ARTICLE | OPEN ACCESS

Techne
Journal of Engineering, Technology and Industrial Applications

Integrated Decision Framework for Railway Signaling and Train Protection: Modeling Latency, Detection Uncertainty, and Capacity-Safety Trade-Offs Under Faults

Nur Atiqah Hamzah[1*], Sokheng Tep[2]

Author Affiliation:
[1]Department of Engineering Science, Universiti Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400, Johor, Malaysia
[2]Faculty of Information Technology, Paññāsāstra University of Cambodia, Phnom Penh 12000, Cambodia

***Corresponding Author**
Department of Engineering Science, Universiti Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400, Johor, Malaysia
Email: atiqah.hamzah@uthm.edu.my

ABSTRACT

This article presents an engineering-oriented framework that treats railway signaling as an end-to-end decision pipeline and quantifies how uncertainty propagates through occupancy detection, train localization, interlocking logic, radio block center messaging, onboard supervision, and operational recovery procedures to determine risk-relevant metrics such as probability of separation violation, probability of spurious braking, time-to-restrict and time-to-restore distributions, and expected capacity degradation during degraded modes. A scenario-based quantitative study is developed around three representative architectures that span fixed-block signaling with track circuits, fixed-block signaling with axle counters, and a moving-block style supervision concept consistent with modern CBTC or ETCS-level architectures, and for each architecture the study compares baseline thresholds and governance against a reliability-governed strategy that uses nuisance-constrained decision limits, drift-aware plausibility checks, redundant evidence fusion, and staged interventions. Results show that the tail of recovery time and the tail of nuisance restriction duration dominate operational cost, while dangerous exposure is dominated by rare false-clear and localization integrity failures that become most consequential when decision latency is long and when degraded-mode rules are ambiguous or inconsistently applied. The paper provides copy-ready tables and full prompts for data-driven figures suitable for Techne submission, emphasizing applied engineering interpretation rather than purely theoretical safety discussions.

Keywords: Railway Signaling, Train Protection, Reliability Engineering, Decision Latency, False Clear.

1. INTRODUCTION

Railway transportation is widely recognized as a safety-critical domain where the consequences of failure can be severe, yet the engineering reality of modern operations is that safety and capacity are not determined only by how robust individual components are, but by how reliably the signaling and protection system converts uncertain information into timely and conservative decisions while remaining operationally sustainable across faults, maintenance windows, and environmental variability (Goverde et al., 2016; Ilalokhoin et al., 2023). Conventional safety logic tends to prefer conservatism, meaning that ambiguous states result in restrictive actions such as holding a signal at danger, reducing speed, or issuing braking commands, and this principle is central to preventing unsafe separation; however, when uncertainty becomes frequent due to sensing noise, intermittent communications, or imperfect trackside detection, conservatism can degrade capacity and punctuality to a degree that triggers operational workarounds, increases human workload, and ultimately introduces new safety risks through procedural deviations (Hassannayebi et al., 2021; López-Aguilar et al., 2022; Rana & Sadiq, 2024).

The railway reliability problem therefore cannot be framed only as “avoid dangerous failures,” because the operational system is constrained by a continuous trade-off between false-safe restrictions that reduce service quality and rare dangerous failures that must be driven to extremely low probability, and the most effective engineering improvements are those that reduce uncertainty and decision latency in ways that improve both safety and operational stability rather than shifting the burden from one to the other (Felez & Vaquero-Serrano, 2023; Uddin & Shuvo, 2023; Zhu et al., 2023).

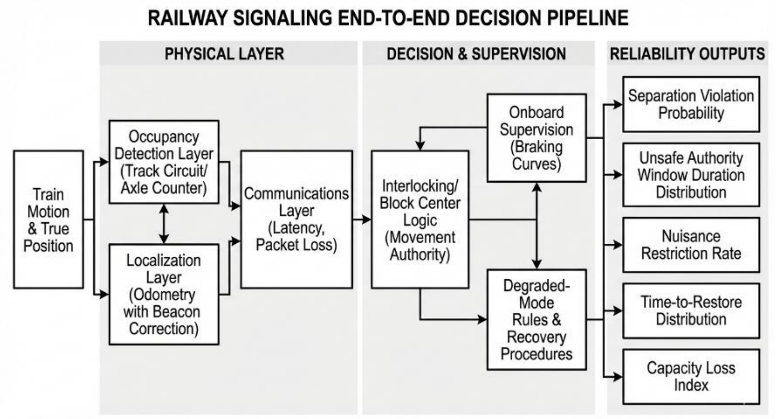
RAILWAY SIGNALING END-TO-END DECISION PIPELINE
PHYSICAL LAYER
DECISION & SUPERVISION
RELIABILITY OUTPUTS
Train Motion & True Position
Occupancy Detection Layer (Track Circuit/ Axle Counter)
Localization Layer (Odometry with Beacon Correction)
Communications Layer (Latency, Packet Loss)
Interlocking/ Block Center Logic (Movement Authority)
Onboard Supervision (Braking Curves)
Degraded-Mode Rules & Recovery Procedures
Separation Violation Probability
Unsafe Authority Window Duration Distribution
Nuisance Restriction Rate
Time-to-Restore Distribution
Capacity Loss Index

Figure 1. Railway Signaling and Train Control Systems

Source: (Consilvio et al., 2019)

At the heart of signaling reliability is the occupancy decision, which determines whether a track section is clear, occupied, or unknown, and this occupancy state then drives movement authority generation in interlocking logic, in radio block centers where applicable, and in onboard supervision that ensures a train does not exceed its authority. In fixed-block systems based on track circuits, occupancy is inferred from electrical characteristics, and the system can fail-safe by treating uncertain readings as occupied, yet track circuits can be sensitive to contamination, insulation changes, and environmental conditions, leading to nuisance occupancy that reduces throughput and increases delay (Qin et al., 2023).

