International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(9s) 2026 pp. 1365-1397
https://doi.org/10.70917/ijcisim-2026-3558
Article

An Intelligent Framework for Signal Integrity and Communication Reliability in CAN-Based Autonomous Vehicle Systems

V. L. Manasa Mandalapu[1], P. Venkatramana[2]

[1]Department of ECE, School of Engineering and Technology, Mohan Babu University.
Email: **manasamandalapu33@gmail.com**
ORCID: **0000-0002-2431-4237**
[2] Mohan Babu University.
Email: **pvramana2604@gmail.com**
ORCID: **0000-0001-5732-6085**

Abstract: The growing dependence of autonomous vehicles on continuous data exchange between electronic control units, sensors, and actuators has increased the need for reliable in-vehicle communication. The Controller Area Network (CAN) remains widely used for automotive communication because of its robustness, simplicity, and real-time message handling capabilities. However, increasing network traffic, electromagnetic interference, signal disturbances, transmission errors, and changing bus conditions can affect signal integrity and reduce communication reliability. Such disturbances may become critical in autonomous vehicle systems, where delayed or corrupted information can influence time-sensitive control decisions. This study proposes an intelligent framework for monitoring signal integrity and evaluating communication reliability in CAN-based autonomous vehicle systems. The framework combines communication-level measurements with an intelligent assessment mechanism to identify abnormal transmission behaviour and estimate the reliability of network conditions. Parameters including signal-to-noise ratio, bit and frame error characteristics, communication latency, bus load, and message loss are considered to represent the operational state of the CAN network. The proposed approach is designed to distinguish stable communication from degraded and potentially unreliable conditions while supporting early identification of communication anomalies. Its performance is evaluated under varying traffic loads and disturbance scenarios and compared with conventional monitoring approaches using reliability and detection-oriented performance measures. The framework is expected to provide a more adaptive method of assessing CAN communication quality than fixed-rule monitoring alone. The study contributes a structured approach for improving communication awareness and supporting dependable data exchange in autonomous vehicle architectures, with potential applicability to advanced driver assistance systems and other safety-critical automotive communication environments.

Keywords: Autonomous Vehicles, Controller Area Network (CAN), Signal Integrity, Communication Reliability, Intelligent Monitoring; In-Vehicle Networks, Anomaly Detection, Automotive Communication Systems.

1. Introduction

Autonomous vehicles depend on the continuous exchange of information among sensing, computation, and control components. Cameras, radar units, electronic control units (ECUs), braking systems, steering controllers, and other embedded devices must communicate within strict timing and reliability constraints. A failure in this communication chain may have consequences beyond ordinary data loss because the exchanged messages often contribute directly to vehicle control decisions. As vehicle functions become increasingly automated, the reliability of the underlying in-vehicle communication network therefore becomes an important part of overall system dependability.

The Controller Area Network (CAN) has been one of the most established communication technologies in automotive electronic systems. Originally developed to reduce complex point-to-point wiring, CAN provides a shared communication medium through which multiple electronic units can exchange messages using priority-based arbitration. Its practical advantages include relatively low implementation cost, deterministic message prioritization, built-in error detection, and fault confinement mechanisms. These characteristics have supported its widespread use in powertrain control, body electronics, chassis systems, and other automotive applications [1], [2]. Even with the introduction of newer communication technologies, CAN continues to remain relevant because a large number of vehicle functions and embedded controllers are designed around the protocol.

The communication environment of an autonomous vehicle, however, is considerably more demanding than that of a conventional vehicle with a limited number of electronic functions. The number of interconnected components has increased, while the volume and timing sensitivity of transmitted information have also become more significant. Messages associated with braking, steering, vehicle dynamics, and supervisory control may coexist with less critical network traffic. Under such conditions, variations in bus load, message priority, transmission delay, electrical disturbances, and communication faults can influence the quality and availability of information. Previous studies on automotive communication systems have highlighted the growing difficulty of satisfying timing and dependability requirements as in-vehicle networks become more complex [3], [4].

Signal integrity is an important physical and communication-level consideration in this context. A transmitted signal may be affected by electromagnetic interference, electrical noise, impedance discontinuities, cable characteristics, termination conditions, and disturbances generated by other electronic components. When signal quality deteriorates sufficiently, the receiver may interpret transmitted bits incorrectly, resulting in corrupted frames, retransmissions, increased delay, or temporary communication disruption. The CAN protocol includes mechanisms such as cyclic redundancy checks, acknowledgement checking, bit monitoring, and error confinement, but protocol-level error handling does not eliminate the underlying conditions responsible for signal degradation [1], [2]. A network may continue operating while experiencing an increasing number of communication disturbances, making early recognition of deteriorating conditions particularly valuable.

Communication reliability in an autonomous vehicle should therefore not be considered only in terms of whether a CAN message eventually reaches its destination. The quality of communication is also influenced by the consistency of message delivery, latency, error frequency, network utilization, and the ability of the system to maintain acceptable operation under changing conditions. A network experiencing intermittent errors or repeated retransmissions may technically remain operational while becoming unsuitable for time-sensitive control tasks. This distinction is important because autonomous driving functions depend not only on correct information but also on its timely and dependable availability.

Conventional CAN monitoring commonly relies on predefined error indicators, diagnostic rules, or fixed thresholds. These approaches are useful for identifying known faults but may provide a limited representation of network behaviour when several communication parameters change simultaneously. For example, an increase in bus load may not independently indicate a fault, and a temporary change in latency may remain within an acceptable range. When such changes occur together with increasing frame errors or deteriorating signal conditions, however, they may represent a developing reliability problem. A monitoring mechanism that evaluates these parameters collectively may therefore provide a more meaningful assessment than isolated threshold-based observations.

The growing complexity of automotive networks has encouraged the application of intelligent and data-driven methods for analysing CAN traffic. Existing research has demonstrated the usefulness of machine learning and anomaly-detection techniques for identifying unusual message patterns and abnormal network behaviour **[6]–[9]**. Much of this work has concentrated on cybersecurity and intrusion detection, where CAN messages are analysed to identify malicious or unexpected traffic. Although these studies demonstrate the potential of intelligent analysis, communication reliability arising from the combined effects of signal quality, network conditions, and transmission behaviour requires further investigation. In particular, there is scope for a framework that relates measurable communication characteristics to an interpretable assessment of network reliability.

This study addresses this requirement by proposing an intelligent framework for signal integrity assessment and communication reliability monitoring in CAN-based autonomous vehicle systems. The proposed framework considers multiple indicators of communication performance rather than treating individual network parameters in isolation. Signal-to-noise characteristics, error behaviour, communication latency, bus load, and message loss are incorporated into a common monitoring process. These observations are then evaluated through an intelligent assessment mechanism to distinguish normal operating conditions from degraded and potentially unreliable communication states.

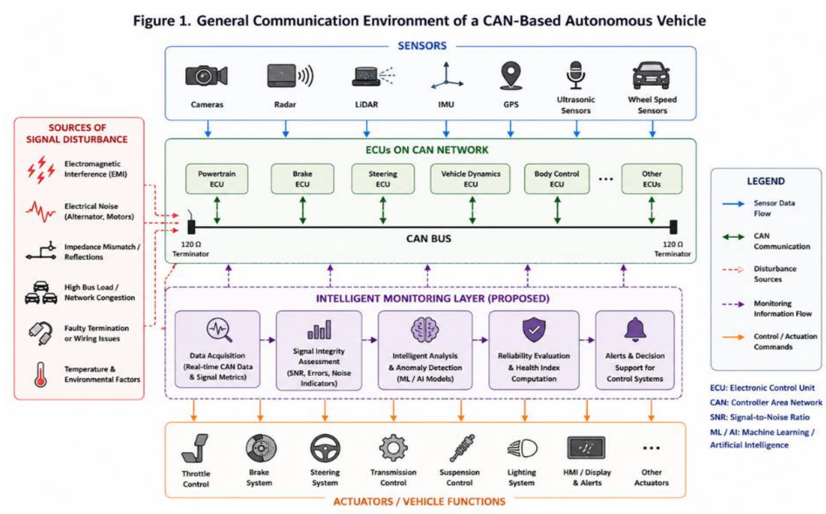

Figure 1: General communication environment of a CAN-based autonomous vehicle

The purpose of the proposed approach is not to replace the error-handling mechanisms already available in CAN. Instead, it introduces an additional level of communication awareness capable of identifying patterns that may indicate progressive degradation or abnormal network behaviour. Such an approach can be useful in situations where individual parameters remain within nominal limits but their combined behaviour suggests a reduction in communication quality. By continuously evaluating the state of the network, the framework is intended to support earlier identification of reliability concerns and provide a more adaptive basis for communication assessment.

The principal contributions of this study are fourfold. First, it presents a unified framework in which signal-related and network-level indicators are considered together for CAN communication assessment. Second, it introduces an intelligent monitoring mechanism for classifying communication conditions according to their reliability characteristics. Third, it evaluates the framework under different traffic and disturbance conditions using performance measures associated with transmission quality, error behaviour, latency, and detection capability. Finally, it provides a comparative basis for examining whether an intelligent multi-parameter assessment can offer advantages over conventional fixed-rule monitoring.

The remainder of the paper is organized as follows. Section 2 reviews previous research on CAN-based vehicular communication, signal integrity, communication reliability, and intelligent network monitoring. Section 3 describes the characteristics and reliability challenges of CAN communication in autonomous vehicle environments. Section 4 presents the architecture and operation of the proposed intelligent framework. Section 5 explains the research methodology, experimental conditions, and performance measures. Section 6 presents and analyses the results, while Section 7 discusses their technical implications and the limitations of the proposed approach. Finally, Section 8 concludes the study and identifies directions for future research.

2. Related Work and Literature Review

Research on in-vehicle communication has developed alongside the increasing use of distributed electronic control systems in modern vehicles. Earlier automotive networks were primarily designed to exchange relatively small amounts of control information among electronic control units (ECUs). The introduction of advanced driver assistance and autonomous driving functions has changed this operating environment considerably. A larger number of sensors, controllers, and actuators now participate in vehicle operation, making communication reliability dependent on both network behaviour and the quality of the physical transmission medium.

2.1 CAN-Based In-Vehicle Communication

The Controller Area Network (CAN) has remained one of the most widely adopted communication protocols in automotive systems because of its distributed architecture, priority-based arbitration, and integrated error-handling mechanisms. CAN allows multiple ECUs to share a common communication medium without requiring a central bus controller. When two or more nodes attempt to transmit simultaneously, message identifiers determine priority, allowing the higher-priority frame to continue without destructive collision. This mechanism is particularly useful for time-sensitive vehicle functions, although its performance depends strongly on message scheduling and network utilization [1], [2].

Tindell et al. [5] established an important analytical basis for evaluating CAN message response times. Their work demonstrated that message priority, blocking, interference from higher-priority traffic, and transmission characteristics must be considered when determining whether messages can satisfy real-time deadlines. This remains relevant to autonomous vehicle communication because increased bus utilization can extend the response time of lower-priority messages even when the network is functioning correctly.

Navet et al. [3] examined broader trends in automotive communication systems and identified increasing electronic complexity as a major challenge for in-vehicle networks. Their analysis showed that communication architectures must satisfy requirements involving real-time behaviour, dependability, cost, and electromagnetic compatibility. These requirements have become even more important with the emergence of highly automated vehicle functions, where communication delays and errors may influence control decisions.

Although CAN was originally developed for robust distributed control, the increasing number of ECUs and the growth of message traffic create operational limitations. A conventional CAN network offers limited bandwidth, and its priority-based arbitration can produce uneven delays under high-load conditions. Consequently, communication reliability cannot be assessed solely by confirming whether frames are successfully transmitted. The timing of message delivery, frequency of retransmission, error occurrence, and overall bus utilization also need to be considered.

2.2 Signal Integrity and Physical-Layer Reliability

The physical quality of a CAN signal has a direct influence on the correctness of data transmission. CAN uses differential signalling through the CAN-H and CAN-L lines, which provides resistance to common-mode noise. Nevertheless, the network remains affected by practical electrical conditions such as electromagnetic interference, improper termination, cable length, connector degradation, impedance discontinuities, reflections, and disturbances produced by motors, switching devices, and other electronic components.

