



Publisher
Sustainability for Regions



REVEALING RESILIENCE: AI ANOMALY DETECTION DRIVEN DESIGN CONSIDERATIONS FOR CYBER PHYSICAL SYSTEMS SUPPORTING CRITICAL INFRASTRUCTURES IN SMALL ISLAND DEVELOPING STATES

Amir Mohammed ¹, Daniel Goitia ², Sheikh Ahad Ahmad ³, Craig Ramlal ⁴

^{1,2,4}*The University of The West Indies, Department of Electrical and Computer Engineering, St Augustine, Trinidad and Tobago*

³*The University of Western Ontario, 151 Richmond Street, London, Ontario, Canada*

E-mails: ¹amirmohammed45@gmail.com; ²daniel.goitia@uwi.edu; ³sheikh.ahmad154@gmail.com; ⁴craig.ramlal@uwi.edu

Received 18 June 2025; accepted 29 August 2025; published 30 September 2025

Abstract. Ensuring the resilience of Cyber Physical Systems (CPSs) has emerged as a critical priority, particularly for small island developing states (SIDS) and low-resource regions such as the Caribbean. These systems, which tightly couple sensing, computation, and control, are increasingly vulnerable to operational disruptions such as cyber-attacks and sensor faults. In this context, resilience must go beyond disturbance tolerance to encompass real-time anomaly detection (AD), system adaptation, and recovery, ensuring sustained operational safety, reliability, and continuity. This paper uses a machine learning based AD case study to examine the resilience of a Vehicular Cyber-Physical System (VCPS) configured for platooning. Rather than proposing a novel detection method, the study leverages an established framework to extract deeper insights into the resilience needs of VCPSs operating under constrained conditions. For regions with limited redundancy and prolonged recovery times, such as SIDS, the findings emphasise the importance of integrated detection mechanisms that identify threats and support timely and adaptive system responses. This work positions anomaly detection as a diagnostic lens for resilience, contributing to sustainable, secure, and trustworthy transportation infrastructure aligned with broader development goals for CPSs.

Keywords: resilience; anomaly detection; Cyber Physical Systems; cyber attacks; Small Island Developing States

Reference to this paper should be made as follows: Mohammed, A., Goitia, D., Ahmad, Sh.A., Ramlal, C. 2025. Revealing resilience: AI anomaly detection driven design considerations for Cyber Physical Systems supporting critical infrastructures in Small Island Developing States. *Insights into Regional Development*, 7(3), 148-169. <http://doi.org/10.70132/p6489444663>

JEL Classifications: C88, C89

Additional disciplines: computer engineering

1. Introduction

Cyberattacks on critical infrastructure are a frequent and escalating global threat, with both the number and sophistication of attacks rising sharply (Riggs et al., 2023). This escalation is driven by rapid digitisation and geopolitical tensions, with weekly attacks on utilities quadrupling since 2020 (KnowBe4, 2024). In recent times internationally, countries have been subjected to such occurrences such as Russian cyberattacks on Ukrainian infrastructure which has risen by nearly 70% (CSIS, 2025), China has experienced an increase of espionage attacks by approximately 150% (CrowdStrike, 2025), while ransomware complaints from U.S. critical-infrastructure organizations have increased by 9% year over year (Internet Crime Complaint Center, 2025). When compared to Latin America and the Caribbean (LAC), this region is currently considered the world's

fastest-growing region for disclosed cyber incidents, averaging about 25% annually over the past decade. LAC also remains among the least protected, with public administration and finance being the most frequently targeted sectors (Cobos & Diao, 2024). In Q2 of 2024, organisations in Latin America experienced a 53% year-over-year rise in weekly attacks, the largest regional jump that quarter (Check Point Team, 2024). Telemetry data from Fortinet has revealed roughly 11% of recorded global exploitation in the Latin America region (FortiGuard Labs, 2025), with a consistent pattern of government and financial entities being mostly targeted from 2023 to 2024 (Positive Technologies, 2023). The industry sector is also a key target, as about one in five ICS (Industrial Control Systems) computers in Latin America had detected or blocked malicious objects in Q1 2025 (Kaspersky Lab, 2025). Some other notable successful cyber-attacks within industry include Stuxnet, Black Energy, WannaCry, Industroyer and Triton (Malik et al., 2023), which contributed to the crippling of national infrastructure systems. Naturally, this highlights the region's vulnerability and inadequate cybersecurity measures amid rapid digital transformation (Brain & Oyadeyi, 2023).

Contemporary critical infrastructures (CIs) comprise interdependent cyber-physical systems (CPSs) alongside human and organisational processes. In this study, we focus on the CPS layer to examine how attacks and fault events at this level affect CPS operation and to identify what must be considered to protect CPS; by extension, these protections shape critical-infrastructure outcomes. CPSs are the integration of computation, communication networks, and physical processes, where embedded systems monitor and control real-world operations (Khalil et al., 2023). These systems underpin CIs such as smart grids, healthcare, military operations, and telecommunications, making them vital to national and regional development (Puig et al., 2016). For emerging economies within small island developing states (SIDS), CPSs are central to modernisation, public safety, and digital economy growth. Consequently, the rising cyber risk to CI translates directly into risks affecting CPSs integrity and reliability (Humayed et al., 2017).

Given these risks, CPS resilience has become an urgent priority, particularly for regions seeking to protect socio-economic progress achieved through digitalisation. In this context, resilience is the capacity to anticipate, absorb, adapt to, and recover from internal faults and external cyber threats (Ross et al., 2021). Without real-time detection mechanisms, CPS become susceptible to cascading failures, jeopardising safe and reliable operation (Palleti et al., 2021). This imperative is even more critical in resource-constrained contexts such as SIDS in the LAC region, where limited redundancy or delayed recovery capacity means a single disruption can have disproportionate effects (Griffor et al., 2017). Building on this, researchers have developed a range of AD strategies for CPS. Prior work spans a wide range of machine learning based approaches which include (i) supervised learners (Biddle & Fallah, 2021) (ii) deep models (Roh et al., 2022), (iii) unsupervised/one-class methods (Song, Hyun, & Cheong, 2021), (iv) hybrid model-based ML schemes (Hao, Yang, & Yang, 2023) and (v) online, transfer or federated variants (Khraisat et al., 2024). These detectors have been applied to false-data injection (FDI) against estimators and sensor fusion, Denial-of-Service (DoS) or jamming on V2X and in-vehicle networks; replay and spoofing misbehaviour in cooperative manoeuvres; and bias/drift faults at sensors and actuators.

Even with these advances, current literature largely focuses on developing individual detection techniques and benchmarking them in scenario-specific attack settings, with limited analysis of the results for resilience outcomes in practice. This constitutes a critical gap, and so our work focuses on attack or anomaly detection (AD) as one of the core processes in the resilience cycle. Rather than proposing a new detector, this study uses a vehicle platooning scenario, an archetypal CPS, directly tied to transportation critical infrastructure, to apply a representative supervised AD method and distil actionable, evidence-based design considerations for CPS resilience. This empirically grounded approach, drawing guidance from observed AD performance in realistic deployment, is especially relevant for Small Island Developing States (SIDS). Although many of the individual insights appear in prior work, they are seldom consolidated into a single, coherent set of AD-informed design considerations for CPS resilience. Our case study provides synthesis and practical guidance for integrating AD

modules into CPS. Framing AD in this way clarifies the capabilities CPS must possess to maintain performance and recover in real operational settings. Accordingly, the contribution extends beyond validating an AD method: it demonstrates how resilience can be operationalised, particularly in resource-constrained SIDS, where transport infrastructure is vital yet fragile and supports digital sustainability agendas aligned with the UN Sustainable Development Goals (UNDP, 2022).

This article is divided into five (5) Sections. Section 1 gives a brief Introduction. Section 2 describes the Vehicle Platoon System (VPS) model as a representative CPS. Section 3 highlights the Anomaly detection method. Section 4 discussed the results produced. Section 5 describes the Insights generated from the study, and Section 6 highlights the conclusion.

2. Vehicular Cyber Physical System – Vehicle Platoon System

The Vehicular Platoon System (VPS) model and its associated components, including the communication topology, control objectives, and anomaly modelling framework used in this study, have been previously detailed (Mohammed et al., 2025). For completeness and continuity, a summary is provided here. The VPS operates using a Predecessor-Follower (PF) communication topology, wherein each vehicle tracks its immediate predecessor's state, allowing for safe inter-vehicular spacing in constrained environments. The vehicle dynamics follow a longitudinal kinematic formulation, with position, velocity, and acceleration represented in a state-space framework as shown in Equation 1, and system architecture depicted in Figure 1.

$$\dot{x}(t) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 1 \\ \frac{1}{\tau} \end{bmatrix} u(t) \quad (1)$$

The communication structure and control objectives, such as the constant time headway (CTH) policy (Equation 2, Figure 2), are consistent with conventional platoon control strategies.

$$d_{cth} = L_v + (V_p \times t_{cth}) \quad (2)$$

Where d_{cth} is the safety distance the following vehicle must maintain, L_v is the vehicle's length, V_p is the velocity of the predecessor and t_{cth} is the time head way constant. Figure 2 highlights the position and velocity profiles for a 3 VPS, when the safety distance is being maintained.

In VPS-based mobility systems, ensuring safety and operational efficiency is crucial, particularly in regions where traffic accidents have economic and health consequences. This control strategy ensures that each vehicle maintains an adaptive distance based on its velocity and time headway constant, promoting safe driving behaviour and minimising the risk of rear-end collisions, an essential consideration for public transport or logistics networks in resource-constrained regional settings.