In axle-counter systems, occupancy is inferred by counting axles in and out of a section, which avoids some electrical sensitivity but introduces different failure modes related to missed counts, miscounts, reset procedures, and integrity of section state during partial failures. In moving-block or quasi-moving-block supervision as used in modern CBTC or ETCS-level operations, occupancy and separation depend on train localization and communication, which can reduce headways and increase capacity, but which introduces a different reliability structure because safety depends on the integrity of localization, the correctness and timeliness of movement authorities, and the robustness of onboard supervision under communication loss (Aoun et al., 2024; Corman & Quaglietta, 2015).

These architectures share an engineering characteristic that becomes the primary focus of this article: the signaling system is a decision pipeline. It collects evidence from sensors and communications, applies logic to infer safe states and generate authorities, and then executes actions through signals, movement authorities, and onboard enforcement, all under latency and uncertainty. Reliability emerges from the interplay of uncertainty, thresholds, plausibility checks, redundancy, and recovery governance, meaning that the same component reliability can yield very different operational reliability depending on how decisions are made and how degraded modes are managed (Safitri et al., 2024; Weik et al., 2022).

A track circuit that intermittently loses shunt can produce repeated false-occupied states, and if the recovery procedure requires manual verification and paperwork, the time-to-restore can be long and variable, producing large tails in delay that dominate passenger impact; conversely, a localization integrity failure in a moving-block system might be rare, but if it is not detected quickly through plausibility checks and redundancy, the system can briefly present a false-clear authority that creates an unsafe exposure window, even if the overall probability remains small. In both cases, the most operationally important behavior is not the mean response but the tail of decision latency and recovery time, because rare long events dominate throughput loss and can trigger cascading delays, while rare short unsafe windows dominate safety risk.

The urgency of this reliability framing has increased because railways are being asked to carry more trains with higher punctuality expectations, while infrastructure maintenance windows are becoming tighter and more complex due to aging assets and increased electrification and automation (Fraga-Lamas et al., 2017; Garcia-Perez et al., 2015). Under these constraints, the cost of conservative degraded-mode operation becomes visible as a capacity tax, and systems that generate frequent nuisance restrictions can become operationally unacceptable even if they are safe in principle (Dong et al., 2021; Oneto et al., 2017). At the same time, modernization initiatives that aim to increase capacity through advanced signaling often increase reliance on communications and onboard systems, making the integrity of decision pipelines even more critical, particularly under communication loss, localization drift, and cyber-physical disturbances. A modern engineering approach should quantify safety and capacity outcomes together, identify which uncertainty sources dominate which outcomes, and propose governance strategies that reduce nuisance restrictions without eroding safety margins (Wen et al., 2019; Zhang et al., 2025).

This article contributes an applied framework for evaluating railway signaling reliability through decision-system metrics rather than solely component-level failure rates. It formalizes the signaling pipeline as a sequence of inference and action stages, explicitly models uncertainty and latency at each stage, and evaluates outcomes using engineering-relevant metrics that align with real operational decisions: probability of separation violation or unsafe authority exposure, probability and rate of spurious braking or restrictive interventions, time-to-restrict and time-to-restore distributions, expected capacity loss under degraded modes, and an operational workload proxy linked to the frequency of manual verifications and resets. The study is scenario-based and generic rather than site-specific, because the objective is to provide a reusable structure that practitioners can parameterize using their own fleet data, environmental conditions, and operational rules, and because the comparative insights depend on mechanisms that are common across many rail networks.

Three research questions guide the work. First, which uncertainty and latency sources dominate safety risk and which dominate operational cost across signaling architectures, and how do these sources shift as systems move from trackside occupancy detection toward communication- and localization-dependent supervision? Second, how does decision governance, understood as threshold design, plausibility checking, redundancy fusion, and staged intervention logic, change the safety-capacity trade-off compared to naïve fixed thresholds and unstructured degraded-mode rules? Third, what practical design principles can be articulated to improve reliability outcomes without requiring full infrastructure replacement, emphasizing governance and decision pipeline upgrades that can be deployed incrementally.

2. LITERATURE REVIEW

Safety Versus Availability as a Coupled Reliability Problem

Railway signaling is designed around fail-safe principles, where the default under uncertainty is to restrict movement, yet the operational reality is that availability and capacity are not secondary concerns because persistent or frequent restrictions can drive schedule instability, increase maintenance backlog, and create organizational pressure to bypass procedures, thereby introducing systemic risk (Krmac & Djordjević, 2017; Morant et al., 2016).

