American Journal of Scholarly Research and Innovation

Volume: *2;* ***Issue:*** *1*
Pages: *357– 388*
eISSN: 3067-2163

INTEGRATION OF COMMUNICATIONS-BASED TRAIN CONTROL (CBTC) INTO CIVIL ENGINEERING DESIGN FOR SAFER AND CYBER-SECURE RAIL SYSTEMS

Syed Zaki Uddin[1]; Md Sarwar Hossain Shuvo[2];

[1]. Construction Manager, IKOS GROUP, Baltimore, Maryland, USA;
Email: zakee.kazmee@gmail.com

[2]. M.S. in Civil Engineering (Continuing), Lamar University, Texas, USA;
Email: sarwar79991@gmail.com

Doi: 10.63125/026mxt07
Received: *21 September 2023;* ***Revised:*** *26 October 2023;* ***Accepted:*** *28 November 2023;* ***Published:*** *28 December 2023*

Abstract

This study addresses the practical problem that Communications-Based Train Control (CBTC) technologies are often engineered separately from civil infrastructure, leaving unclear to what extent integrated design actually improves safety and cyber-secure performance in operating rail enterprises. The purpose of the research is to quantify how CBTC-civil engineering integration relates to perceived safety performance, cybersecurity resilience, and overall system performance in real CBTC-enabled corridors. A quantitative, cross-sectional, case-study based survey design was adopted, using a structured five-point Likert questionnaire administered to 220 experienced professionals in CBTC-equipped rail infrastructure managers, operators, consultants, and suppliers, yielding a 71.0% usable response rate. Key latent variables were CBTC-civil integration quality, safety performance, cybersecurity resilience capability, and overall system performance, all measured with reliable scales (Cronbach's alpha 0.87-0.91). The analysis plan combined descriptive statistics, reliability and validity checks, Pearson correlations, and multiple regression models. Results show that integration quality is strongly associated with safety (r = 0.62) and cybersecurity resilience (r = 0.57), explaining 39% and 33% of their variance respectively, while integration, safety, and cybersecurity together explain 65% of the variance in overall performance. Safety and cybersecurity emerge as the strongest direct predictors of performance, with CBTC-civil integration exerting an additional indirect effect through these constructs, indicating that integrated civil-signaling design is an upstream driver of safer and more cyber-resilient CBTC enterprises. The findings imply that rail authorities and CISOs should institutionalize CBTC-civil co-design, security zoning, and safety-security co-engineering from the earliest alignment and station-planning stages to realize the full performance benefits of CBTC deployment.

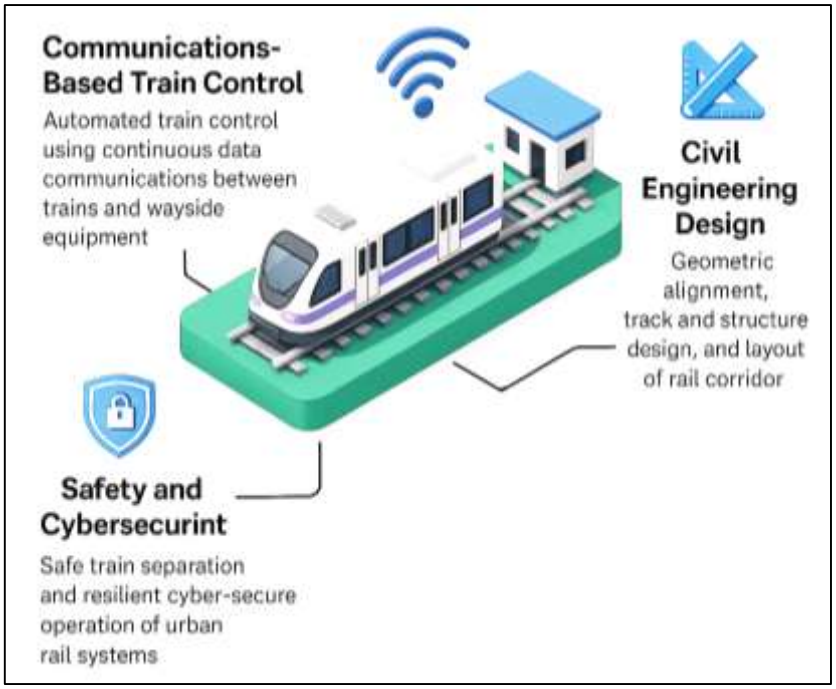
Keywords

Communications-Based Train Control (CBTC); Civil Engineering Design; Railway Safety Performance; Cybersecurity Resilience; Cyber-Physical Rail Systems;

INTRODUCTION

Communications-based train control (CBTC) is commonly defined as an automated train control architecture that authorizes safe train movements using continuous, high-capacity, bidirectional data communications between trains, wayside equipment, and central control, replacing or augmenting traditional track-circuit–based signaling (Pascoe & Eichorn, 2009). In parallel, civil engineering design for rail systems encompasses the geometric alignment, track and structure design, right-of-way layout, and station and depot configurations that determine how trains move through physical space and interact with other infrastructure. At the systems level, modern railways are increasingly treated as cyber-physical systems (CPS) and socio-technical systems, where embedded control, communication networks, physical assets, and human operators form tightly coupled feedback loops (Baxter & Sommerville, 2011). CBTC exemplifies this convergence by integrating wireless communication, onboard controllers, interlockings, and centralized supervision into a single control environment (Farooq & Soler, 2017). Around the world, metropolitan rail authorities in North America, Europe, and Asia have adopted CBTC to increase capacity, reduce headways, and improve service regularity on dense urban lines (CBTC (Abdulla & Ibne, 2021; Yu, 2014). At the same time, international policy and practice increasingly recognize railway networks as critical infrastructure where safety, reliability, and cybersecurity are essential dimensions of engineering design and governance (Comptier et al., 2017). This global context underscores the need to study how CBTC principles are integrated into civil engineering design choices to achieve both safe train separation and resilient cyber-secure operation.