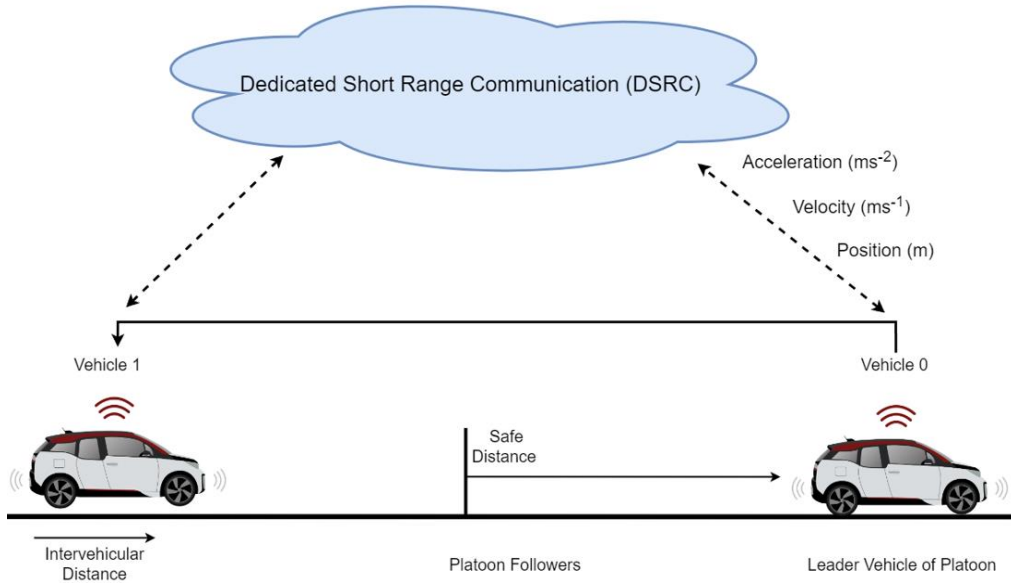


Figure 1. The Vehicle Platoon System
 Source: Adapted by the authors from Mohammed et al. (2024)

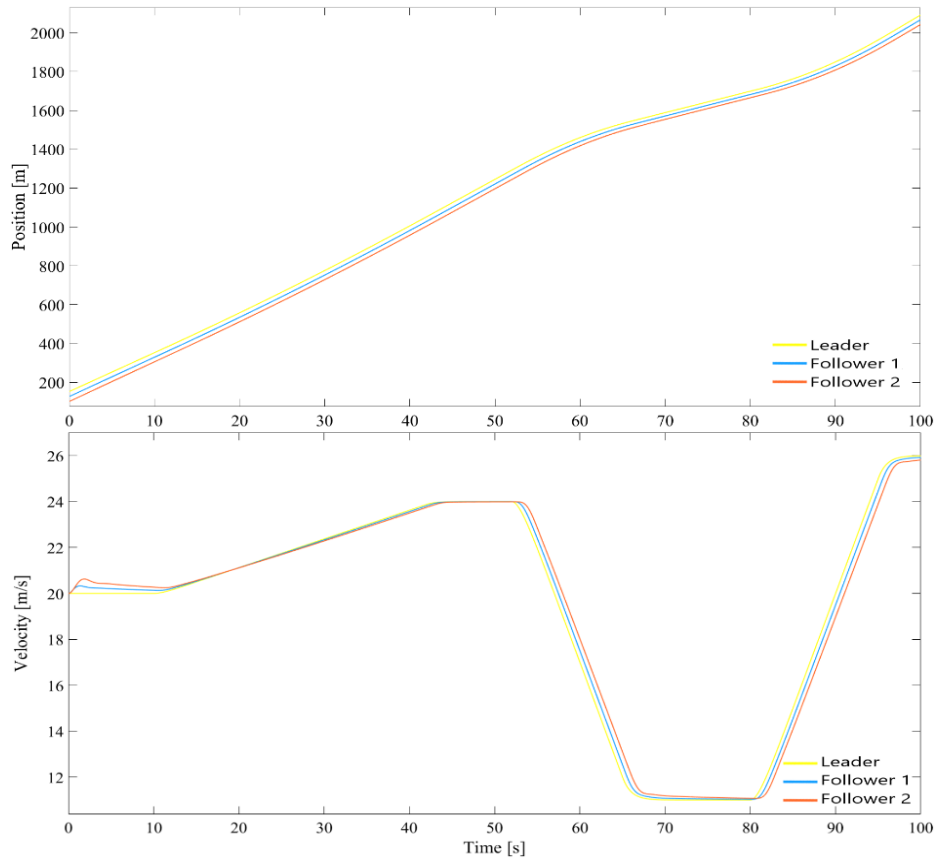


Figure 2. The Position and Velocity Profile for the Platoon System Maintaining the Specified Safety Distance

2.1 Anomaly Modelling

The anomaly scenarios explored in this study also align with our previously published setup. We simulate cyber-physical threats using an FDI attack model to corrupt communicated states such as position and velocity, and a bias fault model to represent sensor degradation in onboard Lidar and Radar systems. These models reflect the dual vulnerabilities faced by CPSs in emerging mobility systems. While full derivations and modelling rationales are provided in (Mohammed et al., 2025) the summary here enables the reader to interpret downstream results in Section 4. The VPS structure and interaction with both cyber and sensor anomalies are illustrated in Figure 3, which provides the foundation for subsequent resilience analysis using machine learning-based AD.

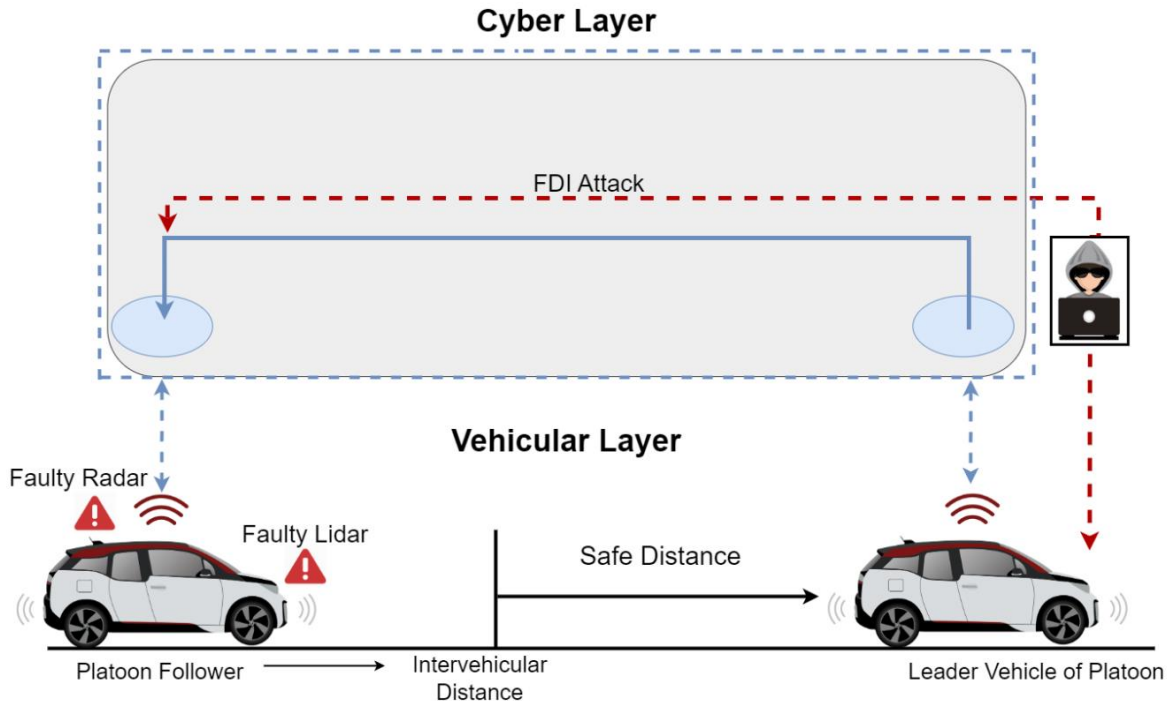


Figure 3. The Position and Velocity Profile for the Platoon System Maintaining the Specified Safety Distance
Source: Adapted by the authors from Mohammed et al. (2024)

2.2 VPS Interaction with Anomaly Model

This section extends the dual-layer anomaly modelling framework originally presented in (Mohammed et al., 2025), where the VPS was analysed under both cyber and fault disturbances. The system architecture, shown in Figure 3, is composed of the Cyber Layer, representing the communication and data-handling infrastructure between the leader and following vehicles, and (2) the Vehicular Layer, encompassing the physical sensors and actuation systems. Together, these layers simulate how the following vehicle maintains a safe inter vehicular distance based on received motion data position and velocity from its leader. The cyber layer is modelled to allow for FDI attacks, wherein adversaries manipulate transmitted state information, such as spoofing or corrupting velocity or position data. Simultaneously, the vehicular layer incorporates intermittent sensor bias faults, simulating real-world issues such as hardware degradation or calibration drift, particularly in onboard Lidar and Radar sensors. These faults and attacks can occur independently or concurrently, introducing complex challenges for system stability and safety. By retaining the anomaly model structure from the prior study while recontextualising it within a resilience-focused evaluation, this section forms the basis for assessing system behaviour under compounding threats. This modelling approach supports realistic resilience testing scenarios aligned with transport infrastructure challenges in resource-constrained regions. Figure 3 reflects this interaction, providing a foundation for the anomaly detection evaluations discussed in later sections.

Cyber Attack and Fault Interaction with VPS model

The VPS is subjected to cyber-attacks and sensor faults. FDI cyber-attacks alter the transmitted state information, such as position and velocity, either individually or simultaneously, at any time and for any duration. Concurrently, the onboard sensors of the following vehicles, namely Lidar and Radar are used to detect the predecessor's distance and velocity, respectively, may be affected by bias faults. These faults can also occur independently or simultaneously, and their magnitude, frequency, and duration are heterogeneous. Moreover, these cyber-attacks and sensor faults can simultaneously occur, making it particularly challenging to maintain reliable state estimation and control. Figure 4 demonstrates the effects of FDI attacks on the transmitted position and velocity data, while Figure 5 illustrates the influence of bias faults on Lidar and Radar sensor measurements. Together, these scenarios underscore the need for a robust and accurate anomaly detection module within the VPS framework.