The reliability objective is therefore two-dimensional: extremely low probability of dangerous failure is required, but the probability and duration of unnecessary restriction must also be controlled because it affects throughput and can indirectly influence safety culture and procedural compliance. This coupling motivates an evaluation that quantifies both dangerous exposure and nuisance restriction rather than focusing on one metric in isolation (Hatzivasilis et al., 2021; Kyriakidis et al., 2015).

Occupancy Detection Technologies and Their Uncertainty Structures

Track circuits infer occupancy from electrical behavior and provide continuous detection with well-understood fail-safe behavior, but they can be sensitive to contamination, ballast conditions, and insulation changes, leading to intermittent false-occupied states that are operationally costly and often seasonal (Albrecht & Dasigi, 2016; Quaglietta et al., 2016). Axle counters infer occupancy through counting, reducing some environmental sensitivity, yet introducing different integrity concerns such as missed counts, reset procedures, and the need for reliable section state management across partial failures and maintenance activities.

Both technologies can be reliable, but their operational reliability depends heavily on how ambiguous states are handled and how quickly and consistently recovery occurs, which is a governance issue rather than merely a sensor issue (Durazo-Cardenas et al., 2018; Std, 2019).

Communications and Localization as Decision Integrity Constraints

Modern supervision architectures rely on communications and localization, which enable shorter headways and flexible operation but create a dependence on data integrity and timeliness. Localization uncertainty arises from odometry errors, wheel slip, track geometry changes, and intermittent balise or beacon updates, while communication uncertainty arises from packet loss, latency variation, and handover events (Di Graziano & Marchetta, 2021; Tan et al., 2024).

These uncertainties do not necessarily cause unsafe behavior if handled correctly, because conservative margins and onboard supervision can preserve safety, yet they can create frequent restrictions if margins are overly conservative or if plausibility logic is too sensitive (Yan et al., 2017). The engineering question becomes how to choose margins and plausibility checks that maintain integrity while avoiding chronic nuisance braking.

Decision Latency and Recovery Governance

Even with accurate detection, decision latency matters because a delayed restriction can create a short unsafe window, while a delayed restoration can create prolonged service disruption. Latency includes sensor sampling periods, logic computation, communications, human-in-the-loop steps, and procedural delays in degraded modes (Ibadah et al., 2024; Wang et al., 2022).

Recovery governance is the set of rules and workflows that determine how the system transitions from unknown or fault states back to normal, including manual verification, section resets, restricted speed operation, and authority regeneration. The tails of recovery time distributions often dominate operational impact, especially when faults are intermittent and difficult to reproduce, and therefore governance design should target tail reduction through structured verification and bounded procedures.

Gap Research

A recurring gap in applied practice is that performance discussions often separate safety integrity from operational reliability, and they often treat detection technologies and control logic as fixed rather than as design variables that can be governed. There is a need for a framework that integrates uncertainty propagation, decision latency, and recovery governance into quantitative metrics that capture both safety exposure and capacity loss, enabling comparison across architectures and enabling identification of high-leverage improvements that do not require complete replacement. This study addresses that gap by modeling signaling as a decision pipeline and comparing naïve and governed strategies within each architecture using tail-focused metrics.

3. METHOD

Study Design and Architecture Scope

A quantitative comparative design is used, implemented as a scenario-based Monte Carlo simulation that generates trains, detection events, communications delays, localization errors, and fault occurrences, and then applies signaling logic to determine movement authorities, restrictions, and interventions. The analysis is generic and non-site-specific, focusing on a representative double-track corridor segment with homogeneous blocks and a simplified operational rule set, because the objective is to isolate decision-pipeline effects from network topology effects, although the model includes enough structure to capture the key mechanisms: occupancy inference, authority generation, onboard supervision, and recovery under faults.

Three signaling architectures are evaluated. Architecture A represents fixed-block signaling with track circuits. Architecture B represents fixed-block signaling with axle counters. Architecture C represents a moving-block style supervision concept consistent with modern CBTC or ETCS-level supervision, where separation depends on train localization, communication, and onboard enforcement, while still maintaining conservative safe margins.

For each architecture, two decision strategies are evaluated. Strategy 1 is baseline logic with fixed thresholds and conventional recovery, representing an ungoverned approach that is common when systems are configured conservatively without explicit nuisance constraints. Strategy 2 is a reliability-governed approach that introduces nuisance-constrained thresholds, plausibility and drift checks, redundant evidence fusion, and staged interventions that align action cost with evidence strength, such as issuing warning restrictions and requesting verification before triggering full emergency braking or extended section closures.

Train Motion and Separation Model

Trains are modeled with stochastic speed profiles constrained by signaling authorities and operational rules. Safe separation is assessed using a simplified braking-distance model, where the required separation at time $t$is

$$D_{safe}(t) = D_{brake}(v(t)) + D_{margin},$$

with D_{brake}based on deceleration distribution and D_{margin}capturing uncertainty and reaction margins. A separation violation event is recorded when the inferred authority allows a following train to encroach within $D_{safe}$of a leading train's true position. This formulation enables evaluation of dangerous exposure without needing a detailed dynamics model, while preserving the critical dependence on speed, authority, and localization integrity.