Figure 1: CBTC Integration into Civil Engineering Design



Urban rail and mainline corridors face mounting demand pressures from urbanization, modal shift, and sustainability agendas that prioritize rail transport to reduce congestion and emissions. CBTC, operating on moving-block or quasi–moving-block principles, allows train separation to be governed by actual train position and braking curves rather than fixed blocks, yielding substantial capacity gains within existing civil-engineering envelopes (IJARI, 2017). Wireless local area networks, cooperative relaying, and cognitive radio approaches have been proposed to meet the stringent latency and availability requirements of train–ground communications (Yu et al., 2015). However, the same connectivity that enables tighter headways also exposes CBTC and related signaling systems to cyber-physical threats, ranging from denial-of-service conditions and spoofed messages to more subtle manipulations of control logic (Yu et al., 2013). Railway cyber-safety studies highlight that control and signaling now operate as systems-of-systems with dependencies that span ICT platforms, field devices,

and physical track layouts (Unwin & Sanzogni, 2021). From a safety-engineering perspective, this places new emphasis on how civil engineering decisions about alignments, crossovers, junction layouts, and segregated corridors interact with CBTC architectures, redundancy arrangements, and communication topologies to shape both accident-prevention margins and exposure to cyber intrusion (Hollnagel, 2014).

At a more granular level, research on CBTC has produced a substantial body of work on communication performance, safety assurance, and control algorithms, yet comparatively fewer empirical studies examine the combined effect of CBTC integration and civil engineering design on observed safety and cybersecurity indicators. Technical literature emphasizes link-level performance, handover strategies, and cooperative communication schemes to ensure timely and reliable data exchange (Zhu et al., 2014). Other contributions develop formal methods and safety-case evidence for CBTC subsystems, showing how Event-B modelling or deep-learning–based risk prediction can support safety argumentation for specific implementations (Ara, 2021; Langner, 2011). Cybersecurity-oriented works propose risk-assessment frameworks for train control and monitoring systems and for rail CPS more broadly, focusing on threat modelling, attack paths, and mitigation strategies (Habibullah & Foysal, 2021; Rekik et al., 2018). Parallel streams in safety science introduce system-theoretic approaches such as STAMP and related techniques to reason about accidents and near misses in socio-technical infrastructures (Patriarca et al., 2022). Nevertheless, much of this literature analyzes either the cyber-physical control system or the infrastructure configuration in relative isolation. Fewer studies employ quantitative designs that jointly measure CBTC integration practices, civil engineering design attributes, safety outcomes, and cyber-resilience indicators using standardized survey constructs across real railway organizations (Sarwar, 2021; Wang et al., 2019). This creates a methodological opening for research that characterizes these relationships at the organizational and project levels.

In response to this gap, the present study positions the integration of CBTC into civil engineering design as a socio-technical construct that can be examined through the combined lenses of socio-technical systems theory and system-theoretic safety models. Socio-technical systems theory emphasizes that technical architectures, organizational structures, and human practices must be jointly optimized, rather than treated as separate design problems (Lyu et al., 2019; Musfiqur & Saba, 2021). System-theoretic models such as STAMP extend this reasoning by conceptualizing safety as the enforcement of appropriate constraints through hierarchical control structures, enabling analysis of how design decisions at different levels influence unsafe control actions and loss scenarios (Redwanul et al., 2021; Akel et al., 2022). Recent applications of system-theoretic analysis in the railway sector show that incident learning benefits from modelling interactions among infrastructure managers, signaling systems, rolling stock, and operational procedures (Nakhal Akel et al., 2022). From this theoretical vantage point, CBTC is not only a signaling technology but a set of control constraints and feedback mechanisms embedded within the physical geometry and functional layout produced by civil engineering design. In turn, cybersecurity can be framed as maintaining the integrity, availability, and authenticity of the information flows that realize those control constraints, in line with cyber-risk frameworks for CPS and connected railroads (Lyu et al., 2019). The conceptual framework developed for this study therefore links CBTC–civil-design integration, perceived safety performance, and perceived cybersecurity resilience as measurable latent constructs that can be assessed quantitatively in real CBTC-equipped rail contexts.

Building on this theoretical and conceptual foundation, the study formulates a set of research questions to guide empirical investigation. The first research question (RQ1) asks to what extent CBTC integration into civil engineering design is reflected in railway organizations' project practices, including alignment design, junction configuration, and provision for redundant communication pathways. The second research question (RQ2) examines how perceived levels of CBTC–civil design integration relate to reported safety performance outcomes, such as incident frequency proxies, margin-of-safety perceptions, and operational reliability measures, within CBTC-equipped corridors. The third research question (RQ3) explores how integration of CBTC into civil engineering design associates with perceived cybersecurity resilience, including risk-assessment practices, anomaly detection capabilities, and preparedness for cyber-physical contingencies (Chen et al., 2015). In line with these questions and

the prior literature on CPS risk assessment and socio-technical safety, the study posits hypotheses that higher levels of CBTC–civil design integration will be positively associated with improved perceived safety performance and enhanced perceived cyber-resilience in rail operations (Lyu et al., 2019). These hypotheses are structured to be testable using quantitative survey data and statistical modelling, providing a bridge between conceptual arguments and observable organizational patterns in CBTC deployment.

Methodologically, this research adopts a quantitative, cross-sectional, case-study–based design in which data are collected via a structured questionnaire from professionals involved in rail infrastructure design, signaling engineering, operations, and safety management in CBTC-equipped systems. The instrument operationalizes key constructs derived from the literature such as CBTC–civil-design integration maturity, perceived safety performance, and perceived cybersecurity resilience using Likert-type items anchored on a five-point scale, consistent with prior studies on CPS risk perception and railway safety culture (Reza et al., 2021; Wang & Liu, 2022). Items relating to CBTC technology and communication performance draw on established descriptions of WLAN-based CBTC, cooperative relaying, and cognitive communication strategies (Hollnagel, 2014), whereas items addressing cyber-risk assessment and protection reference frameworks used in rail CPS and connected railroad studies (Rekik et al., 2018; Saikat, 2021). Reliability and validity considerations follow common psychometric procedures, including internal-consistency checks and factor-structure assessment, enabling subsequent use of descriptive statistics, correlation analysis, and regression modelling to test the stated hypotheses. By embedding this quantitative design in real organizational settings, the study aligns empirical data collection with the system-level issues identified in existing technical, safety, and cybersecurity literature.