Signal integrity problems do not always result in immediate network failure. In many cases, the CAN error-handling mechanism detects an incorrect frame and initiates retransmission. Repeated disturbances, however, may increase communication delay and error counters while reducing the effective availability of the network. For safety-related vehicle functions, a communication channel that repeatedly recovers from errors may still represent a degraded operating condition.

The physical and protocol layers are therefore closely related. Noise and waveform degradation originate at the physical level, while their effects may appear at the communication level as bit errors, frame errors, retransmissions, or delayed message delivery. Traditional network diagnostics often observe these effects after they have already influenced communication. A more comprehensive monitoring strategy should consider both the indicators associated with signal quality and the resulting behaviour of the communication network.

Automotive embedded-system research has also emphasized that dependability must be considered across multiple architectural layers rather than as an isolated property of a single protocol component [4]. This is especially relevant in autonomous vehicles, where sensor information passes through several stages before reaching a control function. A disturbance in communication may therefore propagate beyond the network itself and affect the timeliness or consistency of downstream decisions.

2.3 Communication Reliability and Real-Time Performance

Communication reliability in CAN networks has frequently been studied through timing analysis, fault tolerance, schedulability, and error recovery. The work of Tindell et al. [5] provided a foundation for worst-case response-time analysis, while subsequent research in automotive embedded systems expanded attention toward distributed timing constraints and dependable network architectures [3], [4].

Bus load is one of the principal variables affecting CAN communication performance. As network utilization increases, high-priority messages continue to receive preferential access, whereas lower-priority messages may experience longer waiting times. This behaviour is acceptable when message priorities are properly assigned, but rapidly changing traffic conditions can make static assumptions less representative of actual operation. Autonomous vehicle systems may generate communication patterns that vary according to driving conditions, sensor activity, and control requirements.

Reliability is also affected by the interaction of several parameters. A small increase in latency may not indicate a serious problem when considered independently. Similarly, a temporary rise in bus load or an isolated frame error may remain within acceptable limits. A different interpretation may be required when increased latency occurs together with repeated errors, message loss, and declining signal quality. This interaction motivates the use of multi-parameter assessment rather than independent threshold checks.

Most conventional diagnostic mechanisms are effective when the fault condition is known in advance and can be represented by a specific limit or rule. Their effectiveness may be reduced when network degradation develops gradually or when several individually moderate changes occur at the same time. For this reason, intelligent analysis has increasingly been investigated as a means of learning normal communication behaviour and identifying deviations that are difficult to describe through fixed rules.

2.4 Intelligent Monitoring and Anomaly Detection in CAN Networks

A substantial body of recent CAN research has focused on intelligent anomaly detection. Although much of this literature has been motivated by cybersecurity, the underlying methods are also relevant to communication-health monitoring because they demonstrate that abnormal CAN behaviour can be identified from patterns in network data.

Müter and Asaj [6] introduced an entropy-based approach for detecting anomalies in in-vehicle networks. Their work was based on the observation that normal CAN traffic exhibits relatively stable statistical characteristics and that abnormal activity can alter this behaviour. The study demonstrated the potential of data-driven monitoring without requiring inspection of every message according to a predefined fault rule.

Han et al. [7] proposed an anomaly intrusion detection approach based on survival analysis. Their method considered the timing behaviour of CAN messages and used deviations from expected message arrival characteristics to identify anomalous activity. This work is particularly relevant to communication reliability because message timing can provide information about both abnormal traffic and changes in network performance.

Avatefipour et al. [9] investigated machine-learning-based anomaly detection for CAN communication. Their work illustrated the potential of intelligent classification for distinguishing normal and abnormal network states. Machine-learning methods can consider relationships among several input features, which offers an advantage when network behaviour cannot be represented adequately by a single threshold.

Deep-learning approaches have further extended this direction by analysing temporal and structural patterns in CAN traffic. Such methods can capture nonlinear relationships and sequential dependencies, but they may also introduce higher computational requirements and reduced interpretability. For an in-vehicle monitoring system, high detection performance alone is insufficient; the method must also be suitable for real-time operation and should provide a meaningful representation of why a communication state has been classified as abnormal.

Bozdal et al. [8] reviewed major challenges associated with CAN-based vehicle networks and highlighted the continuing importance of monitoring mechanisms as automotive systems become increasingly connected. Their study primarily addressed security concerns, but it also reinforced a broader issue: CAN communication should no longer be treated as a permanently stable internal channel. Continuous observation of network behaviour is becoming increasingly important as vehicle architectures grow in complexity.

More recent research has continued to explore machine learning, deep learning, temporal modelling, and hybrid techniques for CAN anomaly detection. These studies generally report that data-driven approaches can identify complex deviations more effectively than simple rule-based methods when representative training and evaluation data are available. At the same time, their performance depends on feature selection, dataset quality, computational cost, and the ability to generalize beyond the conditions represented during model development.

2.5 Limitations of Existing Research

The existing literature provides strong foundations in CAN timing analysis, protocol reliability, network security, and intelligent anomaly detection. However, these research directions are often examined separately. Physical signal quality is commonly treated as an electrical or hardware-level problem, while CAN anomaly detection is largely studied from a cybersecurity perspective. Real-time performance studies, in contrast, frequently concentrate on schedulability, latency, and message response time.

This separation creates an important gap for autonomous vehicle communication. A deteriorating network condition may involve several forms of evidence at the same time. Electrical noise may affect signal quality, leading to frame errors and retransmissions. Increased traffic may raise bus utilization and delay message delivery. A developing wiring or termination problem may produce intermittent behaviour rather than an immediate and easily identifiable failure. Monitoring only one category of information may therefore provide an incomplete view of communication health.

A further limitation is the widespread dependence on binary classifications such as normal and abnormal. For communication reliability assessment, a more gradual representation may be useful. Network operation can move from stable to degraded conditions before reaching a critical state. Identifying this intermediate condition can support earlier intervention and may be more valuable than detecting failure only after communication performance has deteriorated substantially.

Table 1. Comparative Summary of Representative Studies Related to CAN Communication Monitoring

Study		**Main Approach**	**Parameters/Information Considered**	**Identified Limitation**
Tindell et al. [5]	Real-time CAN performance	Response-time analysis	Priority, blocking, interference, transmission time	Focused mainly on schedulability and timing
Navet et al. [3]	Automotive communication systems	Architectural and technological analysis	Real-time, dependability and network requirements	Broad system-level analysis rather than intelligent condition monitoring
Müter and Asaj [6]	CAN anomaly detection	Entropy-based analysis	Statistical characteristics of network traffic	Primarily anomaly/security oriented
Han et al. [7]	Vehicular network anomaly detection	Survival analysis	Message timing and arrival behaviour	Limited integration of physical signal-quality indicators
Avatefipour et al. [9]	Intelligent CAN anomaly detection	Machine-learning-based classification	CAN traffic features	Focused mainly on anomalous network activity
Bozdal et al. [8]	CAN network challenges	Security and vulnerability analysis	CAN architecture and attack-related risks	Does not provide an integrated signal-integrity and reliability assessment framework
Proposed Study	Signal integrity and communication reliability	Intelligent multi-parameter monitoring framework	Signal quality, error behaviour, latency, bus load and message loss	Integrates communication-health indicators into a unified reliability assessment

2.6 Research Gap and Motivation

The literature indicates that CAN reliability has been studied from several valuable but largely distinct perspectives. Timing analysis explains whether messages can satisfy real-time requirements; physical-layer studies address electrical transmission quality; and intelligent anomaly-detection research identifies deviations in CAN traffic. What remains less developed is an integrated approach that combines these forms of information to assess the operational reliability of the communication channel itself.

The present study is motivated by the need to connect signal-level degradation with observable network behaviour. Rather than relying on a single indicator, the proposed framework considers signal-to-noise characteristics, communication errors, latency, bus load, and message loss as related observations of CAN network condition. An intelligent assessment mechanism is then used to interpret their combined behaviour and distinguish stable, degraded, and potentially unreliable communication states.

This approach differs from conventional intrusion-detection research because the primary objective is not limited to identifying malicious traffic. It also differs from fixed-threshold diagnostics because reliability is assessed through the collective behaviour of multiple communication indicators. The intended contribution is therefore a communication-health framework capable of providing a broader and more adaptive assessment of CAN operation in autonomous vehicle systems.

3. CAN-Based Communication in Autonomous Vehicle Systems

The communication architecture of an autonomous vehicle is formed by a large number of electronic components that must exchange information within tightly controlled time limits. Sensors observe the vehicle and its surroundings, electronic control units process these observations, and actuators execute commands related to steering, braking, propulsion, and other functions. Although autonomous driving platforms may employ several communication technologies, the Controller Area Network (CAN) continues to serve as an important in-vehicle network for distributed control and coordination among electronic subsystems.

3.1 Role of CAN in the In-Vehicle Communication Architecture

CAN was designed as a multi-master serial communication protocol for embedded control applications. Instead of establishing a dedicated connection between every pair of electronic units, multiple nodes communicate through a shared bus. This architecture reduces wiring complexity and allows messages generated by one node to be observed by other nodes connected to the same network [1], [2].

Communication in CAN is message-oriented rather than address-oriented. A transmitted frame contains an identifier that represents the meaning and priority of the message rather than the physical address of a receiving node. Each ECU determines whether a received message is relevant to its operation. This arrangement is well suited to distributed vehicle control because the same information can be made available to several control units without requiring separate point-to-point transmissions.

A typical autonomous vehicle contains multiple functional domains. Perception-related sensors generate information about the vehicle and its environment, while control units responsible for braking, steering, propulsion, and vehicle dynamics exchange status and command messages. Not all high-bandwidth sensor data are necessarily transmitted directly over conventional CAN. Cameras and LiDAR systems, for example, may use higher-capacity interfaces for raw data transfer. CAN nevertheless remains relevant for control commands, sensor status, actuator information, diagnostic communication, and coordination among embedded controllers.

The communication process can be represented as a sequence in which sensor observations are acquired, processed by one or more ECUs, communicated across the in-vehicle network, and translated into actuator responses. The reliability of this sequence depends on the correct and timely transfer of information between the participating components.

3.2 Message Arbitration and Real-Time Communication

One of the defining characteristics of CAN is its priority-based arbitration mechanism. When multiple nodes attempt to access the bus simultaneously, arbitration is performed using the message identifier. Dominant and recessive bit states allow the highest-priority message to continue transmission while lower-priority nodes stop transmitting and retry later. This process is non-destructive because the winning frame does not need to be retransmitted as a result of the arbitration event [1].

The mechanism is effective for ensuring rapid access for safety-critical or time-sensitive messages. A braking-related message, for example, can be assigned a higher priority than a less time-critical status update. However, priority-based communication also means that message delay is not uniform across the network. Lower-priority frames may experience longer response times when the bus is heavily loaded or when higher-priority messages are transmitted frequently.

Tindell et al. [5] demonstrated that CAN response time is influenced by blocking, interference from higher-priority traffic, transmission time, and message release patterns. These factors remain important in autonomous vehicle systems, where the timing requirements of control messages may vary considerably. A message can be transmitted without corruption and still become operationally unsuitable if it arrives too late for the control task that depends on it.

Bus utilization therefore has a direct relationship with communication performance. At low or moderate utilization, messages can generally access the bus with limited contention. As traffic increases, arbitration occurs more frequently and waiting times may rise, particularly for lower-priority frames. High utilization does not automatically indicate communication failure, but it reduces the available timing margin and can make the network more sensitive to errors and retransmissions.

3.3 CAN Frame Transmission and Error Management

CAN incorporates several mechanisms intended to support reliable data transfer. Depending on the CAN format, a frame contains arbitration information, control fields, data, a cyclic redundancy check, acknowledgement information, and frame delimiters. These elements allow receiving nodes to verify aspects of transmission correctness and participate in error detection [1], [10].

The protocol can detect several forms of communication error, including bit errors, stuffing errors, cyclic redundancy check errors, form errors, and acknowledgement errors. When an error is detected, the affected frame is invalidated and may subsequently be retransmitted. CAN also maintains transmit and receive error counters that influence the error state of a node. A node may progress through error-active, error-passive, and bus-off states depending on the persistence and severity of detected communication problems.