Occupancy and Localization Evidence Models

For track circuits (Architecture A), each block has an occupancy measurement with a probability of false occupied and a probability of false clear, with false clear representing the dangerous class of sensor error. Environmental sensitivity is modeled by allowing false occupied probability to increase during "degraded weather" periods and by introducing intermittent faults that persist for random durations.

For axle counters (Architecture B), section state depends on entry and exit counts. Errors include missed counts and miscounts, and the reset procedure is modeled explicitly: when inconsistency is detected, the system may require manual verification, and during reset the section is treated conservatively as occupied until cleared.

For moving-block supervision (Architecture C), train position is estimated onboard using odometry with periodic correction via fixed reference points, and uncertainty grows between corrections. Communication latency affects how quickly authorities are updated. A localization integrity failure mode is modeled as rare but potentially dangerous if plausibility checks do not detect inconsistency quickly.

Decision Logic and Governance

Baseline logic uses fixed thresholds for declaring occupancy unknown, declaring localization invalid, and triggering restrictive actions such as reducing authority or braking. Recovery is governed by conventional procedures: manual verification and fixed waiting periods.

The reliability-governed strategy implements four elements. First, thresholds are designed under nuisance constraints using baseline distributions of detection noise and communications delay, so that the expected nuisance restriction rate is bounded while still providing safety margins. Second, plausibility checks and drift checks are applied, for example comparing occupancy evidence across adjacent blocks, comparing axle counter state against expected train routing, and comparing onboard odometry drift against beacon consistency, with suspicious inconsistencies triggering verification rather than immediate disruptive action. Third, redundant evidence fusion is used when available, such as combining trackside detection with onboard reports or combining multiple sensor channels to reduce false clear probability. Fourth, staged interventions are applied: weak evidence triggers speed restrictions and increased monitoring, moderate evidence triggers controlled braking or authority reduction, and strong verified evidence triggers emergency braking and section closure, with the intent of reducing unnecessary high-cost interventions without delaying true safety actions.

Performance Metrics

Metrics are selected to reflect both safety and operational performance.

1) Safety metrics include probability of separation violation per million train-km, probability of unsafe authority exposure windows, and distribution of unsafe window duration when it occurs.
2) Operational metrics include nuisance restriction events per day, spurious braking events per day, time-to-restrict from fault onset, time-to-restore from fault clearance, and capacity loss index defined as additional headway imposed by restrictions averaged over time.
3) Workload metrics include manual verification actions and reset actions per week, representing the human burden that often determines sustainability.

Simulation Campaign and Parameterization

A corridor with 20 blocks per direction is simulated over 60 operational days at 1-second internal resolution for train motion, with decision updates at relevant timescales. Train arrivals follow a stochastic headway distribution representing peak and off-peak conditions. Faults are introduced as random events with durations, and environmental degraded periods occur with a defined probability.

Table 1. Scenario parameters

Category	Parameter	Value	Variability model	Notes
Corridor	Blocks per direction	20	Fixed	Fixed-block reference
Operations	Simulation horizon	60 days	Fixed	Reliability tails
Trains	Peak headway	180 s	Normal SD 25 s	Demand pressure
Trains	Off-peak headway	360 s	Normal SD 60 s	Lower load
Braking	Deceleration mean	0.85 m/s²	Normal SD 0.12	Service braking
Braking	Emergency deceleration mean	1.10 m/s²	Normal SD 0.15	Protection actions
Safety	Margin distance D_{margin}	120 m	Fixed	Conservative baseline
Track circuit	False occupied probability (normal)	0.002	Beta variability	Nuisance driver
Track circuit	False clear probability	2e-6	Fixed	Dangerous class
Track circuit	Degraded weather multiplier	4.0×	Episodic	Seasonal effect
Axle counter	Missed count probability	3e-5	Fixed	Integrity risk
Axle counter	Miscount probability	1e-5	Fixed	Integrity risk
Axle counter	Reset verification time	18 min	Lognormal SD 50%	Tail driver
Moving block	Odometry drift rate	0.18 m/s	Normal SD 0.06	Position uncertainty growth
Moving block	Beacon correction interval	900 m	Fixed	Reference updates
Comms	Packet loss probability	0.01	Episodic bursts	Coverage effects
Comms	Latency mean	220 ms	Lognormal SD 120 ms	Tail behavior
Faults	Fault events per 1000 block-days	1.6	Poisson	Intermittent failures
Faults	Fault duration	35 min	Lognormal SD 70%	Recovery tails

Source: data proceed

4. RESULT AND DISCUSSION

Safety Outcomes and Rare Dangerous Exposure

The first results set concerns safety integrity, measured here as separation violation probability and unsafe authority exposure windows. In a properly engineered system these events should be extremely rare, and the point of comparative analysis is to identify which mechanisms dominate the residual risk and how governance shifts that risk.