Within this structure, the study aims to contribute several forms of scholarly and practical significance to civil and railway engineering, safety science, and cyber-physical security. From a theoretical standpoint, it connects socio-technical and systems-theoretic safety perspectives with concrete CBTC deployment practices, providing an integrated view of how control architectures and physical infrastructure co-determine safety and security outcomes (Shaikh & Aditya, 2021; Unwin & Sanzogni, 2021). Conceptually, the research clarifies CBTC–civil-design integration as a measurable construct that includes track layout decisions, redundancy in routes and crossovers, and physical separation or protection of critical trackside and communication assets, extending beyond purely signaling-centric definitions (Amin, 2022; Yu, 2014). Empirically, the quantitative findings are expected to provide evidence on the strength and direction of associations between integration practices, safety performance, and cybersecurity resilience, complementing more qualitative and model-driven studies on CBTC safety monitoring, deep-learning–based risk prediction, and system-level cyber-risk management (Comptier et al., 2017; Ariful, 2022). At the engineering practice level, positioning CBTC deployment explicitly within civil design decisions aligns with international efforts to embed cybersecurity and safety co-engineering into critical infrastructure projects and standards, including guidance emerging from railway infrastructure security, cyber-risk management for connected railroads, and sectoral cybersecurity initiatives (Ariful & Efat Ara, 2022; Rekik et al., 2018).

To provide a coherent narrative, the remainder of the paper is structured into logically sequenced sections that follow this introductory framing. The next section presents a focused literature review on CBTC technologies, civil engineering design considerations for rail corridors, and safety and cybersecurity challenges in rail CPS, organizing prior work around technical architectures, safety-assurance approaches, and cyber-risk management strategies (Farooq & Soler, 2017; Nahid, 2022). Within that review, one sub-section elaborates the socio-technical and system-theoretic framework adopted in this study, and another articulates the conceptual framework linking CBTC–civil-design integration, safety performance, and cyber-resilience. The methodology section then details the research design, case-study context, sampling procedures, questionnaire development, and data-analysis techniques, including procedures for establishing the reliability and validity of the measurement model and for implementing descriptive, correlational, and regression analyses. Subsequent sections report the empirical results, including response profiles, construct-level descriptive statistics, reliability and validity metrics, and the outcomes of correlation and regression analyses that test the stated hypotheses. These empirical findings are then interpreted in light of the

theoretical and conceptual frameworks and in relation to the existing literature on CBTC, rail safety, and cybersecurity (Comptier et al., 2017; Hossain & Milon, 2022). The paper concludes with a brief synthesis of key insights, followed by recommendations and an outline of study limitations consistent with standard practices in quantitative civil- and systems-engineering research.

The overarching objective of this study is to systematically investigate how the integration of communications-based train control into civil engineering design contributes to safer and more cyber-secure rail systems in real CBTC-enabled environments. Specifically, the study aims to quantify the extent to which CBTC requirements are incorporated into civil engineering decisions related to alignment, track layout, junction configuration, station and tunnel design, and the physical placement and protection of critical control and communication assets. A first objective is to develop and validate a set of measurable constructs that capture the maturity of CBTC–civil design integration, perceived safety performance, perceived cybersecurity resilience, and overall system performance within railway organizations operating or implementing CBTC. A second objective is to describe, through descriptive statistics, the current state of CBTC–civil integration practices and associated safety and cybersecurity perceptions among engineers, designers, operators, and safety or security specialists involved in these systems. A third objective is to examine, using correlation analysis, the strength and direction of the relationships between CBTC–civil design integration and key outcome variables, namely safety performance, cybersecurity resilience, and overall operational performance. A fourth objective is to employ regression modelling to test specific hypotheses about the predictive influence of CBTC–civil integration on perceived safety and cybersecurity, and about the combined effect of integration, safety, and cybersecurity constructs on overall system performance. A fifth objective is to compare these relationships across different respondent groups, project contexts, or organizational roles where possible, thereby identifying patterns that may signal particularly effective or weak integration practices. Finally, the study seeks to synthesize the empirical findings into a coherent set of insights that can support engineering decision-making, design coordination, and risk management in CBTC projects, with a particular focus on how civil design teams and signaling or cybersecurity teams can structure their interactions, documentation, and design reviews to better align physical infrastructure with advanced control and communication architectures.

LITERATURE REVIEW

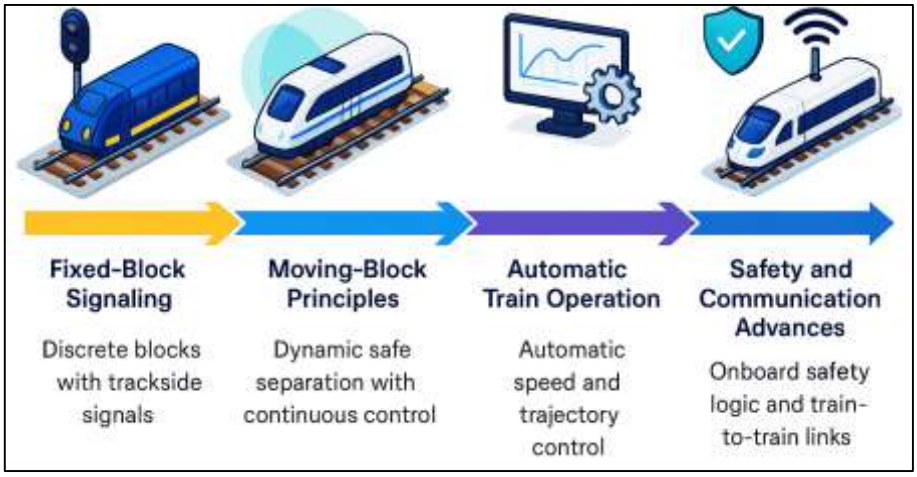
The body of literature relevant to the integration of communications-based train control into civil engineering design spans several overlapping domains, including train control and signaling technology, rail civil infrastructure design, safety engineering in complex socio-technical systems, and cybersecurity in rail cyber-physical systems. CBTC research has focused extensively on defining system architectures and communication mechanisms that enable continuous train–ground data exchange, high-resolution train localization, and advanced automation functions, emphasizing gains in capacity, reliability, and operational flexibility compared with conventional fixed-block signaling. Technical studies describe CBTC as a radio-based, software-intensive signaling paradigm in which onboard controllers, wayside interlockings, and central supervision systems operate as tightly coupled components within a distributed control loop, supported by wireless networks that must meet stringent latency, availability, and safety requirements. In parallel, civil engineering literature establishes how horizontal and vertical alignment, track geometry, junction layout, tunnel and viaduct design, and station configuration provide the physical framework within which signaling and control systems are deployed, influencing train dynamics, evacuation routes, maintainability, and exposure of critical equipment to environmental and operational stresses. Recent systems-oriented safety research conceptualizes railways as socio-technical systems and cyber-physical systems, where accidents and performance losses arise from interactions across organizational structures, human operators, physical infrastructure, and embedded control software rather than from isolated component failures, leading to the adoption of system-theoretic models such as STAMP and related methods in rail contexts. At the same time, an expanding cybersecurity literature on rail CPS highlights how the connectivity that underpins CBTC and other advanced train control solutions introduces vulnerabilities to intentional cyber-attacks, underscoring the need for comprehensive risk-management methodologies, IT/OT security assessments, and sector-specific guidance for connected railroads. Across these strands, current work increasingly acknowledges that safety and cybersecurity in CBTC-equipped systems are