These mechanisms contribute significantly to CAN robustness, but they should not be interpreted as a complete measure of communication health. Error recovery is reactive: it responds after a communication irregularity has been detected. A network exposed to repeated disturbances may continue to deliver data through retransmission while experiencing increasing delay and reduced efficiency. From the perspective of an autonomous vehicle, successful recovery from an error does not necessarily mean that the communication environment is operating under healthy conditions.

The distinction between protocol correctness and communication reliability is therefore important. Protocol mechanisms determine whether an individual frame satisfies defined transmission rules, whereas communication reliability concerns the broader ability of the network to provide dependable information over time. A complete assessment should consequently consider not only detected errors but also the frequency of their occurrence, their effect on latency, message availability, and the conditions under which they arise.

3.4 Signal Integrity in the CAN Physical Layer

At the physical layer, CAN commonly uses differential signalling over a twisted-pair medium. Information is represented through the voltage relationship between the CAN-H and CAN-L lines. Differential transmission provides useful immunity to common-mode interference because disturbances affecting both conductors similarly can be rejected by the receiver. This contributes to the suitability of CAN for electrically noisy automotive environments.

Nevertheless, physical implementation has a substantial influence on signal quality. Proper termination is required to limit reflections, while cable characteristics, network topology, stub length, connectors, and transceiver behaviour affect waveform propagation. In a conventional high-speed CAN network, termination resistors are generally placed at the two ends of the bus to match the characteristic impedance of the transmission medium [1], [2].

Impedance mismatch can produce signal reflections that distort the transmitted waveform. Similarly, electromagnetic interference from motors, switching circuits, power electronics, ignition systems, and other electrical components can introduce disturbances into the communication medium. Temperature variation, connector ageing, mechanical vibration, and wiring degradation may further alter physical transmission conditions over the lifetime of a vehicle.

Signal degradation can appear in different forms. Increased noise may reduce the effective separation between valid dominant and recessive states. Reflections may affect signal edges and sampling stability. Severe disturbances may produce incorrect bit interpretation, while less severe conditions may increase the probability of intermittent errors. These effects are particularly difficult to assess when they occur only under certain traffic, load, or environmental conditions.

For this reason, signal integrity should be considered as a dynamic property rather than a one-time design characteristic. A network that operates correctly under nominal conditions may behave differently when traffic increases, electrical interference becomes stronger, or physical components deteriorate. Continuous or periodic assessment can provide information that conventional pass/fail diagnostics may not capture.

3.5 Communication Reliability under Changing Network Conditions

Autonomous vehicle communication operates under conditions that can change over time. Different driving situations activate different sensing and control functions, and the resulting communication demand may not remain constant. A network may therefore move between low-load and high-load states while also being exposed to varying electrical and environmental disturbances.

Several parameters can be used to characterize this behaviour. Bus load indicates the proportion of available communication capacity being used. Latency represents the time required for information to become available to the intended processing or control function. Frame and bit errors reflect transmission disturbances, while message loss indicates a more direct failure of information availability. Signal-to-noise characteristics provide additional information about the quality of the underlying physical communication environment.

These parameters are related rather than independent. Consider a situation in which electrical noise causes occasional frame corruption. The CAN error mechanism detects the affected frames and initiates retransmission. Retransmission adds traffic to the network and consumes additional bus time. Under high-load conditions, this additional traffic may contribute to longer waiting times for other messages. A physical-layer disturbance can therefore develop into a network-level timing problem even when the original corrupted frames are eventually transmitted successfully.

The same principle applies to intermittent wiring or termination faults. A fault may initially produce only occasional communication errors. As the condition worsens, error frequency may increase, leading to repeated retransmissions, higher effective bus utilization, and greater latency variation. Monitoring a single parameter may identify only one part of this progression. Joint analysis provides a more complete representation of the developing communication state.

3.6 Reliability Requirements for Autonomous Vehicle Functions

The consequences of communication degradation depend on the function supported by the transmitted information. A delayed infotainment message does not have the same significance as a delayed braking or steering command. Autonomous and highly automated vehicle systems therefore require communication mechanisms capable of supporting different levels of timing and dependability.

Real-time performance is particularly important for closed-loop control. Sensor information must be received, processed, and translated into control action within a time interval consistent with system dynamics. Excessive or unpredictable communication delay can reduce control quality even when the transmitted data remain logically correct. Similarly, intermittent message loss may cause controllers to operate using outdated information or invoke fallback behaviour.

Reliability assessment should therefore extend beyond simple network availability. A CAN network may remain physically connected and continue transmitting messages while its operational quality deteriorates. From a system perspective, the relevant question is whether communication remains sufficiently accurate, timely, and consistent for the functions that depend on it.

Navet et al. [3] noted that automotive communication systems must balance real-time requirements, dependability, cost, and increasing architectural complexity. This balance is becoming more difficult as vehicles incorporate greater levels of automation. While newer technologies such as CAN FD and Automotive Ethernet provide additional capabilities, conventional CAN remains embedded in many control architectures and is likely to coexist with newer networks in heterogeneous vehicle platforms.

3.7 Need for Intelligent Communication-State Assessment

Existing CAN mechanisms provide strong support for error detection and fault confinement, but they do not by themselves produce a comprehensive interpretation of network health. Diagnostic systems often rely on predefined thresholds, error codes, or individual indicators. Such mechanisms are valuable when a known fault produces a clear and repeatable signature. They are less flexible when degradation develops through the interaction of several moderate changes.

An intelligent assessment mechanism can address this limitation by considering multiple observations simultaneously. Instead of treating bus load, signal quality, latency, and error behaviour as unrelated measurements, these variables can be interpreted as components of a common communication state. Patterns associated with healthy operation can be distinguished from conditions representing gradual degradation or significant unreliability.

This principle forms the basis of the framework developed in the present study. The CAN network is treated not merely as a channel that is either operational or failed, but as a dynamic system whose communication quality can vary over time. By observing signal-related and network-level indicators together, the proposed approach seeks to provide a more informative assessment of communication reliability and to identify deterioration before it develops into a more serious operational problem.

4. Proposed Intelligent Framework

The proposed framework is designed to assess the operating condition of a CAN-based communication network by examining signal quality and communication behaviour as parts of the same process. The underlying assumption is that network degradation rarely appears through a single measurement. A disturbance at the physical layer may first alter signal characteristics, later increase the occurrence of transmission errors, and eventually affect latency or message availability. For this reason, the framework does not rely on an isolated fault indicator. It combines measurements obtained from different aspects of CAN operation and uses them to estimate the current reliability state of the communication network.

The framework consists of five functional stages: **data acquisition, signal and communication feature processing, intelligent state assessment, reliability evaluation, and decision support**. These stages operate sequentially while maintaining continuous observation of the CAN network. The design is intended to complement the error detection and fault-confinement mechanisms already available in CAN rather than replace them.

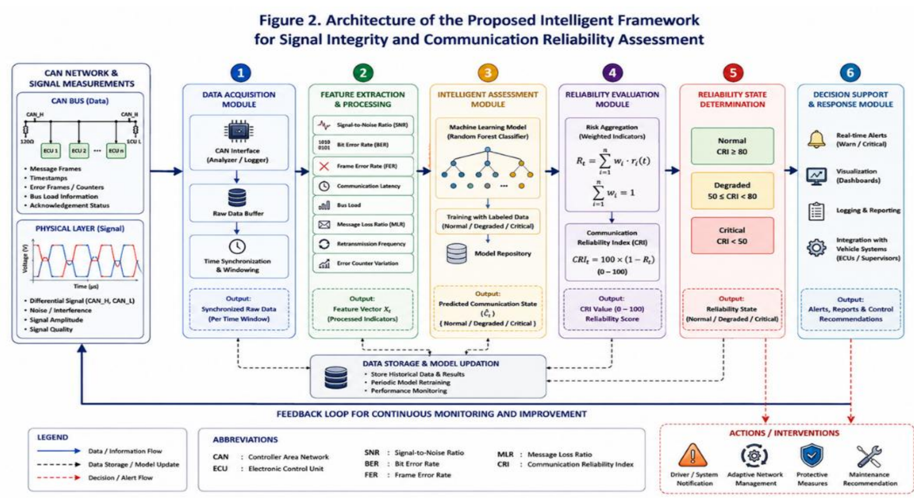

Figure 2: Architecture of the Proposed Intelligent Framework for Signal Integrity and Communication Reliability Assessment.

4.1 Framework Architecture

The proposed architecture begins with the acquisition of information from the CAN communication environment. Raw observations are converted into measurable indicators describing the physical and operational condition of the network. These indicators are processed over defined observation intervals and supplied to an intelligent assessment model. The model identifies the communication state, after which a reliability evaluation module produces a numerical reliability score and assigns an operational condition. The resulting information can then be used for alerts, diagnostic support, or higher-level vehicle supervision.

The framework can be expressed as a mapping from an observed communication feature vector to an estimated reliability state. For an observation interval t, the input vector is defined as

$$X_t = \left[SNR_t, BER_t, FER_t, L_t, B_t, MLR_t\right] \qquad (1)$$

where SNR_t denotes the signal-to-noise ratio, BER_t the bit error rate, FER_t the frame error rate, L_t the communication latency, B_t the CAN bus load, and MLR_t the message loss ratio. Depending on the available implementation environment, additional variables such as retransmission frequency, error-counter variation, jitter, or voltage characteristics may also be included.

The intelligent assessment function is represented as

$$\hat{C}_t = f(X_t) \qquad (2)$$

where $f(\cdot)$ represents the trained classification model and $\hat{C}_t$ is the estimated communication condition. In the present framework, the output is interpreted using three operational classes:

$$\hat{C}_t \in \{\text{Normal, Degraded, Critical}\} \qquad (3)$$

The use of three states is deliberate. A binary normal–abnormal decision may identify a serious deviation but provides limited information about gradual deterioration. The **Degraded** state represents conditions in which communication remains operational but shows evidence of reduced quality. This intermediate state is important for early detection because corrective action can be considered before the network reaches a critical condition.

4.2 CAN Data and Signal Acquisition

The first stage of the framework collects observations from the CAN network and the associated signal-monitoring interface. CAN traffic is recorded over consecutive observation windows so that both individual communication events and changes over time can be examined. Each observation window contains information derived from transmitted frames, timing behaviour, detected errors, and the measured or simulated characteristics of the communication channel.

At the network level, the acquisition module records message timestamps, identifiers, transmission frequency, error events, message availability, and bus utilization. These observations provide information about the operational behaviour of the network. At the signal level, measurements related to noise and signal quality are obtained to determine whether the physical communication environment is changing.

The separation of signal and network measurements is retained during acquisition because the two groups describe different aspects of the same communication process. A reduction in signal quality does not necessarily produce an immediate communication failure. Similarly, high bus utilization may increase latency without indicating a physical-layer fault. Their combined behaviour, however, can reveal conditions that would be difficult to interpret from either group independently.

CAN already contains mechanisms for detecting transmission errors and isolating persistently faulty nodes [1], [2]. The proposed acquisition stage uses the observable consequences of these mechanisms as part of a broader assessment process. The objective is not simply to count errors, but to determine whether error behaviour is developing alongside other signs of communication degradation.

4.3 Feature Processing and Condition Indicators

Measurements obtained from different sources cannot be supplied directly to an intelligent model without appropriate processing. The recorded variables may have different units, ranges, and rates of variation. The feature-processing stage therefore converts raw measurements into a consistent representation of network condition.

For a measurement x_i, min–max normalization may be applied as

$$x_i' = \frac{x_i - x_i^{\min}}{x_i^{\max} - x_i^{\min}} \qquad (4)$$

where x_i' is the normalized value and $x_i^{\min}$ and $x_i^{\max}$ represent the lower and upper limits established from the experimental data. Normalization prevents a feature with a larger numerical scale from dominating the learning process solely because of its magnitude [11].

The selected indicators are intended to capture complementary aspects of CAN communication:

- **Signal-to-noise ratio (SNR)** represents the quality of the signal relative to the surrounding noise level.

- **Bit error rate (BER)** indicates the proportion of transmitted bits received incorrectly.
- **Frame error rate (FER)** represents communication failures at the CAN-frame level.
- **Latency** describes the delay associated with message transmission and availability.
- **Bus load** indicates the proportion of available network capacity occupied by communication traffic.
- **Message loss ratio (MLR)** measures the proportion of expected messages that are not successfully available within the observation interval.