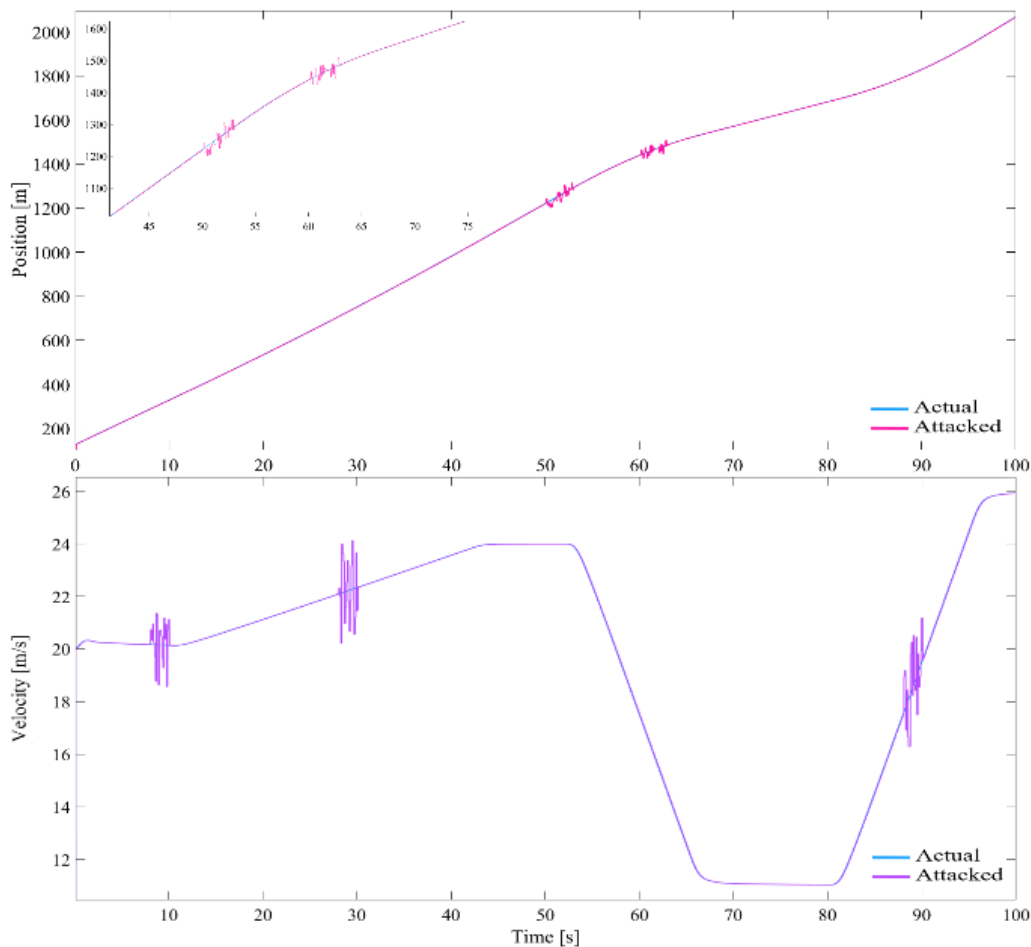


Figure 4. FDI Attacks on Position and Velocity

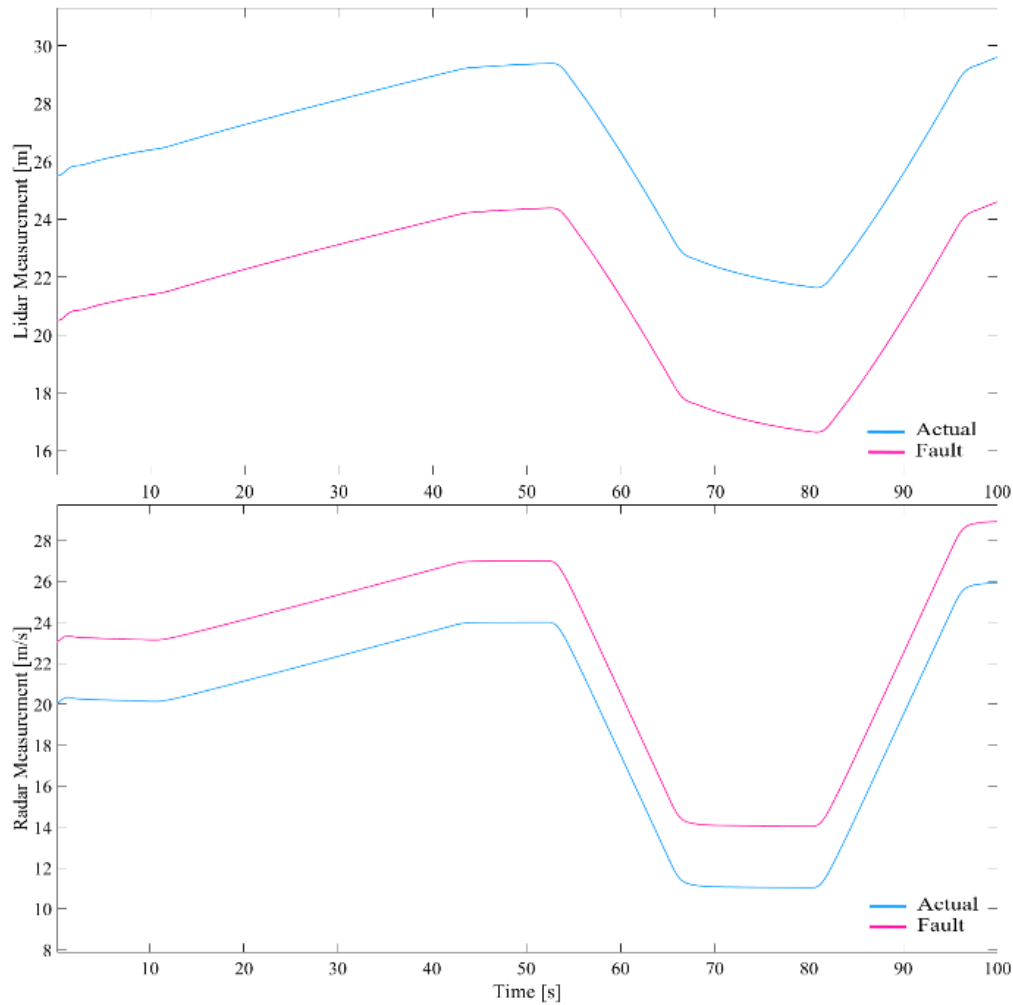


Figure 5. Bias Fault Affecting Both Lidar and Radar

3. Anomaly Detection Method

This section establishes how existing detection mechanisms perform under cyber and sensor anomalies in a VCPS. These empirical observations are later used to extract resilience-related insights such as latency, classification errors, and detection behaviour under concurrent anomalies discussed in Section 4. Thus, this section serves as a diagnostic platform for understanding resilience, not as a contribution to detection algorithm development.

Machine Learning Detection

The detection of FDI cyber-attacks and bias in the sensor measurements for Lidar and Radar is facilitated using supervised learning. This machine learning method uses a known dataset to train an algorithm with a known set of input data features or known responses to make predictions. Utilising supervised learning, four (4) anomaly detectors were trained for the following conditions:

- FDI attacks on position
- FDI attacks on velocity
- Bias faults on Lidar
- Bias Faults on Radar

The training data is formed from 14 independent data sets generated from the simulation. The data sets are as follows: communicated position, communicated velocity, lidar measurements, radar measurements, the change in position, the change in velocity, the change in lidar measurements, the change in radar measurements, position attack class, velocity attack class, position offset, velocity offset, lidar offset, and radar offset. Using different combinations of these data sets, the 4 detectors were trained based on the feature which needed to be predicted such as position, velocity, lidar or radar or a combination of all classes.

Position Anomaly Detector

The position detector was employed to classify the position state, and the classification included two categories: 1) position attacked and 2) position not attacked. In the supervised learning process, the position detector was trained with a diverse mixture of training data. This training set incorporated non-attack data for both position and velocity, as well as FDI attack data on position and FDI attack data on velocity. This comprehensive training approach enabled the detector to gain a deeper understanding of data variations. Using this diverse dataset, the position detector accurately classified the state of the position variable. The position anomaly detector underwent training using the Fine Tree Algorithm within the Classification Learner application in MATLAB 2023a. Details regarding the accuracy of the detector will be discussed later.

Velocity Anomaly Detector

The velocity detector determined whether the velocity state was under attack or not, employing a classification approach like that of the position anomaly detector. The velocity detector underwent training with a diverse set of training data in the supervised learning process. In this instance, the velocity detector included non-attack data for both position and velocity, as well as FDI attacks on position and FDI attacks on velocity data in its training set. This inclusive training approach enabled the velocity detector to classify the state of the velocity variable accurately. The Medium Tree Algorithm was employed to train the velocity detector.

Lidar Anomaly Detector

The Lidar detector was used to classify the state of the Lidar sensor. The classification consisted of either 1) fault detected or 2) no fault detected. In a similar manner, the Lidar detector was trained using a mixture of varying training data within the supervised learning process. In this case, the Lidar detector incorporated several varying scenarios that were applied to the sensor, allowing the Lidar detector to classify the faults accurately. These scenarios consisted of non-faulty data on both the Lidar and Radar sensors, along with faulty data on Lidar and Radar. The algorithm which was used was Ensemble Learning – Bagged Trees for this anomaly detector.

Radar Anomaly Detector

The Radar detector was used to classify the state of the Radar sensor. The training process was similar to that of the Lidar detector using the variation in data for the trained model. The algorithm which was used to train the Radar anomaly detector was a bi-layered neural network.

4. Results

This section highlights the results for the supervised learning anomaly detection modules. The results are broken into three main categories:

- Anomaly Detection for Position, Velocity and Radar
- Anomaly Detection for Position, Velocity and Lidar
- Anomaly Detection for Position, Velocity, Radar, and Lidar

4.1 Anomaly Detection – Position, Velocity and Radar

In the first scenario the system undergoes FDI cyber-attacks on position and velocity with faults on the Radar sensor. Table 1 gives a detailed breakdown of the cyber-attacks, faults and the associated times of execution during the simulation where A represents the affected variable. In Table 1, position is affected by an FDI cyber-attack, which intermittently modifies the real value of position by random values within the range $A \pm 18m$. Therefore, during the associated attack times, between the period of 25(s) – 32(s), the true value will be modified. Similarly, this attack is executed within the listed timelines as seen in Table 1 associated with the position variable. Velocity is also affected by FDI attacks with its corresponding attack times, while the Radar sensor is affected by a bias fault during the associated fault time as seen in Table 1. This scenario essentially encompasses the presence of FDI cyber-attacks and bias faults.

Figure 6 highlights the results for each of the anomaly detectors for position, velocity, Radar and Lidar sensors. Therefore, considering Scenario 1, the performance of the anomaly detection for both position and velocity states can be seen in Figure 6. The plot consists of lows (0) and highs (1), where a low represents no attack and a high represents an anomaly is detected. Figure 6 consists of two plots for each variable: 1) A black broken line, which represents the anomaly window, and 2) A grey broken line, which represents the anomaly detection generated by the trained models for each variable. In the case of position and velocity the grey broken line represents attack detection, while in the case of the Lidar and Radar the grey lines represent fault detection.