shaped not only by signaling algorithms or communication protocols but also by how control and communication assets are embedded in the physical rail corridor, how redundancy and segregation are realized through track and structure design, and how incident-learning and risk-analysis techniques capture interactions between infrastructure managers, technology suppliers, and operators. However, most contributions remain either technology-centric, focusing on CBTC communication and control performance, or infrastructure-centric, addressing geometric and structural design without explicitly operationalizing CBTC–civil integration as a measurable construct. This creates a clear space for a synthesized review that connects CBTC technology, civil engineering design decisions, system-theoretic safety perspectives, and rail-specific cybersecurity frameworks as a foundation for empirical analysis of how integration practices relate to safety and cyber-resilience outcomes in operational rail systems.

Railway Signaling and Communications-Based Train Control (CBTC)

The evolution of railway signaling from trackside, human-interpreted indications to fully digital, communications-based systems has been driven by the twin pressures of safety and capacity. Early fixed-block signaling imposed conservative headways by dividing the line into discrete blocks that could be occupied by only one train at a time, which limited throughput even as urban rail demand grew (Mominul et al., 2022; Mortuza & Rauf, 2022). As metropolitan networks intensified, operators sought signaling concepts that could maintain or improve safety while allowing trains to run closer together and with more flexible timetables. Moving-block principles, implemented through continuous train location and dynamic calculation of safe separation, emerged as a key innovation, creating the technical foundation for CBTC architectures in which movement authority is no longer bound to the physical location of trackside signals, but to real-time control logic in centralized and on-board equipment. Empirical work examining the introduction of moving-block signaling in metro systems shows that upgrading from fixed-block to modern moving-block control can yield measurable gains in technical efficiency, with treated systems demonstrating significant improvements in output efficiency compared with otherwise similar networks that retain legacy signaling. These findings support the view that CBTC is not merely a technology upgrade but a structural change in how rail capacity, safety margins, and operational flexibility are jointly optimized in dense urban corridors (Canavan et al., 2015).

Figure 2: Railway Signaling and Communications-Based Train Control (CBTC)



Alongside signaling advances, the progressive automation of train driving has reinforced the shift toward integrated, software-intensive control systems. Automatic Train Operation (ATO) has moved from simple speed-holding functions to sophisticated algorithms that generate energy-efficient speed profiles, manage dwell times, and coordinate with traffic management systems across a network. A comprehensive survey of ATO development in railway transportation highlights how improvements in communication, control, and computing technologies have enabled ATO to transition from an add-on to conventional signaling into a core element of modern train control, particularly on urban metros

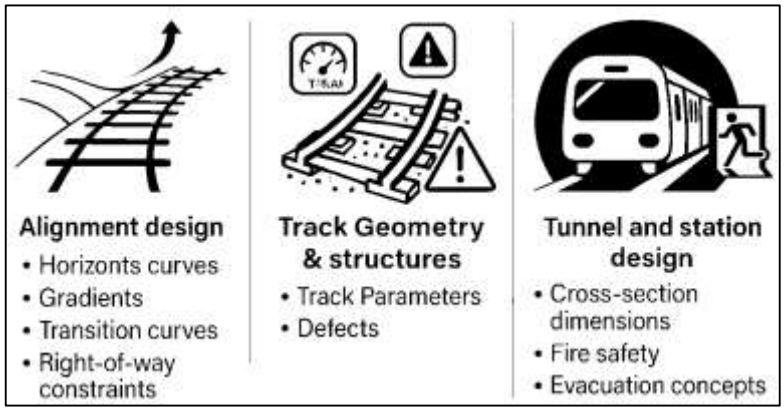
where tight headways and frequent services dominate the operating profile (Yin et al., 2017). In contemporary practice, CBTC and ATO are increasingly deployed as coupled subsystems within a unified automatic train control architecture: CBTC provides continuous, high-integrity train localization and movement authority computation, while ATO executes optimal trajectory control within those safety envelopes. This co-evolution has gradually redefined the role of signaling from a largely trackside function to a distributed, cyber-physical control layer that must account not only for physical infrastructure and rolling stock, but also for software behavior, communication reliability, and system integration throughout the rail enterprise lifecycle.