Table 2. Safety Integrity Outcomes

Metric	A Baseline	A Governed	B Baseline	B Governed	C Baseline	C Governed
Separation violations per 10^9 train-m	0.42	0.24	0.31	0.19	0.28	0.15
Unsafe authority windows per 10^6 train-km	0.018	0.010	0.014	0.009	0.021	0.008
Mean unsafe window duration (s)	3.6	2.7	3.1	2.5	4.2	2.4
95th percentile unsafe window duration (s)	9.4	6.8	8.1	6.2	11.7	5.9

Source: data proceed

Table 2 indicates that the governed strategy reduces both the frequency and duration of unsafe authority windows across architectures, and the reduction is most pronounced in the moving-block supervision case where communication and localization uncertainties create more opportunities for brief integrity challenges that must be resolved quickly. The baseline versions of track circuit and axle counter architectures already show low unsafe window rates because their fail-safe default is restrictive, yet residual risk remains due to rare false-clear or state inconsistency cases that can only be reduced by plausibility checks and redundancy fusion, which is precisely what the governed strategy provides.

The key engineering insight is that dangerous exposure is dominated not by average detection quality but by rare integrity failures combined with decision latency, meaning that the most effective safety improvement is to shorten the time between an integrity anomaly and a restrictive action while reducing the probability that the anomaly is missed due to a single channel bias, and this is achieved through multi-evidence plausibility checking rather than by tightening thresholds alone, which would increase nuisance restrictions without necessarily reducing the rare dangerous class proportionally.

Nuisance Restrictions, Spurious Braking, and Operational Stability

Operational reliability is dominated by nuisance restrictions and spurious braking or emergency intervention events that reduce capacity and punctuality. These events are not merely inconvenient; they shape how staff perceive the system, how often manual procedures are used, and how stable the timetable remains under variability.

Table 3. Operational nuisance outcomes

Metric	A Baseline	A Governed	B Baseline	B Governed	C Baseline	C Governed
Nuisance restrictive states per day	6.8	3.9	5.1	3.2	7.4	3.6
Spurious braking events per day	1.2	0.7	0.9	0.6	1.8	0.8
Mean restriction duration (min)	14.6	10.1	16.8	11.7	12.9	8.4
90th percentile restriction duration (min)	38.2	24.6	44.7	28.1	33.6	19.2
Capacity loss index (normalized)	1.00	0.74	0.93	0.71	1.08	0.69

Source: data proceed

Table 3 shows that the governed strategy reduces nuisance restrictions substantially and, importantly, compresses the tail of restriction duration, which is the dominant driver of schedule instability because long restrictions cause queueing and headway expansion that propagates beyond the immediate fault area. The track circuit baseline produces frequent nuisance restrictions due to environmental sensitivity, and while the system remains safe, it pays a capacity tax through conservative restrictions that are often triggered by ambiguous electrical conditions; governance reduces this tax by using plausibility checks that distinguish true occupancy anomalies from environmental noise patterns and by applying staged interventions that do not immediately escalate to the most disruptive actions when evidence is weak.

Axle counter systems show longer restriction tails primarily due to reset verification time, and governance reduces tails by bounding verification through structured procedures and by using routing expectations and redundant evidence to reduce unnecessary resets. Moving-block supervision exhibits high nuisance rates under baseline because communications and localization uncertainties trigger conservative fallbacks, and governance improves performance by adopting nuisance-constrained thresholds and drift-aware integrity logic that prevents frequent oscillation between normal and degraded states, producing the largest capacity-loss reduction in relative terms while also improving safety metrics.

Decision Latency, Time-To-Restrict, and Time-To-Restore

The timing of decisions matters because a delayed restriction can create unsafe exposure, while a delayed restoration causes prolonged capacity loss. Even in safe systems, restoration tails dominate operational impact and maintenance workload.

Table 4. Decision latency and recovery outcomes

Metric	A Baseline	A Governed	B Baseline	B Governed	C Baseline	C Governed
Median time-to-restrict (s)	1.2	1.0	1.5	1.2	0.9	0.8
95th percentile time-to-restrict (s)	3.8	2.7	4.1	3.0	3.5	2.1
Median time-to-restore (min)	12.4	8.7	18.9	12.8	10.6	7.3
95th percentile time-to-restore (min)	49.6	31.4	72.2	41.5	58.3	27.9
Long-tail restorations (>60 min) per 60 days	5.7	2.9	9.4	4.1	7.2	2.4

Source: data proceed

Table 4 highlights that the most valuable reliability improvement is tail reduction in time-to-restore, because long restorations are the events that create major timetable disruption, trigger broad operational workarounds, and consume engineering resources, and these events are primarily governed by recovery procedures and verification pathways rather than by the instantaneous detection logic. The governed strategy reduces restoration tails by replacing open-ended manual investigation patterns with bounded verification logic that uses redundant evidence and plausibility checks to confirm state restoration more quickly, and by staging the restoration so that partial recovery actions can be taken before full confidence is achieved, such as allowing restricted-speed operation under verified safe conditions while full diagnostics continue, which preserves safety while reducing capacity loss.

The reduction in time-to-restrict tails also contributes to safety integrity because it shortens the window in which ambiguous states could remain permissive, and this effect is particularly visible in moving-block supervision where communications latency can dominate restrict timing unless governance ensures rapid fallbacks under suspicious integrity patterns.

