ETCS, an industrial railway interoperability standard. The evaluation highlighted that the proposed methodology provides high-quality event logs through LLM-based source-code instrumentation and enables effective conformance checking-based control-flow anomaly detection.

Possibilities for industrial exploitation of the proposed approach include implementation through appropriate architectural frameworks for digital twins (see, e.g., [20] and [12]). Future work will further investigate the efficacy of the methodology in real-world case studies, addressing the generalization of

the proposal. In addition, a deeper investigation of the factors linked to LLMs that may influence the outcome of the instrumentation quality will be performed.

## Acknowledgement

The work of Francesco Vitale and Nicola Mazzocca was partly supported by the Spoke 9 “Digital Society & Smart Cities” of ICSC - Centro Nazionale di Ricerca in High Performance-Computing, Big Data and Quantum Computing, funded by the European Union - NextGenerationEU (PNRR-HPC,CUP:E63 C22000980007).

The work of Francesco Flammini was partly supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contracts no. 23.00321 (Academics4Rail) and 24.00528 (PhDs EU-Rail); those projects have been selected within the European Union’s Horizon Europe research and innovation programme under grant agreements no. 101121842 and 101175856, respectively.

Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the funding agencies, which cannot be held responsible for them.

## References

- [1] van der Aalst, W.M.P., Carmona, J., 2022. Process Mining Handbook. Springer, Cham, Switzerland. doi:[10.1007/978-3-031-08848-3](https://doi.org/10.1007/978-3-031-08848-3).
- [2] Anthropic, 2025. Claude sonnet 4.5 system card. <https://www.anthropic.com/clause/sonnet>. System documentation for the Sonnet 4.5 model.
- [3] Beek, M.H.t., Fantechi, A., Gnesi, S., 2018. Product line models of large cyber-physical systems: the case of ERTMS/ETCS, in: Proceedings of the 22nd International Systems and Software Product Line Conference - Volume 1, p. 208–214. doi:[10.1145/3233027.3233046](https://doi.org/10.1145/3233027.3233046).
- [4] Bombarda, A., Bonfanti, S., Gargantini, A., Lei, Y., Duan, F., 2023. RATE: A model-based testing approach that combines model refinement and test execution. Software Testing, Verification and Reliability 33, e1835. doi:[10.1002/stvr.1835](https://doi.org/10.1002/stvr.1835).
- [5] Briand, L., Labiche, Y., Leduc, J., 2006. Toward the Reverse Engineering of UML Sequence Diagrams for Distributed Java Software. IEEE Transactions on Software Engineering 32, 642–663. doi:[10.1109/TSE.2006.96](https://doi.org/10.1109/TSE.2006.96).
- [6] Casaluce, R., Burattin, A., Chiaromonte, F., Lafuente, A.L., Vandin, A., 2024. White-box validation of quantitative product lines by statistical model checking and process mining. Journal of Systems and Software 210, 111983. doi:[10.1016/j.jss.2024.111983](https://doi.org/10.1016/j.jss.2024.111983).
- [7] Chandola, V., Banerjee, A., Kumar, V., 2009. Anomaly detection: A survey. ACM Computing Surveys 41, 15:1–15:58. doi:[10.1145/1541880.1541882](https://doi.org/10.1145/1541880.1541882).