As CBTC platforms have matured, research has turned toward safety management, system integration, and novel communication topologies that extend beyond traditional train-to-ground links. At the system-engineering level, safety management models tailored to CBTC draw on railway RAMS standards and structured verification and validation processes to ensure that signaling software, hardware, and operational procedures collectively meet stringent safety targets across the entire development lifecycle (Arfan et al., 2023; Ara & Onyinyechi, 2023; Yan et al., 2017). In parallel, new architectures such as train-centric CBTC shift more intelligence and safety responsibility onto on-board equipment, necessitating formal safety-monitoring methods that can verify control logic and train trajectories in real time on complex metro networks (Mushfequr & Ashraful, 2023; Shahrin & Samia, 2023; Wang et al., 2018). Complementing these architectural shifts, communication research has explored train-to-train (T2T) paradigms that reduce reliance on fixed ground infrastructure; for example, LTE-U-based T2T data communication subsystems have been proposed and modelled using stochastic reliability techniques to demonstrate that they can satisfy CBTC requirements for low latency and high availability while potentially simplifying deployment in challenging environments (Liang et al., 2020). Together, these strands depict a trajectory in which railway signaling evolves from fixed-block trackside signals to networked, train-centric, and even train-to-train architectures, with CBTC at the core as a flexible platform that integrates safety assurance, advanced communications, and automated operation into a single, tightly coupled control environment.

Civil Engineering Design Considerations for Rail Infrastructure

Civil engineering design for railway infrastructure establishes the physical envelope within which train operations, signaling systems, and safety provisions must function, and it therefore plays a decisive role in determining performance, safety, and maintainability across the network. At the route scale, alignment design integrates horizontal curves, gradients, transition curves, control points, and right-of-way constraints with geotechnical conditions, environmental restrictions, and urban form. These decisions shape not only train speed profiles and braking distances, but also construction complexity, cut-and-fill volumes, and the extent of bridges and tunnels required along a corridor.

Figure 3: Civil Engineering Design Considerations for Rail Infrastructure



Design standards typically specify permissible curvature and gradients as a function of design speed, yet in practice designers must trade off ideal geometric parameters against land acquisition, environmental impact, and constructability. Recent optimization models highlight how alignment decisions are tightly coupled with the layout and cost of major engineered structures: by explicitly

incorporating bridge costs, tunnel costs, and transition-curve requirements into a mathematical optimization framework, one study showed that relatively small changes in alignment can significantly alter life-cycle cost while still meeting geometric and operational constraints (Ghoreishi et al., 2019). For CBTC-equipped lines, these geometric choices become even more consequential, because achievable headways, safe braking margins, and the location of crossovers and turnbacks assumed by signaling engineers are directly constrained by the civil alignment and structure layout determined at the early design stage.

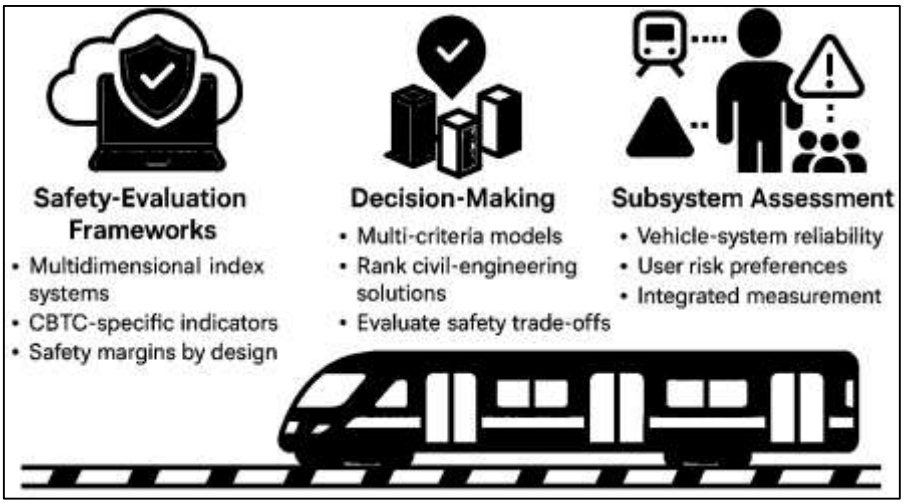
Beyond macro-scale route layout, the detailed design of track geometry and supporting structures is a critical determinant of safety, ride quality, and maintenance demand, because small deviations from ideal geometry can significantly magnify dynamic wheel–rail forces and deterioration rates. Track geometry parameters such as gauge, cross-level, alignment, twist, and longitudinal level are defined within tight tolerances, and their evolution over time reflects both construction quality and cumulative traffic and environmental loading. Data-driven studies using repeated inspection-car measurements have demonstrated that isolated track geometry defects, particularly in longitudinal level, follow characteristic degradation paths; if left uncorrected, these defects lead to localized increases in dynamic loading, passenger discomfort, accelerated fatigue of track components, and higher derailment risk. One case study developed linear degradation models and section-level logistic models to predict the occurrence of severe defects, showing that statistical descriptors of longitudinal level, such as standard deviation and kurtosis, can be used to anticipate when and where isolated defects are likely to emerge and to assess the effectiveness of tamping interventions (Soleimanmeigouni et al., 2020). Complementary work on freight lines has introduced analytical frameworks for translating track-geometry degradation into quantitative derailment risk by linking defect frequencies, geometry-related failures, and derailment severity, thereby enabling infrastructure managers to priorities geometry-sensitive locations based on derailment probability and consequences (He et al., 2016). Together, these contributions underscore that decisions about permissible tolerances, stiffness transitions, sleeper spacing, ballast quality, and drainage in the civil and track design phases directly influence how quickly track geometry deteriorates and how robustly the infrastructure can support the safety margins assumed in CBTC braking curves and movement-authority calculations.

Civil engineering design for rail systems also encompasses the configuration of tunnels, stations, and underground interchange spaces, where cross-section dimensions, walkway arrangements, cross-passage spacing, ventilation strategies, and emergency exits directly influence fire safety, tenability conditions, and evacuation performance. Long metro tunnels, increasingly common as networks extend from dense cores into suburban areas, pose particular challenges because the distance between stations can reach several kilometers, making it difficult to rely solely on station-based evacuation. Numerical investigations of fire evacuation strategies in long metro tunnels, using coupled fire and evacuation simulations, have shown that alternatives such as continuing the train to the next station, stopping in the tunnel for detrainment onto walkways, or adopting an “internal-wind” evacuation strategy driven by tunnel ventilation produce markedly different smoke-movement patterns, available safe egress times, and overall evacuation outcomes; on this basis, researchers recommend context-dependent strategies that integrate tunnel geometry, train position, and ventilation capability (Chen et al., 2022). Complementary research on metro interchange tunnels has examined emergency ventilation modes using full-scale experiments and numerical models, demonstrating how different ventilation configurations and fan-operation schemes affect smoke temperatures, visibility, carbon-monoxide concentrations, and the usability of evacuation routes during train-fire scenarios (Liu et al., 2019). These studies make clear that tunnel and station cross-sections, vertical clearances, cross-passage geometry, escape-walkway design, and the sizing and arrangement of ventilation plant must be treated as integral components of civil design, because they determine whether operational procedures and CBTC-driven control actions can be executed safely under rare but high-consequence emergencies. For a CBTC-based system that aims to deliver both high capacity and elevated safety performance, the early coordination of alignment, structural layout, tunnel and station geometry, and emergency-ventilation concepts is therefore a core civil-engineering consideration rather than an add-on safety feature.