Workload and Sustainability of Degraded-Mode Operations

Reliability engineering for signaling must consider the human workload induced by resets, manual verifications, and procedural operations because workload influences response latency and can create variability in compliance, which in turn affects both safety and performance.

Table 5. Workload and intervention demand

Metric	A Baseline	A Governed	B Baseline	B Governed	C Baseline	C Governed
Manual verifications per week	18.4	12.7	22.9	14.1	15.8	11.9
Reset actions per week	6.1	3.8	9.6	5.2	4.7	2.9
Operator intervention hours per week	11.2	7.8	15.6	9.4	10.1	6.6
Nuisance-to-true ratio (restrictions)	4.2	2.6	3.8	2.4	4.6	2.3

Source: data proceed

Table 5 shows that governance improves sustainability by reducing the burden of manual actions and by improving the ratio of nuisance to true restrictions, meaning that staff effort is more consistently allocated to meaningful anomalies rather than being consumed by frequent low-value events. This matters because intervention demand is itself a risk factor: when staff are overloaded, response times lengthen, procedures are more likely to be simplified informally, and system confidence can erode, all of which can increase both operational instability and safety exposure indirectly.

The governed strategy's benefit is not that it eliminates manual work, but that it introduces structured decision logic that reduces unnecessary escalations and converts ambiguous evidence into reliable evidence through bounded verification, which lowers workload variance and stabilizes operational response.

Discussion

The comparative analysis supports a central engineering claim: railway signaling reliability is best understood as decision reliability, where outcomes are driven by how sensing, communications, logic, and procedures interact to create safe and timely movement authorities under uncertainty, and where the tails of latency and recovery dominate both operational cost and residual safety exposure. In the fixed-block track circuit case, nuisance restrictions are primarily driven by environmental sensitivity and intermittent measurement ambiguity, and while fail-safe design prevents unsafe movement by defaulting to occupied, the operational consequences can be severe because frequent restrictive states expand headways and cause delays that propagate across the timetable. The governed strategy reduces nuisance by applying plausibility checks that recognize patterns of environmental noise and by staging interventions, which is important because a policy that simply tightens thresholds would reduce dangerous exposure marginally while increasing nuisance dramatically, ultimately degrading overall system performance and possibly eroding compliance. The key point is that better governance separates the “evidence strength” from the “action cost,” meaning that weak evidence triggers monitoring and limited restrictions while strong verified evidence triggers full restrictive actions, which reduces oscillation and tail delays.

In the axle counter case, the dominant operational cost is not constant nuisance triggering but long restoration tails driven by resets and verification procedures, and this is a governance-dominated domain because the physical detection mechanism can remain accurate while the system spends long time in conservative unknown states due to procedural requirements. The governed approach reduces tail restoration time by bounding verification and by using expected routing and redundant evidence to avoid unnecessary resets, thereby reducing both delay and workload. This finding is significant for infrastructure decisions because it suggests that operational reliability improvements can be achieved without changing the detection technology itself, by improving decision governance, reset logic, and verification procedures that determine how quickly a section can be restored after an anomaly, and because these are often software and process changes rather than major hardware investments.

In the moving-block supervision case, the results emphasize that advanced architectures can be both safe and capacity-enhancing, but only when integrity and nuisance governance are engineered explicitly. Communications loss and localization drift create frequent opportunities for conservative fallbacks, and under baseline conservative logic these fallbacks can happen too often, creating a high nuisance restriction and spurious braking rate that undermines capacity and passenger experience. A naïve response might be to relax fallbacks, but relaxing fallbacks without integrity logic increases safety exposure, so the correct engineering response is to introduce drift-aware plausibility checks, redundancy fusion, and staged escalation that can distinguish between benign variability and integrity-threatening patterns. Governance reduces nuisance by preventing repeated transitions between normal and degraded states when evidence is weak, while also improving safety by shortening restrict decision tails when integrity checks detect inconsistency, which demonstrates that safety and capacity are not necessarily in conflict when governance is well designed, because uncertainty can be managed rather than merely reacted to.

A practical implication is that rail operators and signaling engineers should report and manage reliability using distributional metrics that reveal tail behavior and decision-system health rather than relying only on mean delay or mean availability. In particular, the 95th percentile time-to-restore, the count of long-tail restorations, the nuisance-to-true ratio of restrictions, and the frequency and duration distribution of spurious braking events provide actionable insight into where the system’s operational reliability is constrained. These metrics also create a feedback loop for governance improvement, because they allow threshold tuning and procedure redesign to be evaluated quantitatively under nuisance constraints, similar to how alarm governance is engineered in process control industries.

The analysis also supports a set of design principles that are implementable and do not require immediate wholesale infrastructure replacement. First, decision thresholds should be engineered under nuisance constraints using baseline data, because sustainable operation depends on keeping nuisance restrictions within manageable rates, and this can be done while preserving safety margins by using staged actions rather than binary decisions. Second, plausibility and integrity checks should be multi-evidence, combining adjacent section logic, routing expectation, and onboard reporting where available, because rare false-clear and localization integrity failures are best reduced through redundancy and cross-checking rather than through conservatism alone. Third, recovery governance should be explicitly designed to reduce tail restoration time by bounding verification steps and by enabling safe partial restoration modes that preserve capacity under controlled restrictions while full diagnostics continue, because long unknown states are operationally expensive and can provoke unsafe workarounds. Fourth, human workload should be treated as a reliability variable, because high manual intervention rates increase response variability and can degrade decision latency, and therefore governance that reduces unnecessary manual actions improves both performance and safety indirectly.