There are four possible outcomes which can exist in the case of anomaly detection: 1) true positive (TP), which means that the detection correctly identified an anomaly, 2) true negative (TN), where the detector correctly identified the absence of an anomaly, 3) false positive (FP), where the system detected an anomaly when there wasn't any existing and 4) false negative (FN) which means that the anomaly detectors detected no anomaly when there was indeed an anomaly. As shown in Figure 6, there are a few recorded instances of FNs and FPs for the anomaly detection associated with the position variable. The anomaly detector for velocity recorded very few FPs. In the case of Radar one instance of a FP was recorded. For each of the associated anomaly detection rates, the performance is very accurate overall, with a few misdetections taking place during the run time of the simulation. The details surrounding the performance of the anomaly detection will be discussed later.

Table 1. The Magnitude of the FDI Cyber Attacks and Bias Faults When Position, Velocity and Radar are Affected

Affected Variable	Cyber Attack/ Fault	Attack Rate %	Attack Time (s)
Position (m)	(FDI) $A \pm 18$	100	25[s] – 32[s] 55[s] – 70 [s] 111[s] – 123[s] 125[s] – 140[s] 130[s] – 135[s]
Velocity (ms^{-1})	$A \pm 10$	100	32[s] – 39[s] 70[s] – 90[s] 100[s] – 109[s] 118[s] – 135[s] 140[s] – 150[s]
Radar Sensor (ms^{-1})	-5 +6 -6 +5 +4	100	10[s] – 15[s] 30[s] – 45[s] 50[s] – 67[s] 79[s] – 95[s] 121[s] – 130[s]

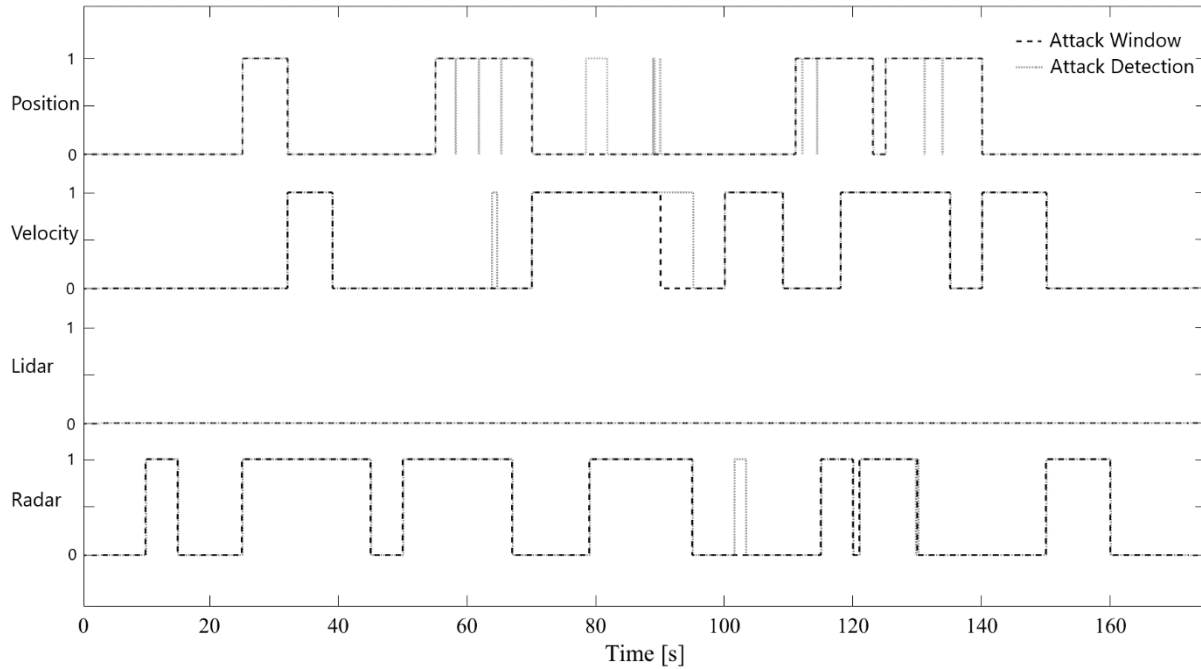


Figure 6. The Associated Anomaly Detection Produced by the Supervised Trained Model for Scenario 1

4.2 Anomaly Detection – Position, Velocity and Lidar

Table 2 highlights the associated execution times of cyber-attacks and faults which affect the position, velocity and Lidar sensor. Figure 7 presents the detection rate for each of the affected states and Lidar sensor. In the case of the anomaly detection rate for the position affected by FDI, it can be seen from Figure 7 that there were a few instances of FPs and FNs. In a similar situation the trained anomaly detector for velocity experienced just one instance of a FN and two instances of a FP. The attack window, as compared to the detection rate, is almost ideal, highlighting the detector's overall good performance. Lastly, there were no FPs or FNs from the detector for the attacked Lidar’s sensor during this scenario.

Table 2. The Magnitude of the FDI Cyber Attacks and Bias Faults When Position, Velocity and Lidar are Affected

Affected Variable	Cyber Attack/ Fault	Attack Rate %	Attack Time (s)
Position (m)	(FDI) $A \pm 18$	100	25[s] – 32[s] 55[s] – 70 [s] 111[s] – 123[s] 125[s] – 140[s] 130[s] – 135[s]
Velocity (ms^{-1})	$A \pm 10$	100	32[s] – 39[s] 70[s] – 90[s] 100[s] – 109[s] 118[s] – 135[s] 140[s] – 150[s]
Lidar Sensor (ms^{-1})	8 -12 11 -9 6	100	10[s] – 15[s] 20[s] – 30[s] 30[s] – 45[s] 60[s] – 80[s] 90[s] – 110[s]

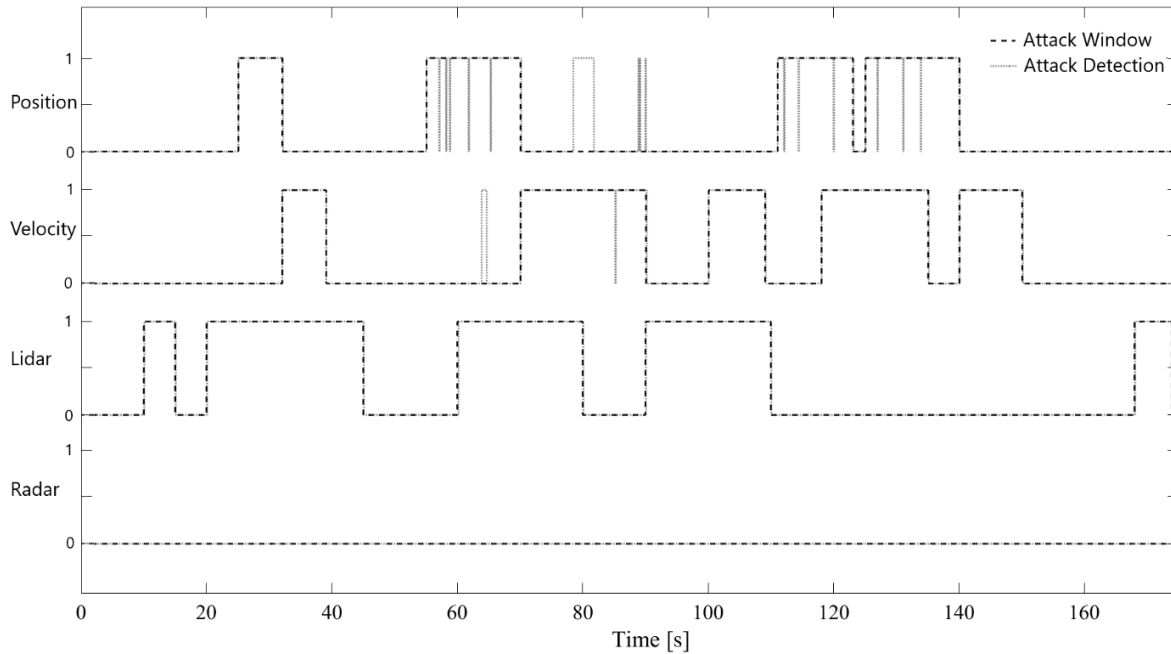


Figure 7. The Associated Anomaly Detection Produced by the Supervised Trained Model for Scenario 2

4.3 Anomaly Detection – Position, Velocity, Lidar and Radar

Table 3 highlights the execution times of cyber-attacks affecting the position and velocity states, along with bias faults on the Lidar and Radar sensors. Figure 8 shows the detection rate for each affected state and sensor. In the case of the detection rate for the position variable affected by FDI attacks, a limited number of FNs were generated with no FPs.

Table 3. The Magnitude of the FDI Cyber Attacks and Bias Faults When Position, Velocity, Lidar and Radar are Affected

Affected Variable	Cyber Attack/ Fault	Attack Rate %	Attack Time (s)
Position (m)	(FDI) $A \pm 18$	100	25[s] – 32[s] 55[s] – 70 [s] 111[s] – 123[s] 125[s] – 140[s] 130[s] – 135[s]
Velocity (ms^{-1})	$A \pm 10$	100	32[s] – 39[s] 70[s] – 90[s] 100[s] – 109[s] 118[s] – 135[s] 140[s] – 150[s]
Lidar Sensor (ms^{-1})	8 -12 11 -9 6	100	10[s] – 15[s] 20[s] – 30[s] 30[s] – 45[s] 60[s] – 80[s] 90[s] – 110[s]
Radar Sensor (ms^{-1})	-5 6 -6 5 4	100	10[s] – 15[s] 30[s] – 45[s] 50[s] – 67[s] 79[s] – 95[s] 121[s] – 130[s]