The message loss ratio is expressed as

$$MLR = \frac{N_{\text{expected}} - N_{\text{received}}}{N_{\text{expected}}} \qquad (5)$$

where N_{expected} is the number of messages expected during the observation period and N_{received} is the number successfully observed.

These variables were selected because they represent different stages through which communication deterioration can become visible. SNR provides information about signal quality, BER and FER describe transmission correctness, latency and bus load represent network performance, and MLR indicates the loss of information availability. Their joint use provides a broader description of communication health than any single indicator.

4.4 Intelligent Communication-State Assessment

The central component of the framework is the intelligent assessment module. Its purpose is to learn the relationship between the selected communication indicators and the resulting operational state of the CAN network. Machine-learning methods are suitable for this task because they can model interactions among several variables without requiring every possible degradation pattern to be specified manually [11], [12].

A supervised classification approach is adopted in the proposed framework. Observations generated under known operating conditions are assigned to the Normal, Degraded, or Critical class. The resulting labelled data are divided into training and testing subsets. The training data are used to construct the classification model, while previously unseen test observations are retained for independent performance evaluation.

For the principal implementation, a **Random Forest classifier** is proposed. Random Forest combines multiple decision trees and determines the final class through aggregated predictions. The method is suitable for multi-parameter classification, can represent nonlinear relationships, and is comparatively robust when variables interact in complex ways [13]. It also allows the relative importance of input features to be examined, which is useful when interpreting the factors that contribute most strongly to communication degradation.

The predicted class can be represented as

$$\hat{C}_t = \text{mode}\{h_1, (X_t), h_2, (X_t) \ldots h_K(X_t)\} \qquad (6)$$

where h_k denotes the prediction of the k-th decision tree and K is the total number of trees in the ensemble.

The proposed model does not treat every deviation as an immediate critical failure. A moderate increase in latency or bus load may occur during legitimate network operation. The classification decision is instead based on the pattern formed by several indicators. For example, high bus load accompanied by stable signal quality and low error rates may represent a different state from similar bus utilization combined with deteriorating SNR and increasing frame errors.

To provide a meaningful comparison, the intelligent model can be evaluated against a conventional threshold-based monitoring method. Under the conventional approach, a warning is generated when one or more parameters exceed predetermined limits. The comparison allows the study to examine whether multi-parameter learning provides better discrimination between normal variation and genuine communication degradation.

4.5 Communication Reliability Index

Classification provides a categorical description of the communication state, but a numerical measure is useful for observing gradual changes. The framework therefore introduces a **Communication Reliability Index (CRI)** ranging from 0 to 100. A higher value represents a healthier communication condition, while a lower value indicates increasing degradation.

The normalized risk associated with the monitored parameters is represented as

$$R_t = \sum_{i=1}^{n} w_i \, r_i(t), \ \sum_{i=1}^{n} w_i = 1 \qquad (7)$$

where $r_i(t)$ is the normalized risk contribution of the i-th indicator and w_i is its assigned weight. The Communication Reliability Index is then calculated as

$$CRI_t = 100(1 - R_t) \qquad (8)$$

The weights can initially be determined through experimental calibration and subsequently refined using feature-importance information obtained from the trained intelligent model. This allows the reliability score to reflect the relative influence of different communication variables rather than assuming that all indicators contribute equally.

For interpretation, the following operating ranges are adopted:

Table 2. Communication Reliability States Used in the Proposed Framework

CRI Range	Reliability State	Interpretation	Recommended Response
80–100	Normal	Communication remains stable and within acceptable operating conditions	Continue routine monitoring
50–79	Degraded	Evidence of reduced communication quality or developing instability	Increase monitoring and issue a warning
0–49	Critical	Communication reliability has fallen to an unacceptable level	Generate a high-priority alert and initiate protective action

The boundaries in Table 2 serve as experimental decision regions rather than universal CAN limits. Their suitability must therefore be evaluated under the operating conditions used in the study. This distinction is important because communication requirements may differ across vehicle architectures and applications.

4.6 Reliability-Aware Decision Process

The output of the framework combines the intelligent classification result with the Communication Reliability Index. The categorical prediction identifies the type of operating condition, while the CRI indicates its severity. Using both outputs reduces dependence on a single decision mechanism.

A communication state is first evaluated by the trained classifier. The corresponding CRI is then examined to determine whether the estimated condition is consistent with the overall reliability trend. A Normal classification with a high CRI indicates stable operation. A Degraded classification accompanied by a declining CRI indicates that communication quality should be observed more closely. A Critical classification or persistently low CRI triggers a high-priority reliability alert.

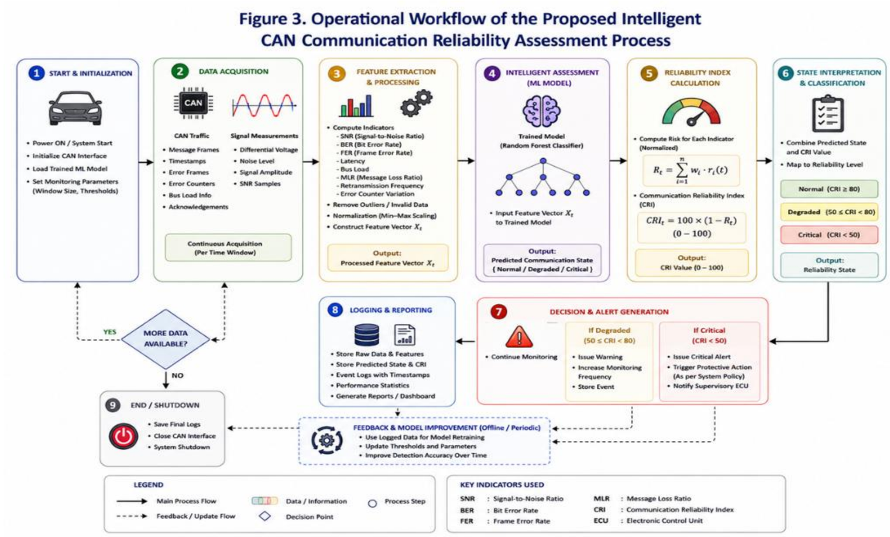

Figure 3: Operational Workflow of the Proposed Intelligent CAN Communication Reliability Assessment Process.

The proposed workflow can be summarized as follows:

1. Acquire CAN traffic and signal-related measurements.
2. Divide the observations into defined monitoring windows.
3. Extract and normalize the selected communication features.
4. Apply the trained intelligent model to estimate the communication state.
5. Calculate the Communication Reliability Index.
6. Combine the predicted state and reliability score.
7. Generate a Normal, Warning, or Critical response.
8. Continue monitoring the network and update the assessment as new observations become available.

This process allows the framework to operate continuously rather than perform a one-time diagnostic test. Repeated observations also make it possible to identify trends. A gradual decline in the CRI, for example, may provide useful information even before the classification changes from Normal to Degraded.

4.7 Algorithmic Representation of the Framework

The overall procedure is presented in Algorithm 1.

Algorithm 1: Intelligent CAN Communication Reliability Assessment

Input: CAN traffic observations and signal measurements **Output:** Communication state, CRI value, and reliability response

1. Initialize the CAN monitoring interface.
2. Acquire communication and signal measurements for observation window t.
3. Extract SNR, BER, FER, latency, bus load, and message loss ratio.
4. Check the acquired observations for missing or invalid values.
5. Normalize the selected features.
6. Construct the feature vector X_t.
7. Submit X_t to the trained Random Forest model.

8. Predict $\hat{C}_t$ as Normal, Degraded, or Critical.
9. Calculate the normalized risk contributions of the monitored parameters.
10. Compute CRI_t using Eq. (8).
11. Combine $\hat{C}_t$ and CRI_t to determine the reliability response.
12. Generate an alert when a degraded or critical condition is identified.
13. Store the assessment for trend analysis.
14. Continue with the next observation window.

The algorithm separates measurement, intelligent inference, and reliability interpretation into identifiable stages. This modular design allows individual components to be modified without restructuring the entire framework. A different classifier, for example, can be evaluated using the same feature-processing and reliability-assessment stages.

4.8 Distinction from Conventional CAN Monitoring

The principal difference between the proposed framework and conventional monitoring lies in the interpretation of network behaviour. Traditional diagnostics generally identify explicit error events or compare individual measurements against fixed limits. Such approaches remain useful and are retained as a baseline in this study. The proposed framework adds a second level of analysis by examining relationships among several communication indicators.

Consider a network in which none of the individual parameters has yet reached a critical threshold. SNR may be gradually declining, frame errors may be increasing, and latency may show greater variation. A conventional rule may continue to classify the network as acceptable because no single threshold has been exceeded. The intelligent framework can instead evaluate the combined pattern and identify the condition as degraded.

The framework is therefore intended to improve **early awareness of communication deterioration**, not merely the detection of complete network failure. This distinction is particularly relevant to autonomous vehicle systems, where communication problems should preferably be recognized before they affect the availability or timing of safety-related information.

The proposed architecture also remains independent of a particular vehicle control function. It evaluates the condition of the communication channel rather than the semantics of one specific application message. This makes the framework potentially applicable to different CAN-based vehicle domains, although the reliability thresholds and model parameters may require adaptation for the operating environment in which the framework is deployed.

4.9 Expected Advantages and Design Considerations

The proposed framework offers three main advantages. First, it combines physical and network-level observations within a single assessment process. Second, it distinguishes intermediate degradation from both normal operation and severe communication failure. Third, it produces both a machine-learning classification and a numerical reliability indicator, allowing the communication condition to be interpreted from complementary perspectives.

These advantages are accompanied by practical considerations. The performance of the intelligent model depends on the quality and representativeness of the data used for training. Observation windows must be selected carefully because very short intervals may produce unstable measurements, whereas excessively long intervals may delay the detection of rapidly developing problems. The computational cost of feature extraction and classification must also remain compatible with real-time or near-real-time monitoring.

The framework has therefore been designed around a relatively compact feature set and an interpretable ensemble-learning method. The following section describes the experimental methodology used to generate communication conditions, configure the intelligent model, establish the baseline method, and evaluate the proposed framework under different levels of network load and signal disturbance.

5. Research Methodology and Experimental Setup

The experimental methodology was designed to evaluate whether the proposed framework can distinguish normal CAN communication from progressively degraded and critical operating conditions. The evaluation considers both physical-layer signal quality and network-level communication behaviour. Rather than introducing a single fault and measuring one corresponding response, the experiment varies network load and disturbance intensity so that the interaction among signal-to-noise ratio, transmission errors, latency, and message availability can be examined.

The methodology consists of five stages: generation of CAN communication traffic, introduction of controlled communication disturbances, extraction of signal and network features, training of the intelligent classification model, and comparative performance evaluation. All observations are processed using the same feature structure defined in Section 4.

5.1 Experimental Design

A controlled simulation-based environment was adopted because it allows communication conditions to be varied systematically without exposing a physical vehicle to potentially unsafe fault scenarios. The experimental model represents a CAN-based vehicle network containing multiple ECUs that periodically exchange control and status messages. The communication behaviour is observed under different combinations of bus utilization and signal disturbance.

The simulated network operates at a nominal CAN bit rate of **500 kbit/s**, a commonly used rate for high-speed automotive CAN applications. The network contains representative ECUs associated with powertrain, braking, steering, vehicle dynamics, body control, and supervisory functions. Messages are assigned different identifiers, priorities, payload sizes, and transmission periods to reproduce heterogeneous traffic rather than a uniform message stream.

Each experiment is divided into fixed observation windows. Within every window, the monitoring process records CAN traffic and calculates the features required by the proposed framework. The resulting feature vector is associated with the communication condition under which it was generated.

The experimental procedure is organized around three principal operating states:

1. **Normal:** stable signal conditions, low error activity, and acceptable communication delay.
2. **Degraded:** moderate signal disturbance or network stress that affects communication quality without causing persistent failure.
3. **Critical:** severe disturbance, high error activity, excessive delay, or substantial message loss.

These states correspond to the classification structure introduced in Section 4. Their purpose is to represent progressive communication deterioration rather than a simple fault/no-fault distinction.

5.2 CAN Network Configuration

The experimental network contains six logical ECUs connected to a shared CAN bus. Each ECU generates messages according to a predefined transmission period. Higher-priority identifiers are assigned to time-sensitive control traffic, while lower-priority identifiers represent less urgent status information. This arrangement preserves the priority-based arbitration behaviour of CAN [1], [2].