- [8] Cinque, M., Cotroneo, D., Corte, R.D., Pecchia, A., 2016. Characterizing Direct Monitoring Techniques in Software Systems. *IEEE Transactions on Reliability* 65, 1665–1681. doi:[10.1109/TSE.2022.3213041](https://doi.org/10.1109/TSE.2022.3213041).
- [9] Cinque, M., Cotroneo, D., Pecchia, A., 2013. Event Logs for the Analysis of Software Failures: A Rule-Based Approach. *IEEE Transactions on Software Engineering* 39, 806–821. doi:[10.1109/TSE.2012.67](https://doi.org/10.1109/TSE.2012.67).
- [10] Cinque, M., Della Corte, R., Pecchia, A., 2019. Discovering Hidden Errors from Application Log Traces with Process Mining, in: 2019 15th European Dependable Computing Conference (EDCC), pp. 137–140. doi:[10.1109/EDCC.2019.00034](https://doi.org/10.1109/EDCC.2019.00034).
- [11] Czepa, C., Zdun, U., 2020. On the Understandability of Temporal Properties Formalized in Linear Temporal Logic, Property Specification Patterns and Event Processing Language. *IEEE Transactions on Software Engineering* 46, 100–112. doi:[10.1109/TSE.2018.2859926](https://doi.org/10.1109/TSE.2018.2859926).
- [12] De Benedictis, A., Flammini, F., Mazzocca, N., Somma, A., Vitale, F., 2023. Digital twins for anomaly detection in the industrial internet of things: Conceptual architecture and proof-of-concept. *IEEE Transactions on Industrial Informatics* 19, 11553–11563. doi:[10.1109/TII.2023.3246983](https://doi.org/10.1109/TII.2023.3246983).
- [13] Delgado, N., Gates, A., Roach, S., 2004. A taxonomy and catalog of runtime software-fault monitoring tools. *IEEE Transactions on Software Engineering* 30, 859–872. doi:[10.1109/TSE.2004.91](https://doi.org/10.1109/TSE.2004.91).
- [14] Denaro, G., Heydarov, R., Mohebbi, A., Pezzè, M., 2023. Prevent: An Unsupervised Approach to Predict Software Failures in Production. *IEEE Transactions on Software Engineering* 49, 5139–5153. doi:[10.1109/TSE.2023.3327583](https://doi.org/10.1109/TSE.2023.3327583).
- [15] Durães, J.A., Madeira, H.S., 2006. Emulation of software faults: A field data study and a practical approach. *IEEE Transactions on Software Engineering* 32, 849–867. doi:[10.1109/TSE.2006.113](https://doi.org/10.1109/TSE.2006.113).
- [16] El-Masri, D., Petrillo, F., Guéhéneuc, Y.G., Hamou-Lhadj, A., Bouziane, A., 2020. A systematic literature review on automated log abstraction techniques. *Information and Software Technology* 122, 106276. URL: [10.1016/j.infsof.2020.106276](https://doi.org/10.1016/j.infsof.2020.106276), doi:[10.1016/j.infsof.2020.106276](https://doi.org/10.1016/j.infsof.2020.106276).
- [17] Elkhawaga, G., Elzeki, O.M., Abu-Elkheir, M., Reichert, M., 2024. Why Should I Trust Your Explanation? An Evaluation Approach for XAI Methods Applied to Predictive Process Monitoring Results. *IEEE Transactions on Artificial Intelligence* 5, 1458–1472. doi:[10.1109/TAI.2024.3357041](https://doi.org/10.1109/TAI.2024.3357041).
- [18] Engelke, A., Schulz, M., 2020. InStrew: leveraging LLVM for high performance dynamic binary instrumentation, in: Proceedings of the 16th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, p. 172–184. doi:[10.1145/3381052.3381319](https://doi.org/10.1145/3381052.3381319).
- [19] European Union Agency for Railways, 2024. Report on Railway Safety and Interoperability in the EU 2024. Technical Report. European Union Agency for Railways (ERA). URL: <https://www.era.europa.eu/system/files/2024-06/Report%20on%20Railway%20Safety%20and%20Interoperability%20in%20the%20EU%202024.pdf>.
- [20] Flammini, F., 2021. Digital twins as run-time predictive models for the resilience of cyber-physical systems: a conceptual framework. *Philosophical Transactions of the Royal Society A* 379, 20200369. doi:[10.1098/rsta.2020.0369](https://doi.org/10.1098/rsta.2020.0369).
- [21] Google DeepMind, 2025. Gemini 2.5: Pushing the frontier with advanced reasoning, multimodality, long context, and next generation agentic capabilities. URL: <https://arxiv.org/abs/2507.06261>, arXiv:2507.06261.
- [22] Gu, S., Rong, G., Zhang, H., Shen, H., 2023. Logging Practices in Software Engineering: A Systematic Mapping Study. *IEEE Transactions on Software Engineering* 49, 902–923. doi:[10.1109/TSE.2022.3166924](https://doi.org/10.1109/TSE.2022.3166924).
- [23] Guan, W., Cao, J., Zhao, H., Gu, Y., Qian, S., 2024. WAKE: A Weakly Supervised Business Process Anomaly Detection Framework via a Pre-Trained Autoencoder. *IEEE Transactions on Knowledge and Data Engineering* 36, 2745–2758. doi:[10.1109/TKDE.2023.3322411](https://doi.org/10.1109/TKDE.2023.3322411).
- [24] Havare, J., Chaudhary, S., Ramakrishnan, G., Maharajan, K., Tamilselvam, S., 2025. A code comprehension benchmark for large language models for code. URL: <https://arxiv.org/abs/2507.10641>, arXiv:2507.10641.
- [25] Huang, C.H., Peled, D.A., Schewe, S., Wang, F., 2016. A game-theoretic foundation for the maximum software resilience against dense errors. *IEEE Transactions on Software Engineering* 42, 605–622. doi:[10.1109/TSE.2015.2510001](https://doi.org/10.1109/TSE.2015.2510001).
- [26] Jongeling, R., Ciccozzi, F., Carlson, J., Cicchetti, A., 2022. Consistency management in industrial continuous model-based development settings: a reality check. *Software and Systems Modeling* 21, 1511–1530. doi:[10.1007/s10270-022-01000-5](https://doi.org/10.1007/s10270-022-01000-5).
- [27] Karaduman, B., Tezel, B.T., Challenger, M., 2023. Rational software agents with the BDI reasoning model for Cyber-Physical Systems. *Engineering Applications of Artificial Intelligence* 123, 106478. doi:[10.1016/j.engappai.2023.106478](https://doi.org/10.1016/j.engappai.2023.106478).