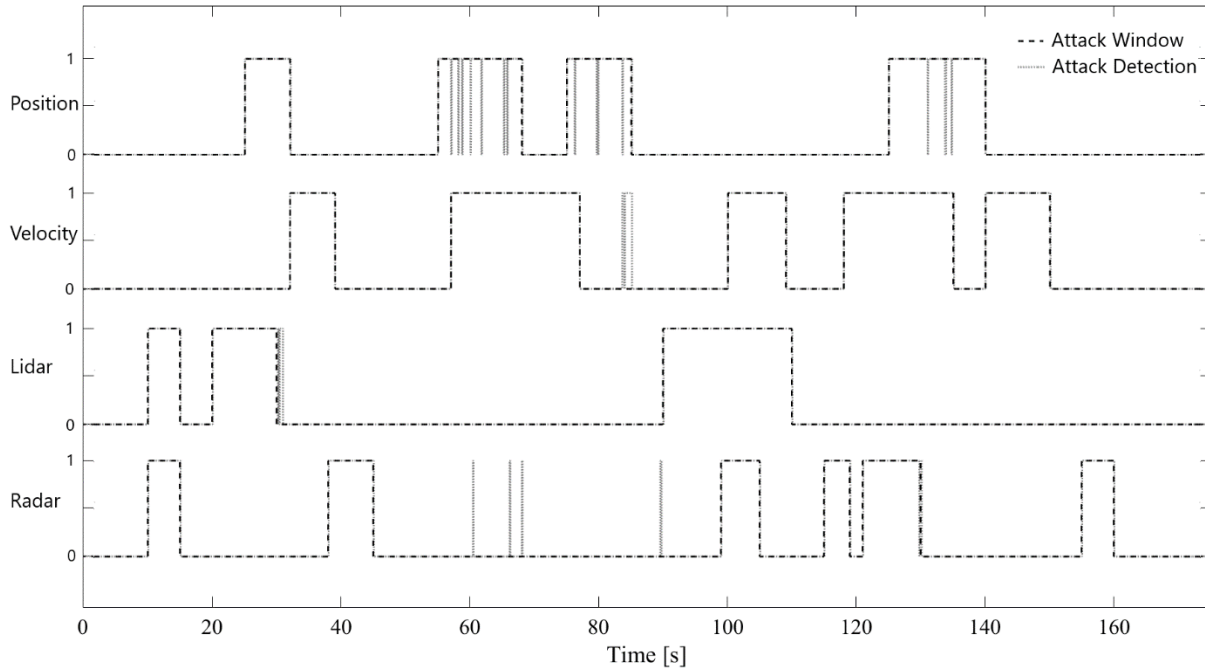


Figure 8. The Associated Anomaly Detection Produced by The Supervised Trained Model for Scenario 3

The anomaly velocity detector recorded a limited number of FPs with no record of any FNs. In the case of Lidar, the detection rate recorded one instance of a FP, a limited number of FPs for Radar and no FNs for both sensors. This scenario showed and overall, very good performance of all detectors.

4.4 Performance of Anomaly Detection Scheme

The popular performance metric used to evaluate the accuracy of trained machine learning models is known as the F1 score. The F1 score can be calculated using recall and precision metrics. The recall is defined as the portion of instances that are correctly predicted as positive to the actual size of the attack class and can be calculated using Equation 5, while the Precision is computed using Equation 6 (Haq, Khan, & Akhunzada, 2021; Khan, Sivaraman, & Honnavalli, 2020).

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

Therefore, using the Recall and Precision values the F1 score can be calculated using Equation 7. Naturally a F1 score ranges from 0 – 1 with 0 being worst case and 1 being best case.

$$F1 = \frac{2 * Precision * Recall}{Precision + Recall} \quad (7)$$

Tables 4, 5 and 6 represent the F1 scores for the anomaly detection method for the three main situations simulated. The anomaly detection scheme produced accurate results based on the high F1 scores computed for each scenario. Additionally, the F1 scores recorded were comparable to other existing anomaly detection methods

presented in literature (Fails & Olsen, 2003; Abu Al-Haija & Zein-Sabatto, 2020; Alkahtani & Aldhyani, 2021; Almasoud et al., 2022; Alsaade & Al-Adhaileh, 2023; Alsulami et al., 2022; Biddle & Fallah, 2021; Hamza et al., 2022; Oucheikh et al., 2020; Roh et al., 2022; Sarwar et al., 2022; Song, Hyun, & Cheong, 2021).

Table 4. The F1 score for the Position, Velocity and Radar Anomaly Detection Scenario

Position, Velocity and Radar						
Detector	TP	FP	FN	Precision	Recall	F1 - Score
Position	483	39	7	0.9253	0.9857	0.9545
Velocity	630	62	0	0.9104	1	0.9531
Radar	819	19	1	0.9773	0.9988	0.9879

Table 5. The F1 score for the Position, Velocity and Lidar anomaly detection scenario

Position, Velocity and Lidar						
Detector	TP	FP	FN	Precision	Recall	F1 - Score
Position	479	39	11	0.9247	0.9776	0.9545
Velocity	629	12	1	0.9813	0.9984	0.9898
Lidar	759	0	1	1	0.9987	0.9993

Table 6. The F1 score for the Position, Velocity, Lidar and Radar anomaly detection scenario

Position, Velocity, Lidar and Radar						
Detector	TP	FP	FN	Precision	Recall	F1 - Score
Position	435	3	15	0.9932	0.9667	0.9797
Velocity	630	17	0	0.9737	1	0.9867
Lidar	350	7	0	0.9804	1	0.9901
Radar	359	6	1	0.9836	0.9972	0.9903

5. Insights from Case Study

As our results have shown, scenarios with F1-scores exceeding 95% still experienced misdetections. This reinforces a crucial systems level insight, resilience must extend beyond detection to include response, recovery, and learning mechanisms. In the context of VPSs, where system coupling and real-time operation amplify the risks of delay or mis-reaction, resilience must be framed as a dynamic, integrated property rather than a binary detection outcome. To this end, the authors present a set of critical insights derived from both simulation results and systems thinking that offer a more nuanced understanding of CPS resilience. While these insights may individually surface across various publications, they are rarely compiled and articulated collectively in a single case study.

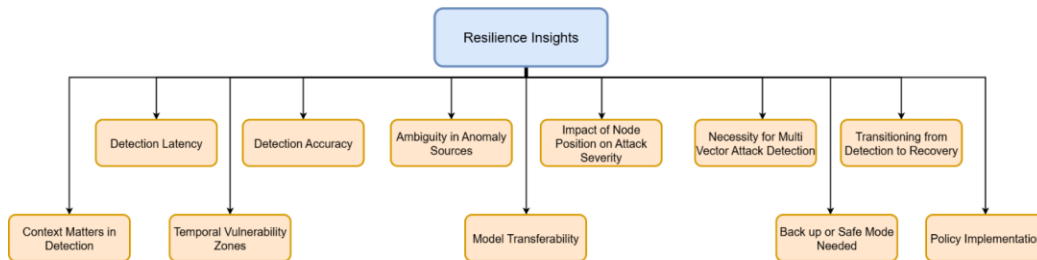


Figure 9. The Insights Drawn from the Case Study

Figure 9 above illustrates key dimensions of resilience insights that will be used to provide a structured and actionable understanding of how anomaly detection performance translates into broader system resilience challenges and opportunities.

5.1 Detection Latency

In the simulated scenarios presented in Figures 6 – 8, the trained anomaly detectors experienced minimal detection delay with faults and cyber attacks detected almost immediately within their onset windows. This outcome reflects the accuracy of the trained detector model and, by extension, the nature of the attacks implemented. In this case study the attack surfaces are relatively limited, and the classifiers were trained under controlled conditions. As such, the issue of detection latency did not manifest in the evaluated test cases. However, this absence of delay under idealised conditions should be given closer attention. In more complex, real-world settings, particularly those involving multiple attack surfaces, evolving anomaly types or higher-dimensional feature spaces, latency in anomaly identification becomes a critical vulnerability. Aspects such as increased model complexity, limited training coverage, or dynamic environmental noise can all introduce subtle delays in detection, even with high offline accuracy. In VPSs, even brief detection delays on the order of 1.5 – 3.9 seconds can cause instability and degrade safety. For instance, a misbehaviour detection system (MDS) with even a modest processing lag may fail to prevent collision risks, especially if fallback modes like Adaptive Cruise Control (ACC) are not sufficiently reactive (Kalogiannis et al., 2022). By contrast, low-latency detection architectures such as those using transformer-based models with decision intervals around 100 ms (Li et al., 2024) demonstrate significant promise in maintaining resilience under high-risk operational conditions. This contrast underscores the importance of developing and deploying detection mechanisms that prioritise not just accuracy, but also timeliness, to ensure the resilience of vehicular platoons under adversarial conditions. This reinforces the point that resilient CPS design must prioritise not only detection accuracy, but also detection timeliness.

5.2 Detection Accuracy (False Positives and False Negatives)

Understanding the impact of FNs and FPs is essential when designing resilient AD systems in VPSs. From the detection plots, there is the existence of FPs and FNs. A FN occurs when an actual anomaly such as FDI or a sensor fault remains undetected. This is arguably the most dangerous situation which can exist, particularly in a tightly coupled system like vehicle platoons. In this situation, misdetection can allow malicious data to enter control loops, resulting in instability. Since the system remains unaware of the ongoing threat, no proper corrective actions can be initiated, leading to an amplified effect downstream which can result in the violation of safety constraints without any warning. As such, many resilience frameworks adopt an approach that prioritises a lower FN rate even at the cost of having slightly elevated FP rates. In safety-critical applications, the cost of missing a real threat naturally outweighs the inconvenience of having a false alarm. In contrast, FPs occur when normal system behaviour is mistakenly flagged as anomalous. While not directly hazardous, FPs can degrade system performance and operational efficiency. False alarms can trigger unnecessary emergency responses like braking, rerouting, or failover control, which increase control effort, fuel use, computational load, and actuator wear, ultimately degrading system performance and operational efficiency. For human-in-the-loop scenarios, frequent false alarms may also lead to operator fatigue, causing delayed or ignored responses to future valid alerts. If unaddressed, high FP rates can eventually result in suppression of alerts altogether, undermining the aspect of trust in the system. Therefore, while FNs may be classed as having greater immediate risks, FPs must be given equal consideration to ensure the reliability, safety, and long-term trustworthiness of the system.

Additionally, FPs and FNs exert broader resilience implications. One key concern is the temporal persistence of misclassifications, whether an FN or FP is quickly corrected or remains unresolved. From a resiliency perspective, these effects underscore the need for temporal awareness in detection systems. Detection models must not only aim to classify accurately in the moment but also include mechanisms for re-evaluating prior classifications over time using updated context. Estimating the confidence of past decisions, especially when operating under uncertainty, is also key. Thus, resilience is not just about getting it right, but about getting it right at the right time and correcting misclassifications before they propagate into significant operational disruption. Therefore, detection systems should be cost-aware, dynamically weighing error penalties in response to context (Schaberreiter et al., 2024).