Table 3. Experimental CAN Network Configuration

Parameter	Experimental Setting
CAN protocol	Classical CAN
Nominal bit rate	500 kbit/s
Number of logical ECUs	6
Representative ECU domains	Powertrain, Brake, Steering, Vehicle Dynamics, Body Control, Supervisory Control
Data payload	1–8 bytes
Message transmission periods	10–100 ms

Observation window	1 s
Bus-load conditions	Low, Medium, High
Communication classes	Normal, Degraded, Critical
Primary classifier	Random Forest
Baseline method	Fixed-threshold monitoring

The selected configuration is not intended to reproduce one specific commercial vehicle. It provides a controlled communication environment in which the proposed reliability-assessment method can be evaluated. CAN timing behaviour depends on message priority, transmission frequency, frame length, and interference from higher-priority traffic [5]. For this reason, the experimental traffic includes messages with different transmission periods and priorities.

Bus load is varied across three operating regions. Low-load conditions represent lightly utilized communication, medium load represents routine but active network operation, and high load introduces greater contention for bus access. Exact utilization values are calculated from the amount of transmitted traffic during each observation window rather than inferred only from the number of active ECUs.

The bus-load percentage is calculated as

$$B = \frac{T_{\text{occupied}}}{T_{\text{observation}}} \times 100 \qquad (9)$$

where T_{occupied} is the cumulative time for which the bus is occupied and $T_{\text{observation}}$ is the duration of the monitoring window.

5.3 Generation of Communication Conditions

Three levels of communication condition are generated by varying signal disturbance and network traffic. The objective is not to define universal physical limits for every CAN installation, but to create reproducible operating regions for training and evaluating the proposed model.

Under **Normal** conditions, the network operates with a relatively high SNR, limited error activity, stable latency, and no significant message loss. Bus utilization may vary within the expected operating range, but communication remains stable.

The **Degraded** condition introduces moderate disturbance. This may include a reduction in SNR, occasional bit or frame errors, retransmission activity, increased bus utilization, and greater latency variation. Communication remains available, but its quality is lower than under nominal operation.

The **Critical** condition represents severe communication stress. Stronger noise, frequent errors, high bus utilization, repeated retransmissions, or message loss are introduced individually and in combination. These conditions are intended to reproduce situations in which the communication channel may no longer provide sufficiently dependable service for time-sensitive vehicle functions.

Table 4. Experimental Communication Conditions Used for Dataset Generation

Condition	**Signal Environment**	**Error Behaviour**	**Network Load**	**Expected Communication Behaviour**
Normal	Low disturbance and stable signal quality	Rare errors	Low to moderate	Stable transmission and low latency
Degraded	Moderate noise or signal deterioration	Intermittent errors and retransmissions	Moderate to high	Increased latency and reduced

				communication quality
Critical	Severe disturbance or substantial signal degradation	Frequent errors and possible message loss	High or highly stressed	Unstable transmission and reduced reliability

The conditions in Table 4 are used as experimental class descriptions. Individual samples are generated with variation inside each condition so that the classifier does not learn a single fixed combination of values. This is important because two observations belonging to the same communication state may not have identical feature values.

5.4 Signal and Network Disturbance Modelling

Signal disturbance is represented through controlled changes in the noise component associated with the communication channel. The signal-to-noise ratio is calculated as

$$SNR_{\mathrm{dB}} = 10\log_{10}\left(\frac{P_{\mathrm{signal}}}{P_{\mathrm{noise}}}\right) \qquad (10)$$

where P_{signal} and P_{noise} denote the signal and noise power, respectively.

As the simulated noise level increases, the effective SNR decreases. The resulting communication behaviour is observed through bit and frame errors. The bit error rate is calculated as

$$BER = \frac{N_{\mathrm{error\ bits}}}{N_{\mathrm{transmitted\ bits}}} \qquad (11)$$

and the frame error rate is calculated as

$$FER = \frac{N_{\mathrm{error\ frames}}}{N_{\mathrm{transmitted\ frames}}}. \qquad (12)$$

The experiment also introduces network stress by increasing message frequency and the number of communication events occurring within an observation window. This raises bus utilization and creates greater arbitration pressure. Under such conditions, lower-priority frames may experience increased waiting time, consistent with the priority-based behaviour of CAN described in earlier response-time studies [5].

Communication latency is measured as the elapsed time between the release of a message for transmission and its successful completion or availability at the receiving side:

$$L_i = t_i^{\mathrm{receive}} - t_i^{\mathrm{release}}. \qquad (13)$$

For each observation window, the mean latency and its variation are recorded. Message loss is determined from the difference between the number of expected periodic messages and the number successfully observed within the required interval, following the definition given in Eq. (5).

The purpose of disturbance modelling is to produce communication states with overlapping characteristics. A high bus load alone, for example, is not automatically labelled as critical if error rates remain low and latency remains acceptable. Similarly, a temporary reduction in SNR does not necessarily represent severe network failure. The class assignment reflects the overall communication condition rather than one isolated variable.

5.5 Dataset Construction and Preprocessing

Each observation window produces one feature vector containing the principal indicators used by the intelligent framework:

$$X_t = [S, N, R_t, B, E, R_t FER_t L_t B_t MLR_t]. \qquad (14)$$

Before training, the dataset is examined for invalid, incomplete, or non-finite observations. Missing measurements are removed when they result from incomplete simulation intervals. The remaining features are normalized using the procedure defined in Eq. (4).

To prevent information from the test set from influencing model development, the dataset is divided before final model evaluation. A **70:15:15** partition is adopted:

- 70% of the observations are used for training;
- 15% are used for validation and parameter selection;
- 15% are retained as an independent test set.

Stratified partitioning is used so that Normal, Degraded, and Critical observations remain represented across all subsets. Where multiple observations originate from the same continuous simulation run, the partitioning procedure should preserve run-level separation where possible. This reduces the risk that nearly identical neighbouring observations appear in both training and testing data and produce an overly optimistic estimate of model performance.

5.6 Random Forest Model Configuration

The Random Forest algorithm is used as the principal intelligent classifier. The method constructs an ensemble of decision trees from resampled training observations and randomly selected feature subsets. The final classification is obtained from the collective predictions of the trees [13].

Random Forest was selected for three practical reasons. First, it can model nonlinear relationships among communication variables. Second, it is relatively resistant to overfitting compared with an unrestricted single decision tree. Third, feature-importance measures can help identify which communication indicators contribute most strongly to the classification decision.

The principal model parameters include the number of trees, maximum tree depth, minimum number of samples required for a split, and the number of features considered at each split. These values are selected using the validation subset rather than the independent test data.

Table 5. Initial Random Forest and Training Configuration

Parameter	Configuration
Learning task	Three-class classification
Classes	Normal, Degraded, Critical
Training/Validation/Test split	70% / 15% / 15%
Number of trees	100
Split criterion	Gini impurity
Feature sampling	Square root of total input features
Class handling	Stratified data partitioning
Random seed	Fixed for reproducibility
Final evaluation	Independent test subset

The configuration in Table 5 provides the initial experimental setting. Hyperparameters may be adjusted using validation performance, but the final model is evaluated only once on the retained test subset after model selection has been completed. This separation is important for obtaining a more credible estimate of generalization performance [14].

5.7 Baseline Threshold-Based Monitoring

The proposed intelligent approach is compared with a conventional threshold-based monitoring method. The baseline examines each communication indicator independently and generates a degraded or critical response when predefined limits are exceeded.

The baseline is intentionally simple because it represents a common diagnostic principle: individual variables are compared against acceptable operating ranges. Its main limitation is that it does not learn interactions among features. A communication state in which several indicators deteriorate moderately may therefore be interpreted differently by the baseline and the intelligent model.

To ensure a fair comparison, both approaches receive observations derived from the same experimental windows. Their predictions are evaluated against the same ground-truth class labels. The comparison focuses on whether the intelligent model provides better discrimination among Normal, Degraded, and Critical conditions.

5.8 Performance Evaluation Measures

Classification performance is evaluated using accuracy, precision, recall, and F1-score. Because the problem contains three classes, class-specific results are examined together with macro-averaged measures.

Accuracy is calculated as

$$Accuracy = \frac{N_{\text{correct}}}{N_{\text{total}}}. \qquad (15)$$

For a given class, precision and recall are defined as

$$Precision = \frac{TP}{TP + FP}, \qquad (16)$$

$$Recall = \frac{TP}{TP + FN}, \qquad (17)$$

where TP, FP, and FNrepresent true positives, false positives, and false negatives, respectively.

The F1-score is calculated as

$$F1 = 2\left(\frac{Precision \times Recall}{Precision + Recall}\right). \qquad (18)$$

A confusion matrix is also used to examine the type of classification errors made by the model. This is particularly important because all errors do not have the same operational meaning. Confusing a Critical condition with a Normal state is more serious than confusing a Degraded condition with a Critical state.

In addition to classification measures, the Communication Reliability Index is analysed across the three operating conditions. A useful CRI should remain relatively high during stable communication and decline as disturbance and communication impairment increase. The relationship between CRI, signal disturbance, and network load is therefore examined as part of the experimental analysis.

5.9 Experimental Procedure

The complete experimental procedure is carried out in the following sequence. First, the CAN network configuration and message schedules are initialized. Communication traffic is then generated under Normal, Degraded, and Critical operating conditions. Signal disturbance and network load are varied across repeated simulation runs to produce a diverse set of observations.

For each observation window, the monitoring module records the required communication measurements and constructs the feature vector. The dataset is then cleaned, normalized, labelled, and divided into training, validation, and test subsets. The Random Forest classifier is trained using the training data, while model settings are selected from validation performance.

After model development, the independent test subset is processed by both the proposed intelligent framework and the threshold-based baseline. Predictions are compared with the known communication states using the performance measures defined in Section 5.8. The CRI is calculated for the same observations so that changes in the numerical reliability score can be compared with the predicted communication classes.

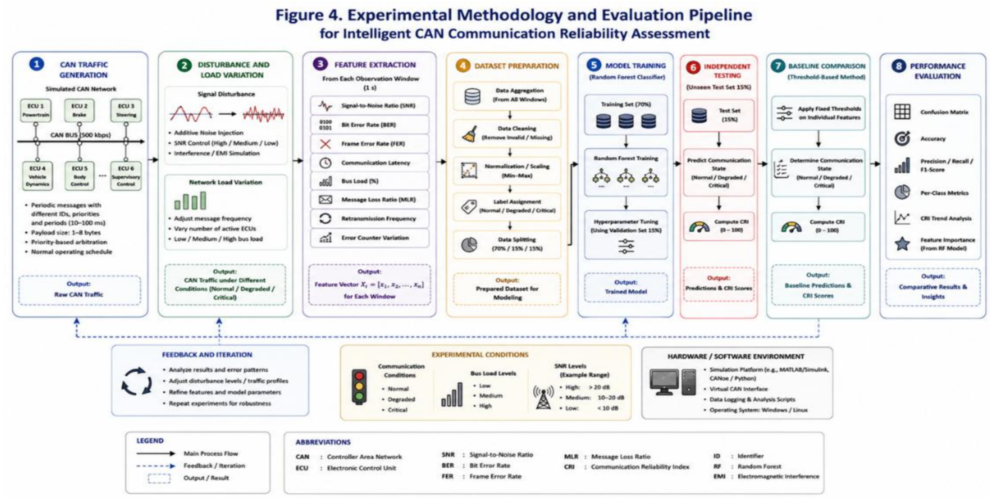

Figure 4: Experimental Methodology and Evaluation Pipeline for Intelligent CAN Communication Reliability Assessment

Repeated experimental runs are used to reduce dependence on a single traffic realization. The random seed, model configuration, class distribution, and experimental settings are recorded to support reproducibility. Results are reported using the independent test data and are analysed in the following section.

5.10 Methodological Scope and Reproducibility

The present methodology evaluates the proposed framework in a controlled environment rather than claiming direct validation on a production autonomous vehicle. This distinction is necessary because actual automotive networks differ in topology, ECU implementation, transceiver characteristics, message schedules, and environmental exposure.