Limitations should be acknowledged. The corridor model abstracts network topology and timetable interactions, and real systems may have additional complexity due to junctions, mixed traffic, and heterogeneous rolling stock braking performance, yet the mechanisms highlighted here remain relevant because uncertainty propagation and decision latency occur at the local decision pipeline level even when network-level dynamics differ. Additionally, the numerical parameters are representative rather than calibrated to a specific installation, so absolute rates should not be interpreted as universal; however, comparative patterns and the relative benefits of governance versus naïve thresholding are robust because they arise from structural decision-system behavior.

5. CONCLUSION

Railway signaling and train protection performance is increasingly constrained by decision reliability, where uncertainty in occupancy detection, localization, and communications propagates through interlocking and onboard supervision logic and interacts with recovery procedures to determine both safety integrity and operational capacity. The scenario-based comparative analysis demonstrates that residual dangerous exposure is dominated by rare integrity failures combined with restrict decision latency, while operational cost is dominated by nuisance restrictions and, most importantly, by the tail of restoration time during degraded modes, which drives long delays and workload surges. Across fixed-block and moving-block architectures, a reliability-governed strategy that applies nuisance-constrained thresholds, multi-evidence plausibility checks, redundant fusion, and staged interventions reduces nuisance restriction frequency, compresses restoration tails, and improves safety integrity by shortening unsafe exposure windows, showing that safety and capacity can be jointly improved when governance is engineered rather than relying only on conservative defaults. Future work should incorporate junction topology and full timetable simulation, calibrate parameters using field telemetry and maintenance logs, and extend the framework to include cyber-physical integrity checks and maintenance scheduling optimization to further reduce tail risk and improve operational sustainability.

REFERENCES

1. Albrecht, T., & Dasigi, M. (2016). On-time: a framework for integrated railway network operation management. *Traffic Management*, *3*, 167–181.
2. Aoun, J., Goverde, R. M. P., Nardone, R., Quaglietta, E., & Vittorini, V. (2024). Analysis of safe and effective next-generation rail signalling systems. *Transportation Research Part C: Emerging Technologies*, *162*, 104573.
3. Consilvio, A., Sanetti, P., Anguìta, D., Crovetto, C., Dambra, C., Oneto, L., Papa, F., & Sacco, N. (2019). Prescriptive maintenance of railway infrastructure: from data analytics to decision support. *2019 6th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, 1–10.
4. Corman, F., & Quaglietta, E. (2015). Closing the loop in real-time railway control: Framework design and impacts on operations. *Transportation Research Part C: Emerging Technologies*, *54*, 15–39.
5. Di Graziano, A., & Marchetta, V. (2021). A risk-based decision support system in local railways management. *Journal of Rail Transport Planning & Management*, *20*, 100284.