5.3 Ambiguity in Anomaly Sources (Sensor Faults Mimic Attacks)

The behavioural similarity between sensor faults and cyber-attacks highlighted in Table 1 proves FDI and the bias sensor fault to be a key challenge from the perspective of accurate anomaly attribution. Both types of anomalies can trigger similar deviations in residual signals calculated as the difference between estimated and observed values, making it difficult to distinguish their true origin. While sensor bias faults often introduce persistent deviations due to hardware degradation, FDI attacks intentionally inject malicious perturbations that mimic such patterns to evade detection. This resemblance between faults and attacks is not coincidental; modern adversarial strategies frequently exploit faults like signatures to bypass anomaly detection, especially those based on model prediction or state estimation (Guo, Sun, & Pang, 2023). As a result, the AD strategy may correctly detect an anomaly but misclassify its nature, mistaking sensor drift for an attack, or worse, failing to recognise an attack disguised as a fault. The implications are nontrivial. If a true fault is misclassified as an attack (Roy & Dey, 2023), this may trigger inappropriate countermeasures, wasting resources and inducing service disruptions. Conversely, an attack disguised as a minor fault (Yang, Murguia, & Lv, 2023) could propagate undetected through the control architecture, compromising safety, coordination, and trust, especially in multi-agent scenarios like vehicle platoons, where even one misdiagnosis can have detrimental effects.

Therefore, resilient AD demands fine-grained attribution based on a deep understanding of the behavioural overlaps between faults and attacks. Developing differentiation-aware detection logic able to contextualise anomalies, analyse residual dynamics over time, and incorporate system-level cues is essential to ensuring that appropriate and proportionate responses are taken. In safety-critical domains, mistaking one for the other is not just a classification error; it's a resilience failure. To address this, modern research emphasises the need for multi-layered detection architectures capable of identifying anomalies and attributing them accurately (Rendall et al., 2025).

This consideration becomes even more critical in the context of larger, high-dimensional systems where the number of attack surfaces increases exponentially. As systems grow in complexity, featuring more sensors, actuators, communication links, and interdependent components, the number of potential points of failure or vulnerability expands. In such settings, it is increasingly plausible for multiple anomalies to occur simultaneously, due to coordinated cyber-attacks or cascading sensor faults. The challenge of accurate anomaly attribution is affected by this dimensionality; the residual space becomes more intricate, and the overlap between fault and attack-induced signatures becomes harder to delineate. Therefore, scaling AD strategies to these more complex environments requires improved sensitivity and specificity and robust contextual reasoning capable of interpreting anomaly behaviour across multiple dimensions and agents.

5.4 Impact of Node Position on Attack Severity

In VPSs, the lead vehicle acts as the reference node by transmitting trajectory information to the following vehicles. Consequently, cyber-attacks targeting this transmitted data can directly compromise the first follower, potentially causing cascading disruptions throughout the platoon. As shown in (Kalogiannis et al., 2022), anomalies affecting Follower 1 can propagate through communication and control loops, amplifying spacing and velocity errors in downstream vehicles. This chain of reactions highlights a critical systemic vulnerability; the compromised integrity of a single upstream agent can destabilise the entire formation due to its role in coordination and synchronisation. From a resilience perspective, this highlights the importance of prioritised detection and protection mechanisms at the lead vehicle. Given that the platoon's overall stability can be greatly influenced by Follower 1's behaviour, resilience-enhancing strategies should be taken specifically on this node. Ultimately, ensuring system resilience is not solely a matter of global detection coverage but also of strategically identifying and fortifying high-impact nodes. Beyond this immediate risk, several broader system design implications emerge that can further enhance resilience in cooperative platooning. One critical consideration is the need to avoid rigid, single-point dependencies by enabling dynamic role reassignment such that if the first following vehicle exhibits anomalous behaviour or fails, another agent within the platoon can assume leadership.

Additionally, rather than treating the information as fully trusted, trust-aware coordination can be employed wherein follower vehicles continuously evaluate the reliability of received signals based on behavioural consistency, local sensing, or consensus with peer vehicles (Hermann et al., 2024). This highlights that resilience in vehicular platoons is not solely about detecting anomalies but about building architectural flexibility, distributed intelligence, and adaptive response capabilities into the system, particularly around critical nodes like that of the lead vehicle.

5.5 Necessity of Multi-Vector Attack Detection Multi Attack Detection is Critical

While the detection framework demonstrated commendable performance under isolated threat conditions, the results clearly reveal that the introduction of additional or unforeseen attack types, especially those for which the detector is not adequately trained, can naturally degrade accuracy and lead to system failure. In Tables 4–6, the simultaneous presence of FDI and sensor faults led to variations in the F1 score, indicating that multi-source disturbances introduced some sort of ambiguity within the classification. This points to a broader concern, as the number of attack surfaces and simultaneous anomalies increases, detection models trained on singular or simplified attack conditions may not generalise well. Such limitations, where misclassification of an attack or falsely flagging normal behaviour can have cascading effects. Therefore, multi-class and multi-modal attack detection becomes essential as we scale toward more complex, real-world environments (Bogdoll et al., 2024). These scenarios often involve blended disruptions, adaptive attack strategies, and variable system contexts. From a resilience perspective, this means detection mechanisms must evolve beyond binary classification or unimodal thresholds. Instead, systems must integrate context-aware, compositional detection architectures that can distinguish overlapping threats, assign confidence levels, and adapt to operational modes (Chen, Shin, & Dadras, 2024). Failing to do so may result in partial situational awareness, delayed containment, and ultimately, reduced resilience under compound stress conditions.

5.6 Transitioning from Detection to Recovery

Accurate and timely detection is critical for CPS resilience, as it is one of the major steps in the resilience cycle. Recovery, the process of returning to nominal behaviour after an anomaly, represents a distinct phase in the cycle. System resilience must therefore include detection and isolation and the speed and effectiveness of re-stabilisation mechanisms. Recovery effectiveness can be quantified using metrics like mean time to recovery (MTTR), which reflects how quickly a system returns to safe and stable operation. In vehicular platooning, prolonged recovery even after accurate anomaly detection can lead to spacing inconsistencies, control jitter, or unnecessary disengagement of automated driving features (Zhu et al., 2023). As such, a truly resilient system must be engineered with recovery in mind. Several additional factors influence this recovery process. One is the availability of fallback mechanisms such as adaptive cruise control, local relative sensing, or degraded control modes that allow the system to maintain safe operation during re-stabilisation. Another is the coordination of recovery across agents, particularly in multi-vehicle systems where unilateral recovery may lead to misaligned behaviour. In this context, graceful degradation becomes a key design goal, rather than full system shutdowns; resilience can be preserved by transitioning to lower-risk operational states.

Lastly, recovery strategies should incorporate learning from past anomalies (Nelson et al., 2025). Logging FPs and FNs along with associated recovery durations and conditions enables future predictive calibration. Systems equipped with self-healing logic are better able to adapt to evolving threats and unforeseen disturbances. Including recovery metrics such as post-anomaly overshoot, damping rate, and control effort in system evaluation frameworks also provides a more complete picture of resilience. Ultimately, embedding recovery as a core design objective enhances robustness and long-term reliability and safety in complex, cyber-physical environments.

5.7 Context Matters in Detection

Operational context significantly influences the effectiveness and consequences of AD. Detection sensitivity varies with factors like vehicle speed, environmental conditions, and traffic density. In platooning where vehicles

travel at high speeds, anomalies such as sensor faults or cyber-attacks may trigger quicker detection due to the generation of prominent system deviations. However, the same anomalies can cause more severe consequences, including amplified spacing errors or instability, making timely and context-aware detection even more critical. For instance, an FDI attack or sensor drift that might be benign or tolerable during lower speeds can result in severe effects at higher speeds, where reaction time is reduced and safety margins are tighter. This reveals that detection thresholds, filtering algorithms, and control logic should have the ability to be adaptive based on real-time operational context, whether the system is accelerating, cruising, or decelerating (Park, 2024). Context-aware detection frameworks, which adjust their sensitivity and response logic based on situational parameters, offer a promising direction to enhance resilience and reduce false alarms without compromising responsiveness under critical conditions.

Building upon this, context-aware systems can further enhance resilience by leveraging historical data to establish behavioural baselines under varying conditions. Through continuous learning, these systems can more accurately distinguish between legitimate operational deviations and anomalies. For instance, temporary spikes in acceleration might be expected during overtaking manoeuvres, whereas similar patterns during steady-state cruising could signal a potential fault or cyber intrusion. Integrating contextual cues from both internal states and external indicators into the detection logic allows for more accurate decision-making. This is crucial in reducing both FPs and FNs, ultimately contributing to safer and more reliable VCPS performance. To extend this further, context-awareness should not be limited to immediate driving behaviour but should also encompass higher-level contextual dimensions such as temporal patterns, spatial location, and mission-critical priorities. Temporal intelligence allows detection systems to align expectations with the system's operational phase. When external signals are incorporated into the detection process, they enrich the model's ability to interpret observed behaviour in its proper context (CAR 2 CAR Communication Consortium, 2021). Ultimately, embedding contextual adaptability into anomaly detection frameworks is fundamental to delivering resilient, trustworthy CPS performance in dynamic and uncertain real-world environments.

5.8 Temporal Vulnerability Zones

The concept of temporal vulnerability zones highlights that not all moments within a system's operational timeline carry equal risk. Figure 4 illustrates FDI attacks during acceleration phases; consequently, this can create a destabilising effect on system operation when compared to time zones with cruising velocities. During acceleration, vehicular systems operate under dynamic transitions, creating a narrower tolerance for external disturbances. In contrast, cruising phases generally involve steadier trajectories and more predictable responses, offering an inherent buffer against anomalies. Recognising these windows of heightened susceptibility allows for more strategic and efficient allocation of detection and mitigation resources. From a resilience standpoint, this supports the development of systems capable of dynamically elevating anomaly detection sensitivity during high-risk transitions such as acceleration, deceleration, or lane merging. Moreover, embedding awareness of temporal vulnerability zones into predictive control models (Bonzanini, Mesbah, & Di Cairano, 2024) and adaptive alert scheduling mechanisms allows the system to anticipate potential disruptions rather than merely react to them. This enhances resilience by minimising disturbance propagation, reducing response latency, and supporting quicker containment and recovery. Ultimately, incorporating temporal intelligence into anomaly detection frameworks transforms resilience from a reactive safeguard into a situationally aware, anticipatory capability optimised to protect the system precisely when it is most exposed to risk.