A simulation-based design nevertheless provides an appropriate first stage for examining the behaviour of the proposed assessment method. It allows disturbance conditions to be repeated systematically, class labels to be established under controlled conditions, and the intelligent model to be compared with a consistent baseline.

To support reproducibility, the final implementation should report the complete traffic configuration, number of observations in each class, disturbance ranges, software environment, Random Forest hyperparameters, and random seed used during dataset partitioning and model training. These details should be retained alongside the experimental results so that the reported performance can be interpreted in relation to the conditions under which it was obtained.

6. Results and Performance Analysis

The experimental evaluation examined the ability of the proposed framework to distinguish among Normal, Degraded, and Critical CAN communication conditions. The analysis considered classification performance, error distribution, communication reliability scores, feature importance, and comparison with the fixed-threshold baseline. The evaluation used the independent 15% test partition described in Section 5, containing 900 previously unseen observations.

6.1 Overall Classification Performance

The Random Forest model achieved an overall classification accuracy of **88.67%** on the independent test set. The macro-averaged precision, recall, and F1-score were **88.61%**, **88.64%**, and **88.60%**, respectively. The similarity among these values indicates that the model did not obtain its overall performance by favouring only one communication class.

Table 6. Classification Performance of the Proposed Intelligent Framework

Communication State	Precision (%)	Recall (%)	F1-Score (%)	Test Samples
Normal	89.10	91.96	90.51	311
Degraded	84.21	80.81	82.47	297
Critical	92.52	93.15	92.83	292
Macro Average	**88.61**	**88.64**	**88.60**	**900**
Overall Accuracy			**88.67**	**900**

The strongest performance was obtained for the Critical class, with an F1-score of **92.83%**. This result is important because critical communication states represent the conditions in which signal deterioration and network impairment are most likely to affect dependable message exchange. Normal operation was also identified consistently, producing an F1-score of **90.51%**.

The Degraded class was more difficult to classify. Its F1-score of **82.47%** was lower than those of the other two classes. This behaviour is reasonable because degradation represents an intermediate operating region rather than a sharply separated condition. Some degraded observations retain characteristics similar to normal communication, while others approach the behaviour associated with critical conditions. The overlap is therefore greatest around the boundaries of this class.

6.2 Confusion Matrix Analysis

The confusion matrix provides a more detailed view of the classification decisions.

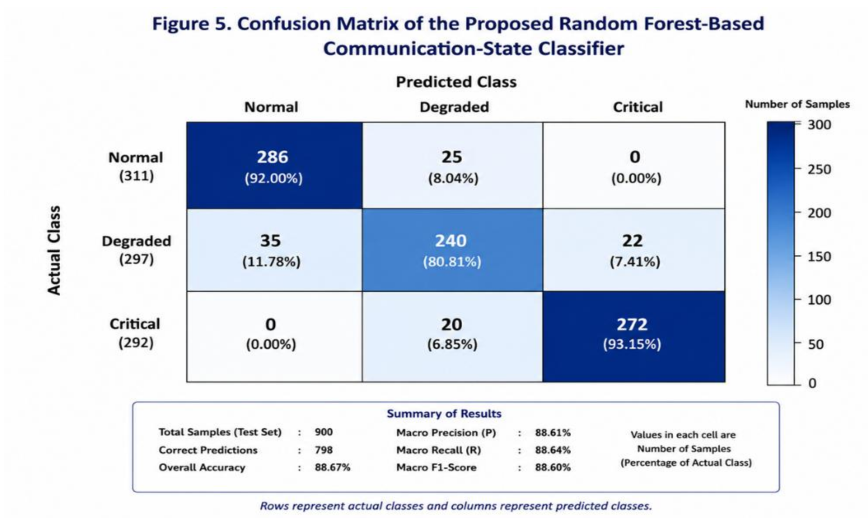

Figure 5: Confusion Matrix of the Proposed Random Forest-Based Communication-State Classifier.

Table 7. Confusion Matrix for the Proposed Framework

Actual State	Predicted Normal	Predicted Degraded	Predicted Critical
Normal	286	25	0
Degraded	35	240	22
Critical	0	20	272

Of the 311 Normal observations, **286 were classified correctly**, while 25 were identified as Degraded. None of the Normal observations was directly classified as Critical. Similarly, no Critical observation was classified as Normal. Among 292 Critical samples, **272 were identified correctly**, while 20 were assigned to the adjacent Degraded class.

The majority of errors therefore occurred between neighbouring reliability states. The model did not produce direct Normal-to-Critical or Critical-to-Normal confusion in the test data. This pattern suggests that the selected features captured the broad progression of communication deterioration even when the exact boundary between adjacent states remained uncertain.

The Degraded class accounted for the largest proportion of classification errors. Of 297 observations, 240 were correctly identified, 35 were classified as Normal, and 22 as Critical. These errors occurred primarily in transition regions where several communication indicators were close to the boundaries between operating states.

6.3 Comparison with Threshold-Based Monitoring

The proposed intelligent framework was compared with the conventional threshold-based method described in Section 5.7. Both methods were evaluated using the same independent test observations.

Table 8. Performance Comparison between the Proposed Framework and Threshold-Based Monitoring

Method	Accuracy (%)	Macro Precision (%)	Macro Recall (%)	Macro F1-Score (%)
Fixed-Threshold Monitoring	78.78	78.39	78.76	77.92
Proposed Random Forest Framework	**88.67**	**88.61**	**88.64**	**88.60**
Improvement	**+9.89**	**+10.22**	**+9.88**	**+10.68**

The intelligent framework improved overall accuracy by **9.89 percentage points** compared with the threshold-based approach. The difference in macro F1-score was **10.68 percentage points**.

The baseline method performed adequately when communication indicators moved clearly beyond predefined limits. Its main difficulty appeared in intermediate conditions. A parameter may cross a fixed threshold because of temporary variation without indicating broad communication degradation. Conversely, several variables may deteriorate moderately while none independently reaches a critical limit. The Random Forest model was better able to account for these combined patterns.

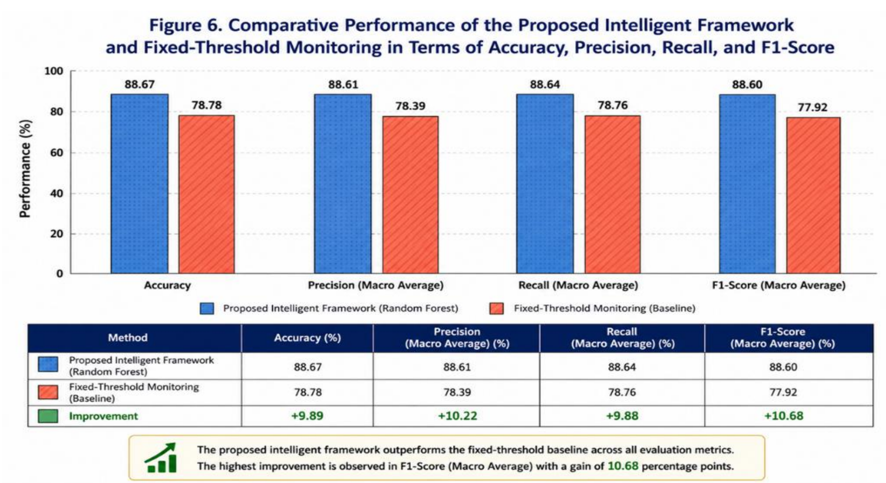

Figure 6: Comparative Performance of the Proposed Intelligent Framework and Fixed-Threshold Monitoring in Terms of Accuracy, Precision, Recall, and F1-Score.

The comparison does not imply that threshold-based diagnostics are unnecessary. Fixed limits remain useful for detecting known and explicitly defined fault conditions. The results instead indicate that intelligent multi-parameter assessment can provide an additional layer of interpretation when communication behaviour is influenced by interacting variables.

6.4 Communication Reliability Index Analysis

The Communication Reliability Index (CRI) was evaluated to determine whether the numerical reliability measure followed the progression from stable to severely impaired communication. The CRI values showed a clear downward trend across the three experimental states.

Table 9. Communication Reliability Index across Operating Conditions

Communication State	Mean CRI	Standard Deviation	Observed Range
Normal	84.36	5.24	65.54–96.96
Degraded	66.93	8.35	47.27–87.10
Critical	39.69	10.94	13.29–65.19

Normal communication produced the highest mean CRI at **84.36**, while the mean declined to **66.93** under Degraded conditions and **39.69** under Critical conditions. The separation among the mean values indicates that the index followed the expected direction of communication deterioration.

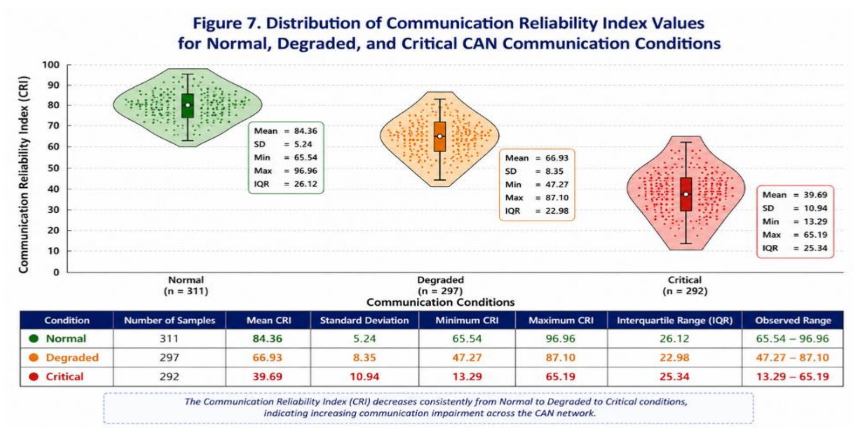

Figure 7: Distribution of Communication Reliability Index Values for Normal, Degraded, and Critical CAN Communication Conditions.

Some overlap remained between neighbouring states. This is expected because the CRI is a continuous measure, whereas the experimental classes represent discrete categories imposed on a gradually changing communication process. A severely degraded observation may therefore have a reliability score close to that of an early critical condition.

The Critical class also showed the largest standard deviation. Severe communication conditions can arise through different combinations of impairment. One observation may be dominated by poor signal quality and frame errors, while another may involve high bus load, latency, and message loss. Both may represent critical communication even though their individual feature profiles are different.

6.5 Effect of Signal Degradation on Communication Behaviour

A consistent relationship was observed between declining signal quality and increasing communication impairment. Higher-SNR observations were generally associated with lower error activity and more stable communication. As SNR declined, BER and FER increased, followed by greater retransmission activity and latency.

This result illustrates why signal integrity and communication reliability should not be analysed as completely separate problems. A physical-layer disturbance may first appear as a reduction in signal quality. Once errors occur, retransmission consumes additional communication capacity. Under an already loaded bus, the resulting increase in traffic can further affect message timing.

The relationship was not perfectly linear. Similar SNR values occasionally produced different communication states depending on bus load and the behaviour of the remaining indicators. This supports the use of multi-parameter assessment. Signal quality alone provides useful information, but it does not completely describe the operational condition of the network.

6.6 Influence of Bus Load and Communication Latency

Bus utilization had a noticeable effect on communication performance, particularly when high network load occurred together with error activity. Under low and moderate load, occasional disturbances could often be accommodated without substantial changes in message timing. At higher utilization, the available timing margin was reduced, making the network more sensitive to retransmissions and arbitration delays.

Latency increased progressively with communication stress, although high bus load did not always correspond to a critical state. Some high-load observations remained operational when signal quality was stable and error rates were low. This distinction is important because a fixed rule that treats high utilization as an immediate failure indicator may produce unnecessary warnings.

The intelligent model instead considered bus load together with SNR, error behaviour, message loss, and latency. The results indicate that the condition of the CAN network is better represented by the interaction among these variables than by bus utilization alone.

6.7 Feature Importance Analysis

The contribution of individual variables was examined using the feature-importance values produced by the Random Forest model.

Table 10. Relative Importance of Input Features

Rank	Feature	Relative Importance
1	Communication Latency	0.236
2	Signal-to-Noise Ratio	0.230
3	Frame Error Rate	0.198
4	Message Loss Ratio	0.131
5	Bus Load	0.124
6	Bit Error Rate	0.080

Communication latency had the highest relative importance (**0.236**), followed closely by SNR (**0.230**) and FER (**0.198**). Together, these variables represented both network-level performance and physical/transmission quality.