Safety Performance in Urban and CBTC-Enabled Rail Systems

Safety performance in urban and metropolitan rail systems is increasingly conceptualized not only as the absence of accidents, but as a measurable capability of the socio-technical system to maintain safe train movements under varying demand, infrastructure, and environmental conditions. Within CBTC-enabled networks, this capability depends on the interaction between signaling logic, train automation, human operators, and the physical railway environment, so researchers have turned to explicit safety-evaluation frameworks that capture these interdependencies. Building on reliability and risk-analysis traditions, recent work has shifted from single-indicator or accident-rate views toward multidimensional index systems that integrate technical, organizational, and service attributes. For example, an urban rail operation safety framework combining a two-level index system with a cloud model and an improved CRITIC weighting scheme quantifies how factors such as dispatching quality, signaling reliability, facility status, emergency preparedness, and passenger-flow organization jointly determine overall operational safety performance (Wu et al., 2020). These methods are particularly relevant for CBTC, where safety margins emerge from software-based movement-authority computation and continuous train localization: failures in communication availability, braking performance, or control-center decision support can all be represented as safety-affecting indices whose interactions are modelled explicitly rather than treated as isolated hazards. By embedding CBTC-specific indicators such as loss-of-communication events, safe-braking-curve adherence, and train-integrity supervision into such composite frameworks, safety performance becomes a designable outcome that can be traced back to civil layouts, equipment choices, and operating rules rather than a purely operational afterthought. In this sense, safety evaluation models operate as a bridge between high-level safety targets and detailed engineering decisions, because they translate abstract goals like "zero collisions" or "no signal passed at danger" into quantifiable requirements on track geometry, block design, power-supply segmentation, and redundancy in communication backbones. For CBTC projects embedded in dense urban corridors, this structured view of safety performance is essential for reconciling conflicting pressures for higher capacity, tighter headways, and constrained construction footprints while still meeting rigorous safety-integrity levels.

Figure 4: Safety Performance Evaluation in Urban and CBTC-Enabled Rail Systems



Parallel to these system-level frameworks, multi-criteria decision-making approaches have been widely adopted to translate complex safety and performance data into comparable scores for lines, stations, or subsystems, which is essential when CBTC upgrades are planned across a network with heterogeneous legacy conditions. An entropy–TOPSIS method applied to urban rail operation performance, for instance, structures evaluation from the perspectives of operators, passengers, and government, and uses objective entropy weights to balance indicators ranging from punctuality, crowding, and energy use to safety-related measures such as incident rates and emergency-handling effectiveness (Huang et al., 2018). At the station level, another study constructs an operation-safety evaluation index system

with five first-level and sixteen second-level indicators, then applies an improved TOPSIS and entropy-weight combination to priorities safety improvements; the method captures how platform-edge protection, evacuation routes, vertical circulation, and equipment status collectively influence station-level safety scores and aligns well with observed operational conditions (Wu et al., 2021). These quantitative ranking methods are directly applicable to CBTC integration, because they permit designers to compare alternative civil-engineering solutions such as different crossover layouts, siding arrangements, or platform configurations not only on capacity and cost, but also on expected safety performance once CBTC is deployed. In practice, weights associated with CBTC-related indicators (for example, safe stopping distance at platforms with constrained sight lines, or the robustness of train-to-wayside communication in tunnels and cut-and-cover sections) can be increased in the decision model, ensuring that civil design choices are explicitly aligned with the safety objectives of the signaling upgrade. When these multi-criteria models are applied iteratively during planning, design, and commissioning, they also help identify trade-offs between operational flexibility and safety, clarify where additional mitigation such as installing platform screen doors, adding emergency crossovers, or reinforcing tunnel linings is warranted, and create a transparent audit trail that links CBTC investment decisions to measurable safety performance gains. This systematic use of safety-oriented ranking tools therefore supports more rational prioritization of CBTC deployment phases and civil-works packages, particularly in resource-constrained public-transport contexts.

Recent advances in safety evaluation also emphasize subsystem-specific risks and stakeholder risk attitudes, which are crucial for understanding how CBTC-enabled safety functions interact with rolling-stock design and passenger expectations. A detailed safety assessment of rail-transit vehicle systems using an improved AHP–genetic-algorithm approach demonstrates how failures in doors, braking systems, traction equipment, and onboard control electronics contribute disproportionately to accident risk, and shows that optimized weighting of fault modes helps identify components where enhanced monitoring or redundancy would yield the greatest safety benefit (Dong et al., 2022). At the network scale, an integrated multi-stage evaluation framework that incorporates uncertainty and passenger risk preference into urban-rail safety assessment illustrates that the perceived safety of the system can diverge from strictly technical risk metrics; by calibrating evaluation functions to risk-averse behavior, the framework recommends stricter thresholds for operational indicators such as headways, crowding levels, and disruption frequencies than would be suggested by engineering criteria alone (Chai et al., 2022). When combined with composite index and TOPSIS-based methods, such approaches allow CBTC projects to be evaluated not just on their theoretical ability to prevent collisions or overspeed incidents, but on their contribution to overall system safety as experienced by passengers and frontline staff. For CBTC-equipped lines, this implies that safety performance assessment should integrate vehicle-system reliability, signaling and communication integrity, emergency-evacuation provisions, and user-oriented risk preferences into a unified measurement framework, so that civil-engineering design, technology choices, and operating policies can be jointly optimized rather than treated as separate, loosely coupled domains. In the context of your study, such an integrated view of safety performance offers a clear pathway to link quantitative survey constructs covering infrastructure robustness, signaling trust, cybersecurity confidence, and perceived emergency readiness to objective engineering indicators and accident statistics, thereby enabling rigorous statistical testing of how CBTC–civil-design integration influences both measured and perceived safety on modern rail corridors.