5.9 Model Transferability

Model transferability is a foundational aspect of resilience in CPSs (Sajjadi, Dinmohammadi, & Shafiee, 2025), especially in vehicular platooning where dynamic environmental changes are frequent. While the trained models demonstrate strong performance under the conditions they were developed and tested on, their effectiveness may significantly decline when exposed to unfamiliar or unanticipated scenarios. In real-world deployments, vehicles encounter a diverse range of operational states, such as varying road gradients, speed zones, any of which can

change the underlying data distribution and undermine detection accuracy if not properly accounted for during training. This limitation in transferability directly undermines the resilience of CPS, as it prevents systems from maintaining high detection accuracy when exposed to novel conditions. From a resilience perspective, adaptability is essential. Systems must be capable of not just identifying anomalies under known conditions but also responding effectively when entering previously unseen environments. The inability to do so can lead to a surge in FNs and FPs, or, more dangerously, complete system failure. To enhance resilience, modern detection frameworks must integrate continuous learning, domain adaptation, or transfer learning techniques (Rajapaksha et al., 2023). These strategies enable models to update themselves using new data encountered during operation or leverage knowledge from related domains to maintain robustness. Integrating such flexibility into detection architectures, systems can better absorb shocks, operate effectively across changing conditions, and ensure sustained safety and reliability for resilient CPS design.

5.10 Back Up or Safe Mode Needed

As shown in the referenced simulations, even after an anomaly is correctly identified, the system's ability to maintain operational continuity depends on what actions are taken next. Without a built-in fallback mechanism or safe mode controller, the system may still collapse or require manual intervention, which undermines the very purpose of autonomous resilience (Liu & Wang, 2021). A safe mode acts as a protective layer that the system defaults to when anomalies are detected, ensuring that core safety parameters are upheld regardless of anomaly type or severity. Designing for fail-operational behaviour, resilient VCPS architectures increasingly incorporate fail-operational control schemes that allow vehicles to continue functioning under degraded conditions. These may include pre-programmed emergency behaviours, redundant control logic, or switching to more conservative control parameters post-anomaly. Thus, integrating fallback control systems is essential to transition from anomaly aware to resilient.

5.11 Need for Strategic Policy Implementation

The need for robust policy is evident as cyber-physical resilience encompasses technical concerns requiring strategic regulation for low-resource SIDS. Under constraints of infrastructure fragility and limited redundancy, this amplifies the impact of disruptions, detection latency, containment delay, and recovery duration metrics, which can serve as actionable indicators that need to be monitored and enforced. These metrics allow transport authorities and mobility regulators to assess system robustness quantitatively, supporting informed investment, risk assessment, and incident preparedness planning. For example, a resilience audit framework built on these indicators could be used to grade readiness across vehicle fleets, evaluate vendors' control systems, or mandate minimal safety performance under anomalous conditions. Strategic policies will need to define minimum performance thresholds and outline enforcement measures for performance metrics or require built-in fallback mechanisms for certified autonomous platforms. In SIDS, where infrastructure investment must be prioritised carefully, embedding such metrics into procurement or regulatory standards ensures long-term system sustainability, reduces vulnerability to cyberattacks or faults, and promotes public confidence in intelligent transport deployments.

Conclusion

This study addressed a persistent gap in the CPS security literature where most work develops and benchmarks individual detection algorithms in scenario-specific settings but seldom explains how those results translate into resilience outcomes. Using an archetypal CPS tightly coupled to transportation critical infrastructure vehicle platooning, this work adopted evidence first approach, a representative supervised AD method was applied in a realistic case study, and the empirical results were used to produce a coherent set of AD-informed design considerations for CPS resilience. The contribution explicitly maps detection performance to resilience outcomes, consolidating insights usually scattered across separate publications into a single, operationally framed set of considerations to drive concrete CPS design choices. While not exhaustive, the set provides a concise guide to

what should be prioritised when integrating AD modules in CPS. These guidelines are particularly pertinent to SIDS, where thin operational buffers, intermittent connectivity, and longer restoration timelines can be further exacerbated if design considerations are not adequately addressed. This guidance can also aid engineers, operators, and policymakers in specifying, procuring, and deploying resilient CPS, especially in SIDS, moving the discussion from benchmark accuracy to maintained service, safe recovery, and sustained societal value.

References

- Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks. *Electronics*, 9(12), 2152. <https://doi.org/10.3390/electronics9122152>
- Alkahtani, H., & Aldhyani, T. H. H. (2021). Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms. *Complexity*, 2021(1), 5579851. <https://doi.org/10.1155/2021/5579851>
- Almasoud, A.S., Eisa, T.A.E., Al-Wesabi, F.N., Elsafi, A., Duhayyim, M.A., Yaseen, I., Hamza, M.A., Motwakel, A. (2022). Parkinson's Detection Using RNN-Graph-LSTM with Optimization Optimization Based on Speech Signals. *Computers, Materials and Continua*, 72(1), 871-886. <https://doi.org/10.32604/cmc.2022.024596>
- Alsaade, F. W., & Al-Adhaileh, M. H. (2023). Cyber Attack Detection for Self-Driving Vehicle Networks Using Deep Autoencoder Algorithms. *Sensors*, 23(8), 4086. <https://doi.org/10.3390/s23084086>
- Alsulami, A. A., Abu Al-Haija, Q., Alqahtani, A., & Alsini, R. (2022). Symmetrical Simulation Scheme for Anomaly Detection in Autonomous Vehicles Based on LSTM Model. *Symmetry*, 14(7), 1450. <https://doi.org/10.3390/sym14071450>
- Biddle, L., & Fallah, S. (2021). A Novel Fault Detection, Identification and Prediction Approach for Autonomous Vehicle Controllers Using SVM. *Automotive Innovation*, 4(3), 301-314. <https://doi.org/10.1007/s42154-021-00138-0>
- Bogdoll, D., Hamdard, I., Röbller, L. N., Geisler, F., Bayram, M., Wang, F., ... Zöllner, J. M. (2024, September 26). *AnoVox: A Benchmark for Multimodal Anomaly Detection in Autonomous Driving*. arXiv. <https://doi.org/10.48550/arXiv.2405.07865>
- Bonzanini, A. D., Mesbah, A., & Di Cairano, S. (2024). Perception-aware model predictive control for constrained control in unknown environments. *Automatica*, 160, 111418. <https://doi.org/10.1016/j.automatica.2023.111418>
- Brain, S., & Oyadeyi, O. (2023). Funding Crime Online: Cybercrime and its Links to Organized Crime in the Caribbean. *The Commonwealth Cybercrime Journal*, 1(3), 84-110.
- CAR 2 CAR Communication Consortium. (2021). *White Paper on Misbehaviour Detection and Reporting to Misbehaviour Authority*. CAR 2 CAR Communication Consortium.
- Check Point Team. (2024, July 16). Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks. Retrieved August 25, 2025, from Check Point Blog website: <https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/>
- Chen, C.-Y., Shin, K. G., & Dadras, S. (2024). Context-Aware Anomaly Detection Using Vehicle Dynamics. *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*, 531-545. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3678890.3678895>
- Cobos, E., & Diao, H. (2024, November 28). From fiction to reality: How Latin America became the world's most critical cyber battleground. Retrieved August 24, 2025, from World Bank Blogs website: <https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe>
- CrowdStrike. (2025). *2025 CrowdStrike Global Threat Report: China's Cyber Espionage Surges 150% with Increasingly Aggressive Tactics, Weaponization of AI-powered Deception Rises*. CrowdStrike. Retrieved from <https://ir.crowdstrike.com/node/14226/pdf>
- CSIS. (2025, May). Significant Cyber Incidents. Retrieved August 24, 2025, from <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

INSIGHTS INTO REGIONAL DEVELOPMENT

ISSN 2669-0195 (online) <https://jssidoi.org/ird/>

2025 Volume 7 Number 3 (September)

<http://doi.org/10.70132/p6489444663>

Fails, J. A., & Olsen, D. R. (2003). Interactive machine learning. *Proceedings of the 8th International Conference on Intelligent User Interfaces*, 39-45. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/604045.604056>

FortiGuard Labs. (2025). 2025 Global Threat Landscape Report. Retrieved from <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf>

Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J. (2017). *Framework for cyber-physical systems: Volume 2, working group reports* (No. NIST SP 1500-202; p. NIST SP 1500-202). Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.1500-202>

Guo, H., Sun, J., & Pang, Z.-H. (2023). Residual-Based False Data Injection Attacks Against Multi-Sensor Estimation Systems. *IEEE/CAA Journal of Automatica Sinica*, 10(5), 1181-1191. <https://doi.org/10.1109/JAS.2023.123441>

Hamza, M., Ben, S., Larabi-Marie-Sainte, S., Nour, M., Al-Wesabi, F., Motwakel, A., ... Duhayyim, M. (2022). Optimal Bidirectional LSTM for Modulation Signal Classification in Communication Systems. *Computers, Materials & Continua*, 72(2), 3055-3071. <https://doi.org/10.32604/cmc.2022.024490>

Hao, W., Yang, T., & Yang, Q. (2023). Hybrid Statistical-Machine Learning for Real-Time Anomaly Detection in Industrial Cyber-Physical Systems. *IEEE Transactions on Automation Science and Engineering*, 20(1), 32-46. <https://doi.org/10.1109/TASE.2021.3073396>

Haq, I. U., Khan, T. A., & Akhunzada, A. (2021). A Dynamic Robust DL-Based Model for Android Malware Detection. *IEEE Access*, 9, 74510-74521. <https://doi.org/10.1109/ACCESS.2021.3079370>

Hermann, A., Trkulja, N., Lucena, A. R. F. D., Kiening, A., Petrovska, A., & Kargl, F. (2024). WIP: A Trust Assessment Method for In-Vehicular Networks using Vehicle Risk Assessment. *Proceedings Symposium on Vehicle Security & Privacy*. Presented at the Symposium on Vehicle Security & Privacy, San Diego, CA, USA. San Diego, CA, USA: Internet Society. <https://doi.org/10.14722/vehiclesec.2024.23016>

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, 4(6), 1802-1831. <https://doi.org/10.1109/JIOT.2017.2703172>