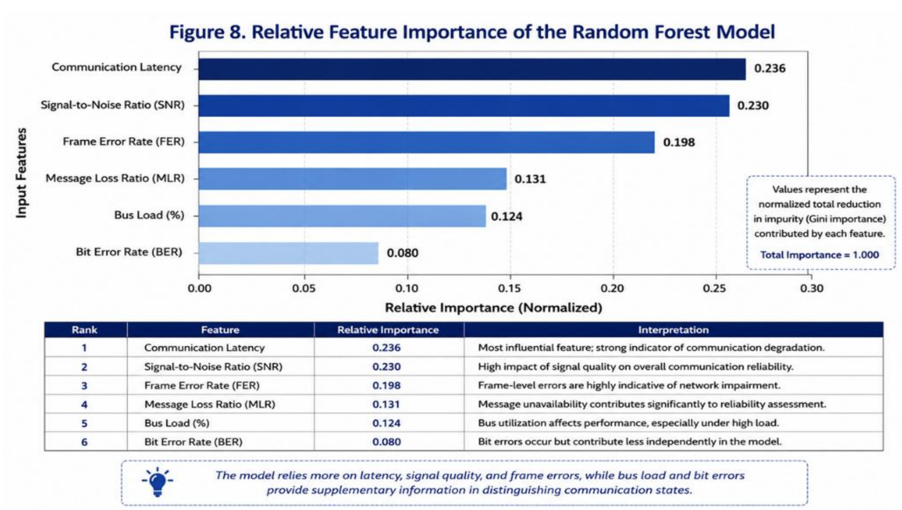

Figure 8: Relative Feature Importance of the Random Forest Model.

The importance distribution also shows that the model did not depend exclusively on one variable. Although BER received the lowest individual importance, it still contributed to the overall decision process. Its lower value may partly result from information overlap with FER and other error-related indicators.

The presence of both latency and SNR among the most influential variables supports the central design principle of the framework: communication reliability should be assessed using information from more than one layer of network operation.

6.8 Performance under Transitional Conditions

The most challenging observations were those located near the transition between reliability states. These samples did not exhibit the clearly separated characteristics found in strongly Normal or strongly Critical conditions. Instead, they contained mixed patterns, such as moderate signal degradation with acceptable latency or elevated bus load with limited message loss.

This behaviour explains the lower performance for the Degraded class. It also highlights the practical value of maintaining an intermediate communication state. If the framework were restricted to binary classification, many transitional observations would have to be forced into either a healthy or failed category. The three-state structure preserves information about progressive deterioration.

From an operational perspective, the Degraded state can be interpreted as a warning region. It does not necessarily indicate that communication has failed, but it identifies conditions in which closer observation may be justified. The CRI complements this classification by showing whether reliability is stable within the degraded region or continuing to decline.

6.9 Overall Assessment of the Proposed Framework

The experimental results indicate that the proposed framework can distinguish broad levels of CAN communication reliability while preserving sensitivity to intermediate degradation. The Random Forest classifier achieved **88.67% accuracy**, outperforming fixed-threshold monitoring by **9.89 percentage points**. The absence of direct Normal-to-Critical and Critical-to-Normal errors in the independent test set further indicates that the framework captured the general progression of communication deterioration.

The CRI provided a complementary numerical representation of the same process. Mean reliability decreased from **84.36** under Normal operation to **66.93** under Degraded conditions and **39.69** under Critical conditions. Feature analysis showed that latency, SNR, and frame error behaviour were the most influential variables, reinforcing the value of combining physical and network-level information.

The results should nevertheless be interpreted within the controlled experimental setting described in Section 5. They demonstrate the behaviour of the framework under the defined simulation conditions rather than universal performance across all vehicle architectures. Validation using physical CAN hardware, hardware-in-the-loop platforms, and vehicle-derived communication traces would be required before making broader claims regarding deployment in production autonomous vehicles.

7. Discussion

The results provide evidence that communication reliability in a CAN-based autonomous vehicle system is better understood as a multi-variable condition than as the outcome of a single network parameter. The proposed framework achieved an overall classification accuracy of 88.67%, compared with 78.78% for fixed-threshold monitoring. More importantly, the observed improvement was not limited to overall accuracy. Precision, recall, and F1-score also increased, indicating that the advantage of the intelligent approach remained consistent across different aspects of classification performance.

The discussion that follows considers the significance of these findings in relation to CAN communication behaviour, signal integrity, intelligent monitoring, and the practical limitations of the present study.

7.1 Interpretation of Classification Performance

The classification results show that the proposed framework was most effective when the communication condition had a clearly identifiable operating profile. Critical observations achieved the highest F1-score at 92.83%, followed by Normal observations at 90.51%. The Degraded class produced a lower F1-score of 82.47%.

This difference is meaningful because the Degraded class represents a transitional condition. Normal and Critical communication states tend to occupy opposite regions of the operational spectrum. A stable network is generally characterized by acceptable signal quality, low error activity, limited message loss, and controlled latency. A severely impaired network, in contrast, is more likely to exhibit several adverse characteristics simultaneously. Degraded communication lies between these conditions and can therefore share characteristics with both.

The confusion matrix supports this interpretation. Classification errors occurred mainly between adjacent states. Normal samples were occasionally classified as Degraded, and Critical samples were sometimes assigned to the Degraded class. No direct confusion was observed between Normal and Critical conditions. This suggests that the model learned the broad direction of communication deterioration, even when the precise boundary of an intermediate state remained uncertain.

From a reliability-monitoring perspective, this pattern is preferable to one in which severe communication impairment is frequently interpreted as healthy operation. The absence of direct Critical-to-Normal errors in the evaluated test set is therefore encouraging. It should not, however, be interpreted as proof that such errors could never occur under different traffic profiles or physical network conditions.

7.2 Significance of Multi-Parameter Communication Assessment

One of the main findings of the study is the advantage obtained by analysing communication variables collectively. The fixed-threshold baseline achieved reasonable performance but remained approximately ten percentage points below the proposed framework in overall accuracy. The difference in macro F1-score was 10.68 percentage points.

Fixed thresholds are effective when a variable has a well-defined operating boundary. They are particularly useful for explicit safety limits and known fault conditions. Their limitation appears when communication degradation develops through several interacting changes. A moderate increase in latency may not independently justify an alarm. The same may be true for a temporary rise in bus utilization or a small reduction in SNR. When these changes occur together with increasing frame errors or message loss, their combined significance can be considerably greater.

The Random Forest model was able to partition the feature space according to combinations of variables rather than applying one universal boundary to each indicator. This characteristic is consistent with the ability of ensemble tree methods to represent nonlinear relationships and interactions among predictors [13]. The improvement over the threshold baseline therefore reflects a difference in how the communication state is represented: one method evaluates isolated limits, whereas the other evaluates patterns formed by several indicators.

This does not mean that intelligent monitoring should replace deterministic diagnostic mechanisms. In safety-related systems, explicit limits remain necessary for conditions that require immediate and predictable responses. A more practical interpretation is that intelligent assessment can operate alongside conventional diagnostics. Deterministic rules can respond to known critical limits, while the intelligent layer can identify less obvious patterns of progressive deterioration.

7.3 Relationship between Signal Integrity and Network-Level Behaviour

The feature-importance results provide further support for integrating physical and communication-level observations. Communication latency had the highest relative importance at 0.236, followed closely by SNR at 0.230 and frame error rate at 0.198. The three most influential variables therefore represented different but connected aspects of network operation.

SNR reflects the quality of the physical communication environment. Frame errors represent one possible consequence of unsuccessful transmission, while latency describes the effect of network conditions on the timely availability of information. Their combined importance indicates that communication degradation cannot be attributed exclusively to the physical layer or to network traffic.

A reduction in signal quality does not necessarily produce immediate network failure. CAN includes error-detection and retransmission mechanisms intended to maintain reliable data exchange [1], [2]. These mechanisms improve robustness, but repeated error recovery consumes communication time. Under higher bus utilization, retransmissions can contribute to additional contention and delay. A physical-layer disturbance may therefore produce consequences that become visible later as a network-level timing problem.

The experimental observations followed this general relationship. Lower SNR was associated with increasing error activity, but similar signal conditions did not always produce the same reliability state. Bus load, message loss, and latency influenced the final communication outcome. This explains why SNR was highly important without becoming the sole determinant of classification.

The result is also consistent with the broader understanding of automotive communication as a system-level problem involving timing, dependability, physical implementation, and network architecture [3], [4]. For autonomous vehicle applications, these dimensions become increasingly interdependent because communication supports control functions with different levels of timing sensitivity.

7.4 Importance of Communication Latency

Communication latency emerged as the most influential individual feature in the Random Forest model. This finding deserves particular attention because a CAN message may be transmitted without corruption and still become unsuitable for a time-sensitive control function if it arrives too late.

Earlier work on CAN response-time analysis demonstrated that message delay depends on factors including priority, blocking, transmission time, and interference from higher-priority traffic [5]. The present results extend this reasoning into the reliability-assessment context. Latency was not treated only as a schedulability measure; it also acted as an observable consequence of changing network conditions.

An increase in latency can originate from several sources. Higher bus utilization increases contention for access to the communication medium. Error-induced retransmissions consume additional bus time. Repeated interference can further reduce effective communication efficiency. Latency can therefore accumulate information about several underlying conditions, which may explain its strong contribution to the classifier.

At the same time, latency should not be interpreted independently. A busy but correctly functioning network may show increased delay without being critically unreliable. The model's use of latency together with signal quality, error behaviour, and message loss is therefore more informative than applying a single latency limit to every operating situation.

7.5 Interpretation of the Communication Reliability Index

The Communication Reliability Index provided a continuous representation of network condition alongside the categorical predictions of the classifier. Mean CRI decreased from 84.36 under Normal conditions to 66.93 for Degraded communication and 39.69 for Critical conditions. This progression indicates that the index responded in the expected direction as communication impairment increased.

The overlap between neighbouring CRI distributions is also important. Communication degradation is not naturally divided into perfectly separated numerical regions. A network can move gradually from stable operation toward a more serious condition. Consequently, some observations near a class boundary are expected to have similar reliability scores despite receiving different categorical labels.

This characteristic supports the use of classification and CRI together. The class label provides a simple operational interpretation, whereas the numerical index preserves information about severity and trend. Two observations may both be classified as Degraded while having substantially different CRI values. A score near the Normal boundary may indicate mild deterioration, whereas a continuously declining score approaching the Critical region may justify a stronger response.

For practical monitoring, the trend of the index may be as important as its value at one instant. A gradual decline across successive observation windows can indicate progressive deterioration even before the system changes class. This could be useful for predictive maintenance or early warning, although longitudinal validation would be required before making such claims for a production vehicle.

7.6 The Role of the Degraded Communication State

The inclusion of an intermediate Degraded state is one of the important design choices in the proposed framework. Binary classification is attractive because it simplifies the decision process, but it can conceal the transition between healthy communication and severe impairment.

The lower classification performance obtained for the Degraded class reflects the difficulty of this intermediate region rather than necessarily indicating that the class is unnecessary. In fact, the uncertainty surrounding this state is one reason why it is useful. Communication conditions do not always move directly from fully acceptable operation to failure. Intermittent errors, gradually increasing latency, declining signal quality, or unstable message availability can appear before a more serious condition develops.

An early warning state provides a mechanism for representing this uncertainty. Instead of immediately declaring failure, the monitoring system can increase observation frequency, record the developing event, or request further diagnostic evaluation. In an actual vehicle implementation, the response would need to depend on the affected communication domain and the safety relevance of the messages involved.

The three-state structure therefore offers a compromise between oversimplified binary monitoring and an excessively complex set of diagnostic categories. Future work could extend this representation by using probabilistic outputs or continuous risk estimation rather than relying entirely on fixed class boundaries.

7.7 Implications for Autonomous Vehicle Communication

Autonomous and highly automated vehicles depend on information that is not only correct but also available at the required time. Communication degradation can affect the transfer of sensor status, actuator commands, vehicle-state information, and coordination messages among electronic controllers. The significance of a communication problem therefore depends on both its technical severity and the function supported by the affected messages.