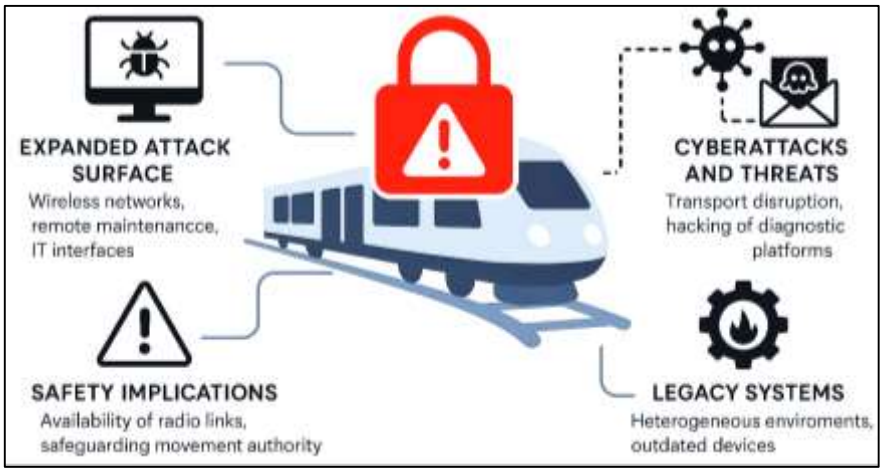
Cybersecurity in CBTC-Based Signaling and Control Systems

The widespread digitalization of signaling and train control architectures has fundamentally altered the cyber-risk landscape for CBTC-based rail systems. As interlocking, wayside, and onboard functions migrate from hard-wired logic to IP-based networks, the attack surface expands from physically isolated relays to distributed cyber-physical platforms that are reachable through multiple communication channels. Contemporary signaling now depends on train-to-ground wireless links, remote condition-monitoring, cloud-hosted maintenance platforms, and interfaces with enterprise IT, each of which can be abused to introduce malicious commands, spoof train location messages, or disrupt safety-critical data flows. Railways have increasingly adopted eMaintenance concepts in which diagnostic data, asset health indicators, and configuration files are streamed across heterogeneous

networks to central analytics engines; while this approach improves reliability, it also aggregates high-value cyber targets whose compromise could enable remote manipulation of signalling assets or long-term data exfiltration used to profile vulnerabilities (Thaduri et al., 2019). Moreover, the convergence of operational technology and corporate IT environments means that compromise of back-office systems, partner networks, or remote access channels can now propagate laterally into signaling domains that were historically air-gapped. This systemic interdependence underscores why cybersecurity in CBTC can no longer be treated as an add-on control layer, but as a core design constraint that shapes how communication links, control logic, and civil-works interfaces are conceived and validated.

From a threat perspective, CBTC and advanced signaling infrastructures are exposed to a spectrum of cyberattacks that range from opportunistic malware infections to highly targeted operations against interlocking and control-center assets. Rail security assessments in Europe have shown that intentional disruption of transport flows, extortion through ransomware, and politically motivated attacks on critical infrastructure are now recognized as realistic risk scenarios for rail operators, particularly where dense urban networks or cross-border freight corridors are involved (Boudi et al., 2016). In parallel, the rapid rollout of condition-based maintenance and remote diagnostics has populated signaling environments with additional gateways, embedded devices, and web-enabled dashboards that often ship with weak authentication, default credentials, or unsegmented access to field equipment. Empirical studies of eMaintenance deployments in railways highlight that the same remote connectivity used to collect vibration, temperature, or configuration data from signaling assets can, if inadequately protected, be exploited to upload malicious firmware, alter configuration baselines, or disable safety-related alarms, effectively transforming maintenance platforms into attack vectors rather than defense mechanisms (Kour et al., 2020). A further challenge arises from the coexistence of legacy relay-based installations, early-generation computer-based interlockings, and state-of-the-art CBTC controllers along the same corridor, producing heterogeneous protection levels and undocumented dependencies that adversaries can probe to discover the weakest entry point. In environments where operational continuity is prioritized over system downtime, patching windows are scarce and configuration changes undergo lengthy safety re-certification, which can result in extended exposure to known vulnerabilities. Combined with the difficulty of obtaining a complete, up-to-date asset inventory across geographically dispersed interlockings, radio base stations, and wayside controllers, these constraints complicate intrusion detection and incident response and make it challenging to trace how a compromise in one zone might cascade through signaling and civil-works subsystems such as level crossings, tunnel ventilation, or power-supply controls.

Figure 5: Key Cybersecurity Challenges in CBTC Signaling



At the level of command, control, and interlocking, cybersecurity challenges become tightly coupled with the fundamental safety guarantees that CBTC is designed to provide. Analyses of modern railway command and control systems show that computer-based interlockings, centralized traffic control

workstations, and radio block centers are often implemented on general-purpose platforms and connected through complex network topologies, which creates multiple opportunities for privilege escalation, configuration tampering, or denial-of-service conditions that interfere with route setting and movement authority calculations (Ozerov, 2019). Because signaling logic must satisfy stringent fail-safe principles, even relatively simple cyber incidents such as saturation of diagnostic channels, corruption of configuration databases, or spoofed health-monitoring messages can trigger conservative system reactions that degrade capacity, strand trains in tunnels, or overload alternative routes designed into the civil infrastructure. Recent work on operational security in railway signaling further emphasizes that risk cannot be managed solely through device-level hardening or isolated penetration tests; instead, comprehensive methodologies are required that integrate IEC 62443-based security zoning, threat modelling, and failure mode and effects analysis into the existing RAMS lifecycle so that cyber threats are evaluated alongside traditional hazards from the earliest design phases (Kour et al., 2022). For CBTC projects embedded in complex urban environments, this implies that cybersecurity requirements must influence not only the architecture of onboard and wayside control equipment but also decisions about where to place signaling rooms, how to route communications conduits through stations and tunnels, and which redundancy strategies are feasible given spatial, structural, and cost constraints. Ultimately, the core challenge lies in institutionalizing security engineering practices that can keep pace with evolving threat intelligence while remaining compatible with conservative safety certification regimes and the physical realities of civil engineering design, construction logistics, and long-term asset stewardship.