Internet Crime Complaint Center. (2025). *Federal Bureau of Investigation's Internet Crime Report*. Federal Bureau of Investigation. Retrieved from Federal Bureau of Investigation website: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Kalogiannis, K., Khodaei, M., Bayaa, W. M. N. M., & Papadimitratos, P. (2022). Attack Impact and Misbehavior Detection in Vehicular Platoons. *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 45-59. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3507657.3528552>

Kaspersky Lab. (2025). *Threat landscape for industrial automation systems. Q1 2025*. Kaspersky Lab. Retrieved from <https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-Q1-2025-En.pdf>

Khalil, S. M., Bahsi, H., Dola, H. O., Korötko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems—A Case Study of a Microgrid System. *Computers & Security*, 124, 102950. <https://doi.org/10.1016/j.cose.2022.102950>

Khan, S., Sivaraman, E., & Honnavalli, P. B. (2020). Performance Evaluation of Advanced Machine Learning Algorithms for Network Intrusion Detection System. In M. Dutta, C. R. Krishna, R. Kumar, & M. Kalra (Eds.), *Proceedings of International Conference on IoT Inclusive Life (ICIL 2019), NITTTR Chandigarh, India* (pp. 51-59). Singapore: Springer. https://doi.org/10.1007/978-981-15-3020-3_6

Khraisat, A., Alazab, A., Singh, S., Jan, T., & Jr. Gomez, A. (2024). Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions. *ACM Comput. Surv.*, 57(1), 7:1-7:38. <https://doi.org/10.1145/3687124>

KnowBe4. (2024). *Cyber Attacks on Infrastructure: The New Geopolitical Weapon*. KnowBe4. Retrieved from https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf

Li, J., Yang, Y., Zhang, R., & Lee, Y. (2024, April 17). *Overconfident and Unconfident AI Hinder Human-AI Collaboration*. arXiv. <https://doi.org/10.48550/arXiv.2402.07632>

Liu, Y., & Wang, W. (2021). A Safety Reinforced Cooperative Adaptive Cruise Control Strategy Accounting for Dynamic Vehicle-to-Vehicle Communication Failure. *Sensors*, 21(18), 6158. <https://doi.org/10.3390/s21186158>

- Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. *Computers*, 12(4), 79. <https://doi.org/10.3390/computers12040079>
- Mohammed, A., Marine, L., Ramlal, C., & Muddeen, F. (2025). A Vehicular Cyber-Physical Framework for Studying the Effects of Multiple Disturbances with Application to Connected Autonomous Vehicles. *Transport and Telecommunication Journal*, 26(3), 250-265. <https://doi.org/10.2478/tjt-2025-0019>
- Mohammed, A., Ramlal, C., Marine, L., & Muddeen, F. (2024). Resilient Event Triggered Interval Type-2 Fuzzy Sliding Mode Control for Connected and Autonomous Vehicles Subjected to Multiple Cyber Attacks. *Journal of Advanced Transportation*, 2024(1), 2790548. <https://doi.org/10.1155/2024/2790548>
- Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (No. NIST SP 800-61r3; p. NIST SP 800-61r3). Gaithersburg, MD: National Institute of Standards and Technology (U.S.). <https://doi.org/10.6028/NIST.SP.800-61r3>
- Oucheikh, R., Fri, M., Fedouaki, F., & Hain, M. (2020). Deep Real-Time Anomaly Detection for Connected Autonomous Vehicles. *Procedia Computer Science*, 177, 456-461. <https://doi.org/10.1016/j.procs.2020.10.062>
- Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, 4(1), 8. <https://doi.org/10.1186/s42400-021-00071-z>
- Park, G. (2024). Optimal vehicle position estimation using adaptive unscented Kalman filter based on sensor fusion. *Mechatronics*, 99, 103144. <https://doi.org/10.1016/j.mechatronics.2024.103144>
- Positive Technologies. (2023, December 21). Cybersecurity threatscape for Latin America and the Caribbean: 2022–2023. Retrieved August 25, 2025, from Positive Technologies website: <https://global.ptsecurity.com/en/research/analytics/latam-cybersecurity-threatscape-2022-2023/#Navigation-6>
- Puig, V., Escobet, T., Sarrate, R., & Quevedo, J. (2016). Fault Detection and Isolation in Critical Infrastructure Systems. In C. G. Panayiotou, G. Ellinas, E. Kyriakides, & M. M. Polycarpou (Eds.), *Critical Information Infrastructures Security* (pp. 3-12). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-31664-2_1
- Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., & Madzudzo, G. (2023). Improving In-vehicle Networks Intrusion Detection Using On-Device Transfer Learning. *Proceedings Inaugural International Symposium on Vehicle Security & Privacy*. Presented at the Inaugural International Symposium on Vehicle Security & Privacy, San Diego, CA, USA. San Diego, CA, USA: Internet Society. <https://doi.org/10.14722/vehicsec.2023.23088>
- Rendall, K., Mylonas, A., Vidalis, S., & Gritzalis, D. (2025). MIDAS: Multi-layered attack detection architecture with decision optimization. *Computers & Security*, 148, 104154. <https://doi.org/10.1016/j.cose.2024.104154>
- Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, 23(8), 4060. <https://doi.org/10.3390/s23084060>
- Roh, H., Oh, S., Song, H., Han, J., & Lim, S. (2022). Deep Learning-based Wireless Signal Classification in the IoT Environment. *Computers, Materials & Continua*, 71(3), 5717–5732. <https://doi.org/10.32604/cmc.2022.024135>
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (No. NIST SP 800-160v2r1; p. NIST SP 800-160v2r1). Gaithersburg, MD: National Institute of Standards and Technology (U.S.). <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- Roy, T., & Dey, S. (2023, November 15). *On Distinguishability of Anomalies as Physical Faults or Actuation Cyberattacks*. arXiv. <https://doi.org/10.48550/arXiv.2311.09342>
- Sajjadi, P., Dinmohammadi, F., & Shafiee, M. (2025). Fault Detection of Cyber-Physical Systems Using a Transfer Learning Method Based on Pre-Trained Transformers. *Sensors (Basel, Switzerland)*, 25(13), 4164. <https://doi.org/10.3390/s25134164>
- Sarwar, A., Hasan, S., Khan, W. U., Ahmed, S., & Marwat, S. N. K. (2022). Design of an Advance Intrusion Detection System for IoT Networks. *2022 2nd International Conference on Artificial Intelligence (ICAI)*, 46-51. <https://doi.org/10.1109/ICAI55435.2022.9773747>

Schaberreiter, T., Andriessen, J., Cappiello, C., Papanikolaou, A., & Pardijs, M. (2024). Human-in-the-loop Anomaly Detection and Contextual Intelligence for Enhancing Cybersecurity Management. In R. Mitkov, S. Ezzini, T. Ranasinghe, I. Ezeani, N. Khallaf, C. Acarturk, ... P. Rayson (Eds.), *Proceedings of the First International Conference on Natural Language Processing and Artificial Intelligence for Cyber Security* (pp. 127-136). Lancaster, UK: International Conference on Natural Language Processing and Artificial Intelligence for Cyber Security. Retrieved from <https://aclanthology.org/2024.nlpaics-1.15/>

Song, Y., Hyun, S., & Cheong, Y.-G. (2021). Analysis of Autoencoders for Network Intrusion Detection. *Sensors*, 21(13), 4294. <https://doi.org/10.3390/s21134294>

UNDP. (2022). *United Nations Development Programme Digital Strategy 2022-2025*. Retrieved from https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-Full-Document_ENG_Interactive.pdf

Yang, T., Murguia, C., & Lv, C. (2023). Risk Assessment for Connected Vehicles Under Stealthy Attacks on Vehicle-to-Vehicle Networks. *IEEE Transactions on Intelligent Transportation Systems*, 24(12), 13627-13638. <https://doi.org/10.1109/TITS.2023.3292188>

Zhu, X., Shen, Y., Zhang, Z., & Yan, M. (2023). Stability Analysis of the Vehicular Platoon with Sensing Delay and Communication Delay: CTCR Paradigm via Dixon Resultant. *Applied Sciences*, 13(21), 11807. <https://doi.org/10.3390/app132111807>

Author Contributions: Conceptualization: *Amir Mohammed, Daniel Goitia*; methodology: *Amir Mohammed, Daniel Goitia, Sheikh Ahad Ahmad and Craig Ramlal*; data analysis: *Amir Mohammed, Daniel Goitia, Sheikh Ahad Ahmad*, writing original draft preparation: *Amir Mohammed, Daniel Goitia, Craig Ramlal* writing; review and editing: *Craig Ramlal, Sheikh Ahad Ahmad*; visualization: *Amir Mohammed, Daniel Goitia*. All authors have read and agreed to the published version of the manuscript.

Amir MOHAMMED is a PhD Student at the University of the West Indies. B.Sc.(e) in Electrical and Computer Engineering and MAsc in Electrical and Computer Engineering from the University of the West Indies. Research interests include Fuzzy Systems, Resilient Control, Artificial Intelligence and Cyber Physical Systems.

ORCID ID: <https://orcid.org/0000-0001-9420-1601>

Daniel GOITIA is a PhD candidate in the Department of Electrical and Computer Engineering at The University of the West Indies (UWI), St. Augustine. His research interests focus on wireless communication, with emphasis on 6G networks, the Internet of Things (IoT), and cybersecurity. He is passionate about advancing secure, efficient, and scalable communication technologies for the future digital landscape.

ORCID ID: <https://orcid.org/0009-0001-6737-9567>

Sheikh AHMAD is a SCADA Supervisor in the municipal water and wastewater industry in Ontario, Canada with a M.Eng. in Electrical and Computer Engineering specializing in Robotics and Controls from Western University, London, Ontario, Canada. Research interests include Industrial SCADA/Automation and Operational Technology Cyber Security.

ORCID ID: <https://orcid.org/0009-0003-7983-0292>

Craig RAMLAL is the Executive Director of the Artificial Intelligence Innovation Centre (AIIC), at the UWI and the Head of the Control Systems Group in the Department of Electrical and Computer Engineering, Faculty of Engineering, at the University of the West Indies, St. Augustine.

ORCID ID: <https://orcid.org/0000-0002-0960-528X>

This is peer-reviewed scientific journal <https://jssidoi.org/ird/page/peer-review-policy>

Copyright © 2025 by author(s). Publishing rights by UAB Sustainability for Regions
This work is licensed under the Creative Commons Attribution International License (CC BY).
<http://creativecommons.org/licenses/by/4.0/>