- [28] Kejstová, K., Ročkai, P., Barnat, J., 2017. From model checking to runtime verification and back, in: Runtime Verification: 17th International Conference, RV 2017, Seattle, WA, USA, September 13–16, 2017, Proceedings 17, Springer. pp. 225–240. doi:[10.1007/978-3-319-67531-2\\_14](https://doi.org/10.1007/978-3-319-67531-2_14).
- [29] Laroche, F., Guihéry, L., 2013. European Rail Traffic Management System (ERTMS): Supporting competition on the European rail network? *Research in Transportation Business & Management* 6, 81–87. doi:[10.1016/j.rtbm.2012.12.006](https://doi.org/10.1016/j.rtbm.2012.12.006).
- [30] Liu, C., 2018. Automatic Discovery of Behavioral Models From Software Execution Data. *IEEE Transactions on Automation Science and Engineering* 15, 1897–1908. doi:[10.1109/TASE.2018.2844725](https://doi.org/10.1109/TASE.2018.2844725).
- [31] Mamudu, A., Bandara, W., Wynn, M.T., Leemans, S.J., 2024. Process Mining Success Factors and Their Interrelationships. *Business & Information Systems Engineering* , 1–20doi:[10.1007/s12599-024-00860-z](https://doi.org/10.1007/s12599-024-00860-z).
- [32] Martin, N., Fischer, D.A., Kerpedzhiev, G.D., Goel, K., Leemans, S.J., Röglinger, M., van der Aalst, W.M., Dumas, M., La Rosa, M., Wynn, M.T., 2021. Opportunities and challenges for process mining in organizations: results of a Delphi study. *Business & Information Systems Engineering* 63, 511–527. doi:[10.1007/s12599-021-00720-0](https://doi.org/10.1007/s12599-021-00720-0).
- [33] Nethercote, N., Seward, J., 2007. Valgrind: a framework for heavyweight dynamic binary instrumentation, in: Proceedings of the 28th ACM SIGPLAN Conference on Programming Language Design and Implementation, p. 89–100. doi:[10.1145/1250734.1250746](https://doi.org/10.1145/1250734.1250746).
- [34] Pan, J., Liu, Z., Li, D., Wang, L., Li, B., 2023. An empirical study of software architecture resilience evaluation methods. *Journal of Systems and Software* 202, 111726. doi:[10.1109/TDSC.2015.2429128](https://doi.org/10.1109/TDSC.2015.2429128).
- [35] Pecchia, A., Weber, I., Cinque, M., Ma, Y., 2020. Discovering process models for the analysis of application failures under uncertainty of event logs. *Knowledge-Based Systems* 189, 105054. doi:[10.1016/j.knosys.2019.105054](https://doi.org/10.1016/j.knosys.2019.105054).
- [36] Pradhan, S., Dubey, A., Levendovszky, T., Kumar, P.S., Emfinger, W.A., Balasubramanian, D., Otte, W., Karsai, G., 2016. Achieving resilience in distributed software systems via self-reconfiguration. *Journal of Systems and Software* 122, 344–363. doi:[10.1016/j.jss.2016.05.038](https://doi.org/10.1016/j.jss.2016.05.038).
- [37] Prokop, L.E., 2024. Historical aerospace software errors categorized to influence fault tolerance, in: 2024 IEEE Aerospace Conference, pp. 1–12. doi:[10.1109/AER058975.2024.10521061](https://doi.org/10.1109/AER058975.2024.10521061).
- [38] Sakurada, M., Yairi, T., 2014. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction, in: Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis, Association for Computing Machinery, New York, NY, USA. pp. 4–11. doi:[10.1145/2689746.2689747](https://doi.org/10.1145/2689746.2689747).
- [39] Schubert, E., Sander, J., Ester, M., Kriegel, H.P., Xu, X., 2017. Dbscan revisited, revisited: Why and how you should (still) use dbscan. *ACM Transactions on Database Systems* 42. doi:[10.1145/3068335](https://doi.org/10.1145/3068335).
- [40] Singh, P., Pal, N.R., Verma, S., Vyas, O.P., 2017. Fuzzy Rule-Based Approach for Software Fault Prediction. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 47, 826–837. doi:[10.1109/TSMC.2016.2521840](https://doi.org/10.1109/TSMC.2016.2521840).
- [41] Tavares, G.M., Oyamada, R.S., Barbon, S., Ceravolo, P., 2023. Trace encoding in process mining: A survey and benchmarking. *Engineering Applications of Artificial Intelligence* 126, 107028. doi:[10.1016/j.engappai.2023.107028](https://doi.org/10.1016/j.engappai.2023.107028).
- [42] Tetlie, G., Muller, G., Kokkula, S., 2024. Literature review and research design for systems integration: Case study in defense systems, in: The Proceedings of the 2023 Conference on Systems Engineering Research, Springer Nature Switzerland, Cham. pp. 691–705. doi:[10.1007/978-3-031-49179-5\\_47](https://doi.org/10.1007/978-3-031-49179-5_47).
- [43] Tröls, M.A., Mashkoor, A., Egyed, A., 2019. Multi-faceted consistency checking of collaborative engineering artifacts, in: 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), IEEE. pp. 278–287. doi:[10.1109/MODELS-C.2019.00044](https://doi.org/10.1109/MODELS-C.2019.00044).
- [44] Viganò, E., Cornejo, O., Pastore, F., Briand, L.C., 2022. Data-driven mutation analysis for cyber-physical systems. *IEEE Transactions on Software Engineering* 49, 2182–2201. doi:[10.1109/TSE.2022.3213041](https://doi.org/10.1109/TSE.2022.3213041).
- [45] Vitale, F., Pegoraro, M., van der Aalst, W.M., Mazzocca, N., 2025. Control-flow anomaly detection by process mining-based feature extraction and dimensionality reduction. *Knowledge-Based Systems* 310, 112970. doi:[10.1016/j.knosys.2025.112970](https://doi.org/10.1016/j.knosys.2025.112970).
- [46] Wang, X., Yang, L., Li, D., Ma, L., He, Y., Xiao, J., Liu, J., Yang, Y., 2022. MADDC: Multi-Scale Anomaly Detection, Diagnosis and Correction for Discrete Event Logs, in: Proceedings of the 38th Annual Computer Security Applications Conference, p. 769–784. doi:[10.1145/3564625.3567972](https://doi.org/10.1145/3564625.3567972).
- [47] Weidmann, N., 2018. Tolerant consistency management in model-driven engineering, in: Proceedings of the 21st ACM/IEEE International Conference on Model