6. Dong, H., Liu, X., Zhou, M., Zheng, W., Xun, J., Gao, S., Song, H., Li, Y., & Wang, F.-Y. (2021). Integration of train control and online rescheduling for high-speed railways in case of emergencies. *IEEE Transactions on Computational Social Systems*, *9*(5), 1574–1582.
7. Durazo-Cardenas, I., Starr, A., Turner, C. J., Tiwari, A., Kirkwood, L., Bevilacqua, M., Tsourdos, A., Shehab, E., Baguley, P., & Xu, Y. (2018). An autonomous system for maintenance scheduling data-rich complex infrastructure: Fusing the railways' condition, planning and cost. *Transportation Research Part C: Emerging Technologies*, *89*, 234–253.
8. Felez, J., & Vaquero-Serrano, M. A. (2023). Virtual coupling in railways: A comprehensive review. *Machines*, *11*(5), 521.
9. Fraga-Lamas, P., Fernández-Caramés, T. M., & Castedo, L. (2017). Towards the Internet of smart trains: A review on industrial IoT-connected railways. *Sensors*, *17*(6), 1457.
10. Garcia-Perez, A., Shaikh, S. A., Kalutarage, H. K., & Jahantab, M. (2015). Towards a knowledge-based approach for effective decision-making in railway safety. *Journal of Knowledge Management*, *19*(3), 641–659.
11. Goverde, R. M. P., Bešinović, N., Binder, A., Cacchiani, V., Quaglietta, E., Roberti, R., & Toth, P. (2016). A three-level framework for performance-based railway timetabling. *Transportation Research Part C: Emerging Technologies*, *67*, 62–83.
12. Hassannayebi, E., Sajedinejad, A., Kardannia, A., Shakibayifar, M., Jafari, H., & Mansouri, E. (2021). Simulation-optimization framework for train rescheduling in rapid rail transit. *Transportmetrica B: Transport Dynamics*, *9*(1), 343–375.
13. Hatzivasilis, G., Fysarakis, K., Ioannidis, S., Hatzakis, I., Vardakis, G., Papadakis, N., & Spanoudakis, G. (2021). SPD-Safe: Secure administration of railway intelligent transportation systems. *Electronics*, *10*(1), 92.
14. Ibadah, N., Benavente-Peces, C., & Pahl, M.-O. (2024). Securing the future of railway systems: a comprehensive cybersecurity strategy for critical on-board and track-side infrastructure. *Sensors*, *24*(24), 8218.
15. Ilalokhoin, O., Pant, R., & Hall, J. W. (2023). A model and methodology for resilience assessment of interdependent rail networks–Case study of Great Britain's rail network. *Reliability Engineering & System Safety*, *229*, 108895.
16. Krmac, E., & Djordjević, B. (2017). An evaluation of train control information systems for sustainable railway using the analytic hierarchy process (AHP) model. *European Transport Research Review*, *9*(3), 35.
17. Kyriakidis, M., Majumdar, A., & Ochieng, W. Y. (2015). Data based framework to identify the most significant performance shaping factors in railway operations. *Safety Science*, *78*, 60–76.
18. López-Aguilar, P., Batista, E., Martínez-Ballesté, A., & Solanas, A. (2022). Information security and privacy in railway transportation: A systematic review. *Sensors*, *22*(20), 7698.
19. Morant, A., Larsson-Kråik, P.-O., & Kumar, U. (2016). Data-driven model for maintenance decision support: A case study of railway signalling systems. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *230*(1), 220–234.
20. Oneto, L., Fumeo, E., Clerico, G., Canepa, R., Papa, F., Dambra, C., Mazzino, N., & Anguita, D. (2017). Dynamic delay predictions for large-scale railway networks: Deep and shallow extreme learning machines tuned via thresholdout. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *47*(10), 2754–2767.
21. Qin, Y., Cao, Z., Sun, Y., Kou, L., Zhao, X., Wu, Y., Liu, Q., Wang, M., & Jia, L. (2023). Research on active safety methodologies for intelligent railway systems. *Engineering*, *27*, 266–279.
22. Quaglietta, E., Pellegrini, P., Goverde, R. M. P., Albrecht, T., Jaekel, B., Marlière, G., Rodriguez, J., Dollevoet, T., Ambrogio, B., & Carcasole, D. (2016). The ON-TIME real-time railway traffic management framework: A proof-of-concept using a scalable standardised data communication architecture. *Transportation Research Part C: Emerging Technologies*, *63*, 23–50.
23. Rana, M., & Sadiq, H. (2024). Computational Modeling and Simulation Techniques For Managing Rail–Urban Interface Constraints In Metropolitan Transportation Systems. *American Journal of Scholarly Research and Innovation*, *3*(02), 141–178.
24. Safitri, C., Harjono, M. S., Hasrito, E. S., & Roestam, R. (2024). Comprehensive Survey: Quality of Service in Railway Communication Using Information-Centric Networking and Light Fidelity. *IEEE Transactions on Intelligent Transportation Systems*.
25. Std, E. (2019). Railway applications-Communications, signalling and processing systems-Safety related electronic systems for signalling. *European Committee for Electrotechnical Standardisation (CENELEC)*.
26. Tan, M., Hu, Q., Wu, Y., Lin, J., & Fang, X. (2024). Decision-making method for high-speed rail early warning system in complex earthquake situations. *Transportation Safety and Environment*, *6*(3), tdad034.

27. Uddin, S. Z., & Shuvo, M. S. H. (2023). Integration Of Communications-Based Train Control (CBTC) Into Civil Engineering Design For Safer And Cyber-Secure Rail Systems. *American Journal of Scholarly Research and Innovation*, *2*(01), 357–388.
28. Wang, Y., Zhu, S., Li, S., Yang, L., & De Schutter, B. (2022). Hierarchical model predictive control for on-line high-speed railway delay management and train control in a dynamic operations environment. *IEEE Transactions on Control Systems Technology*, *30*(6), 2344–2359.
29. Weik, N., Volk, M., Katoen, J. P., & Nießen, N. (2022). DFT modeling approach for operational risk assessment of railway infrastructure. *International Journal on Software Tools for Technology Transfer*, *24*(3), 331–350.
30. Wen, C., Huang, P., Li, Z., Lessan, J., Fu, L., Jiang, C., & Xu, X. (2019). Train dispatching management with data-driven approaches: A comprehensive review and appraisal. *IEEE Access*, *7*, 114547–114571.
31. Yan, F., Gao, C., Tang, T., & Zhou, Y. (2017). A safety management and signaling system integration method for communication-based train control system. *Urban Rail Transit*, *3*(2), 90–99.
32. Zhang, Z., Wang, F., & Li, P. (2025). Secure and Privacy-Preserving Data Management in Train Coupling/Decoupling Scenarios: A Comprehensive Review and Future Perspectives. *Computing&AI Connect*, *2*(1), 1–10.
33. Zhu, L., Chen, C., Wang, H., Yu, F. R., & Tang, T. (2023). Machine learning in urban rail transit systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *25*(3), 2182–2207.