The proposed framework does not attempt to determine the functional safety consequence of every CAN message. Instead, it provides an assessment of communication condition that could serve as an additional input to a higher-level supervisory mechanism. A supervisory controller could combine communication-health information with application-specific requirements before deciding whether to continue normal operation, increase monitoring, activate redundancy, or enter a fallback state.

Such integration would require substantially more validation than the present simulation-based study provides. Nevertheless, the framework illustrates how communication monitoring can move beyond simple error counting. By combining signal integrity, transmission behaviour, and network performance, the system obtains a broader representation of communication health.

This is particularly relevant to heterogeneous vehicle architectures. Future vehicles are likely to combine Classical CAN, CAN FD, Automotive Ethernet, and other communication technologies rather than rely on a single network protocol. A general communication-health concept based on measurable quality and reliability indicators may therefore have value beyond one specific bus technology, although the selected features and decision limits would need to be adapted.

7.8 Comparison with Earlier Intelligent CAN Monitoring Research

Much of the intelligent CAN monitoring literature has focused on detecting cyberattacks or anomalous message behaviour. Entropy-based analysis has been used to identify deviations in network traffic [6], while timing characteristics and survival analysis have been applied to detect unusual message patterns [7]. Machine-learning approaches have further demonstrated that CAN observations can be classified according to learned patterns rather than only predefined rules [9].

The present framework differs in its primary objective. The focus is not restricted to malicious or unauthorized traffic. Instead, the model considers communication degradation arising from signal disturbance, transmission errors, network loading, latency, and message loss. A communication anomaly may therefore be relevant even when no cyberattack is present.

This distinction is important because reliability and security can produce overlapping symptoms without being identical problems. Unusual message timing may result from malicious activity, network congestion, retransmission, or a developing physical fault. A reliability-oriented framework should therefore avoid assuming that every deviation represents an attack.

The proposed study contributes to this broader interpretation by combining signal-related and network-level features within a communication-state model. The results indicate that such integration can improve classification compared with isolated fixed thresholds under the experimental conditions considered.

7.9 Practical Limitations

The results should be interpreted in relation to several limitations. First, the evaluation was conducted in a controlled simulation-based environment. Although this approach enables repeatable variation of traffic and disturbance conditions, it cannot reproduce every characteristic of a physical automotive network. Real vehicles contain differences in wiring topology, transceiver behaviour, grounding, connector condition, electromagnetic exposure, ECU scheduling, and message patterns.

Second, the class definitions and CRI boundaries used in this study are experimental. The ranges of 80–100 for Normal, 50–79 for Degraded, and below 50 for Critical provide a structured basis for evaluation, but they should not be treated as universal automotive standards. A production implementation would require calibration against the timing and reliability requirements of the specific vehicle architecture.

Third, the Random Forest model was trained using the conditions represented in the experimental dataset. Machine-learning performance depends on the similarity between training data and future operating conditions. Previously unseen fault mechanisms or substantially different traffic profiles may reduce classification performance. Validation across multiple network configurations is therefore necessary.

Fourth, the feature-importance values should be interpreted as properties of the trained model and dataset rather than universal rankings of CAN reliability factors. The importance of latency, SNR, or error behaviour may change when the experimental environment, feature distribution, or vehicle architecture changes.

Finally, the study evaluates communication state rather than complete vehicle safety. A high or low reliability score does not directly determine whether an autonomous driving function is safe. Such a conclusion would require integration with system-level hazard analysis, functional safety requirements, redundancy mechanisms, and application-specific timing constraints.

7.10 Directions for Further Validation

The next stage of evaluation should move from controlled simulation toward physical and hardware-assisted testing. A CAN test bench containing real transceivers, configurable termination, controllable noise injection, and representative ECUs would allow the relationship between physical signal degradation and network behaviour to be examined more directly.

Hardware-in-the-loop experiments would provide a further step by introducing realistic controller timing and closed-loop behaviour. Vehicle-derived CAN traces could also be used to examine whether the model generalizes to communication patterns that were not generated by the original experimental setup.

Future work should additionally investigate temporal models capable of considering sequences of reliability observations. The present framework classifies communication using features extracted from individual observation windows. A temporal approach could examine whether a series of small changes forms a meaningful degradation trend.

The CRI weighting mechanism also requires further validation. Feature importance provides one basis for assigning relative influence, but alternative approaches could include data-driven optimization, probabilistic reliability models, or domain-specific weighting based on the criticality of communication functions.

Despite these limitations, the present results support the central premise of the study. Signal integrity and communication reliability are closely connected, and their combined assessment provides more information than isolated monitoring of individual CAN parameters. The proposed framework offers a structured basis for identifying normal operation, intermediate degradation, and critical communication conditions while retaining both categorical and continuous representations of network health.

8. Conclusion and Future Work

This study presented an intelligent framework for assessing signal integrity and communication reliability in CAN-based autonomous vehicle systems. The work was motivated by the observation that communication degradation is rarely represented adequately by a single network measurement. Changes in signal quality, error behaviour, bus utilization, message availability, and communication delay can occur together and may collectively indicate a developing reliability problem even when individual parameters have not reached critical limits.

The proposed framework combined six principal communication indicators: signal-to-noise ratio, bit error rate, frame error rate, communication latency, bus load, and message loss ratio. These measurements were processed through a Random Forest classifier to distinguish among Normal, Degraded, and Critical communication states. A

Communication Reliability Index was also introduced to provide a continuous representation of network condition alongside the categorical classification result.

The experimental evaluation showed that the proposed framework achieved an overall classification accuracy of **88.67%**, with a macro precision of **88.61%**, macro recall of **88.64%**, and macro F1-score of **88.60%**. In comparison, the fixed-threshold monitoring method achieved an accuracy of **78.78%** and a macro F1-score of **77.92%**. The intelligent framework therefore improved accuracy by **9.89 percentage points** and macro F1-score by **10.68 percentage points** under the experimental conditions considered.

The classification results also revealed a meaningful pattern in the distribution of errors. Normal and Critical conditions were identified with F1-scores of **90.51%** and **92.83%**, respectively, while the Degraded state produced a lower F1-score of **82.47%**. Most incorrect predictions occurred between neighbouring communication states. No direct confusion between Normal and Critical conditions was observed in the independent test set. This indicates that the model captured the general progression of communication deterioration, although transitional conditions remained more difficult to separate.

The Communication Reliability Index provided an additional view of this progression. Mean CRI values decreased from **84.36** during Normal operation to **66.93** under Degraded conditions and **39.69** under Critical conditions. The overlap observed between neighbouring classes reflects the continuous nature of communication deterioration and supports the use of the CRI together with discrete state classification. A categorical label can indicate the current operating region, while the numerical index can provide information about severity and developing trends.

Feature-importance analysis further demonstrated the value of combining measurements from different aspects of CAN operation. Communication latency, signal-to-noise ratio, and frame error rate were the three most influential variables in the trained model. This finding supports the central argument of the study that physical signal conditions and network-level communication behaviour should not be assessed independently. A disturbance originating at the physical layer can contribute to transmission errors and retransmissions, which may subsequently affect bus utilization and message timing.

The proposed framework is not intended to replace the error-detection, retransmission, and fault-confinement mechanisms already available in CAN. These mechanisms remain fundamental to reliable CAN operation. Instead, the framework adds an assessment layer that interprets several communication indicators together and provides an estimate of the broader network condition. Such an approach may be useful for identifying progressive degradation that is difficult to represent using isolated fixed thresholds.

The findings should nevertheless be considered within the scope of the experimental design. The evaluation was conducted in a controlled simulation-based environment using defined communication conditions and a representative CAN network configuration. The reported performance therefore demonstrates the behaviour of the framework under those conditions rather than establishing universal performance for all autonomous vehicle architectures. Real vehicle networks differ in topology, message scheduling, transceiver characteristics, electromagnetic exposure, wiring configuration, and functional requirements.

Future work should first focus on validation using physical CAN hardware. A laboratory test bench containing actual CAN controllers and transceivers would allow signal degradation to be introduced through controlled changes in noise, termination, wiring, and network loading. Such experiments would provide a stronger basis for examining the relationship between measured physical-layer disturbances and the communication indicators used by the framework.

Hardware-in-the-loop testing represents a further direction. Integrating the monitoring framework with real or representative vehicle controllers would make it possible to evaluate communication reliability under more realistic timing and control conditions. Vehicle-derived CAN traces should also be incorporated to determine whether the trained model generalizes beyond synthetically generated traffic.

The intelligent assessment component can be extended in several ways. Random Forest was selected in the present study because of its ability to represent nonlinear relationships while retaining comparatively straightforward interpretation. Future investigations could compare it with gradient-boosting methods, support vector machines, neural networks, and temporal learning models. Sequence-based approaches may be particularly useful for detecting gradual degradation because they can consider how communication indicators evolve across successive observation windows rather than treating each window independently.

Further development of the Communication Reliability Index is also required. The weighting scheme can be calibrated using larger experimental datasets and domain-specific reliability requirements. Future versions may incorporate message criticality so that degradation affecting braking or steering communication is treated differently from degradation affecting less time-sensitive traffic. Probabilistic confidence measures could also be incorporated to represent uncertainty near the boundaries between Normal, Degraded, and Critical states.

Another important direction is the extension of the framework to heterogeneous in-vehicle networks. Modern vehicle architectures increasingly combine Classical CAN with CAN FD, Automotive Ethernet, and other communication technologies. Although the specific indicators and thresholds would differ, the underlying principle of combining physical and network-level observations could be adapted to these environments. A unified communication-health framework capable of monitoring several network technologies would be valuable for increasingly complex vehicle architectures.

In conclusion, the study demonstrates that intelligent multi-parameter monitoring can provide a more informative assessment of CAN communication reliability than isolated fixed-threshold analysis under the evaluated conditions. By combining signal integrity indicators, transmission behaviour, network performance, machine-learning-based classification, and a continuous reliability index, the proposed framework provides a structured basis for distinguishing stable communication from progressive degradation and critical impairment. Further validation on physical hardware and real vehicle communication data is necessary, but the results establish a foundation for developing more adaptive communication-health monitoring mechanisms for future autonomous and safety-critical automotive systems.

References

1. R. Bosch GmbH, CAN Specification Version 2.0. Stuttgart, Germany: Robert Bosch GmbH, 1991.
2. W. Voss, A Comprehensible Guide to Controller Area Network. Greenfield, MA, USA: Copperhill Technologies Corporation, 2005.
3. N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert, “Trends in automotive communication systems,” Proceedings of the IEEE, vol. 93, no. 6, pp. 1204–1223, 2005.
4. N. Navet and F. Simonot-Lion, Eds., Automotive Embedded Systems Handbook. Boca Raton, FL, USA: CRC Press, 2008.
5. K. Tindell, A. Burns, and A. J. Wellings, “Calculating controller area network (CAN) message response times,” Control Engineering Practice, vol. 3, no. 8, pp. 1163–1169, 1995.
6. M. Müter and N. Asaj, “Entropy-based anomaly detection for in-vehicle networks,” in Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 2011, pp. 1110–1115.
7. M. L. Han, B. I. Kwak, and H. K. Kim, “Anomaly intrusion detection method for vehicular networks based on survival analysis,” Vehicular Communications, vol. 14, pp. 52–63, 2018.
8. M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN bus security challenges,” Sensors, vol. 20, no. 8, Art. no. 2364, 2020.
9. O. Avatefipour, A. S. Al-Sumaiti, A. M. El-Sherbeeny, E. M. Awwad, M. A. Elmeligy, M. A. Mohamed, and H. Malik, “An intelligent secured framework for cyberattack detection in electric vehicles’ CAN bus using machine learning,” IEEE Access, vol. 7, pp. 127580–127592, 2019.
10. K. H. Johansson, M. Törngren, and L. Nielsen, “Vehicle applications of controller area network,” in Handbook of Networked and Embedded Control Systems, D. Hristu-Varsakelis and W. S. Levine, Eds. Boston, MA, USA: Birkhäuser, 2005, pp. 741–765.
11. C. M. Bishop, Pattern Recognition and Machine Learning. New York, NY, USA: Springer, 2006.
12. T. M. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.
13. L. Breiman, “Random forests,” Machine Learning, vol. 45, pp. 5–32, 2001.
14. T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning: Data Mining, Inference, and Prediction, 2nd ed. New York, NY, USA: Springer, 2009.