Driven Engineering Languages and Systems: Companion Proceedings, pp. 192–197. doi:[10.1145/3270112.3275339](https://doi.org/10.1145/3270112.3275339).

- [48] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A., 2012. Experimentation in Software Engineering. Springer, Berlin, Heidelberg. doi:[10.1007/978-3-642-29044-2](https://doi.org/10.1007/978-3-642-29044-2).
- [49] Zee, K., Kuncak, V., Taylor, M., Rinard, M., 2007. Runtime checking for program verification, in: Runtime Verification: 7th International Workshop, RV 2007, Vancouver, Canada, March 13, 2007, Revised Selected Papers 7, Springer. pp. 202–213. doi:[10.1007/978-3-540-77395-5\\_17](https://doi.org/10.1007/978-3-540-77395-5_17).
- [50] Zhang, T., Zheng, X., Zhang, Y., Zhao, J., Li, X., 2015. A declarative approach for Java code instrumentation. Software Quality Journal 23, 143–170. doi:[10.1007/s11219-013-9220-4](https://doi.org/10.1007/s11219-013-9220-4).
- [51] Zhao, Y., Rammig, F., 2009. Model-based runtime verification framework. Electronic Notes in Theoretical Computer Science 253, 179–193. doi:[10.1016/j.entcs.2009.09.035](https://doi.org/10.1016/j.entcs.2009.09.035).
- [52] Zimmermann, L., Zerbato, F., Weber, B., 2023. What makes life for process mining analysts difficult? A reflection of challenges. Software and Systems Modeling , 1–29doi:[10.1007/s10270-023-01134-0](https://doi.org/10.1007/s10270-023-01134-0).
- [53] Zoppi, T., Ceccarelli, A., Capecchi, T., Bondavalli, A., 2021. Unsupervised Anomaly Detectors to Detect Intrusions in the Current Threat Landscape. ACM/IMS Transactions on Data Science 2. doi:[doi.org/10.1145/3441140](https://doi.org/10.1145/3441140).