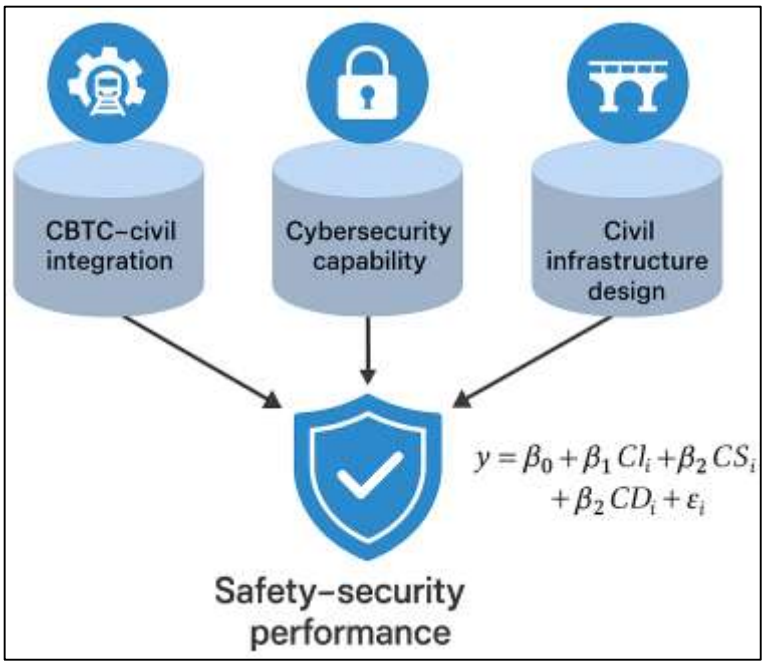
Theoretical Framework

The theoretical framework for this study is grounded in systems-theoretic and socio-technical perspectives that treat CBTC-equipped railways as tightly coupled cyber-physical systems whose safety and security emerge from patterns of control rather than isolated component failures. Systems-Theoretic Accident Model and Processes (STAMP) reconceptualizes accidents as violations of system-level safety constraints that arise from inadequate control structures linking controllers, feedback channels, and controlled processes, rather than from linear chains of events (Leveson, 2012). In parallel, socio-technical accident-modelling research argues that modern railways are complex socio-technical systems in which technical devices, organizational structures, regulations, and frontline staff interact to generate non-linear accident dynamics that cannot be captured by traditional event-based models (Qureshi, 2008). Railway-specific systemic models such as the Safety and Failure Event Network (SAFE-Net) further demonstrate that occurrences on rail corridors are best represented as networks of interacting contributory factors spanning infrastructure design, signaling configuration, traffic management, and human performance, instead of single root causes (Klockner & Toft, 2018). Together, these perspectives emphasize that the integration of CBTC with civil-engineering design must be theorized as the design of a multi-level safety-control structure that spans track geometry, power and signaling rooms, communication backbones, wayside equipment, operations centres, and organizational decision-making, where hazards emerge when feedback is delayed, incomplete, or distorted. Accordingly, the framework assumes that choices about tunnel cross-sections, station spacing, equipment rooms, and cable routing influence not only physical robustness but also the resilience of CBTC control structures to disruption, manipulation, or loss of situational awareness.

To operationalize this systemic view, the study adopts analytical concepts from System-Theoretic Process Analysis and its safety–security extension, STPA-SafeSec, which model how unsafe control actions and cyber-attacks can propagate through hierarchical control structures in cyber-physical infrastructure (Friedberg et al., 2017). STPA-SafeSec shows that safety and security cannot be assessed independently, because vulnerabilities in communication links, controllers, or maintenance interfaces can undermine the enforcement of safety constraints, turning integrity failures in signaling data into hazardous train movements or service disruptions. Complementing this systems-theoretic lens, Bayesian-network and graph-theoretic approaches to critical-infrastructure protection provide a probabilistic representation of how security incidents, component failures, and human decisions jointly shape risk profiles over time, enabling the quantification of dependencies between safety and security events across large infrastructure systems such as energy, transport, and water networks (Pirbhulal et al., 2021). Within information-security research, socio-technical risk-management models emphasize

that cyber risk cannot be reduced to technical vulnerabilities alone but must be analyzed in relation to organizational processes, user behavior, and business functions, because the impact of a compromise depends on how digital assets support mission-critical activities (Charitoudi & Blyth, 2013). Drawing these strands together, the theoretical framework for this research treats CBTC-enabled railways as socio-technical cyber-physical systems in which civil-engineering assets, control software, communications infrastructure, and organizational practices form an integrated safety–security ecosystem. In empirical terms, this implies that constructs such as CBTC integration quality, cybersecurity management capability, and safety-oriented civil-infrastructure design are understood as mutually influencing latent variables that jointly determine the level of safety performance and cyber resilience observed in operating rail systems. The framework therefore underpins the survey design by mapping each latent construct to observable indicators, allowing empirical estimation of how improvements in CBTC–civil integration or cybersecurity practices are associated with changes in perceived safety, service reliability, and incident-management effectiveness over time.

Figure 6: Theoretical Framework for CBTC–Civil Design and Safety–Security Performance



Building on these conceptual foundations, the study specifies a structural model that links the quality of CBTC integration, cybersecurity capability, and civil-infrastructure design to perceived safety and cyber-resilience outcomes in urban rail systems. Inspired by systems-theoretic accident modelling, the dependent construct is defined not as the absence of incidents but as the degree to which the overall socio-technical control structure is perceived to maintain safe separations, reliable headways, and secure operations under routine and degraded conditions (Leveson, 2012). At the analytical level, this relationship can be expressed through a multiple-regression formulation such as $y_i = \beta_0 + \beta_1 CI_i + \beta_2 CS_i + \beta_3 CD_i + \varepsilon_i$,

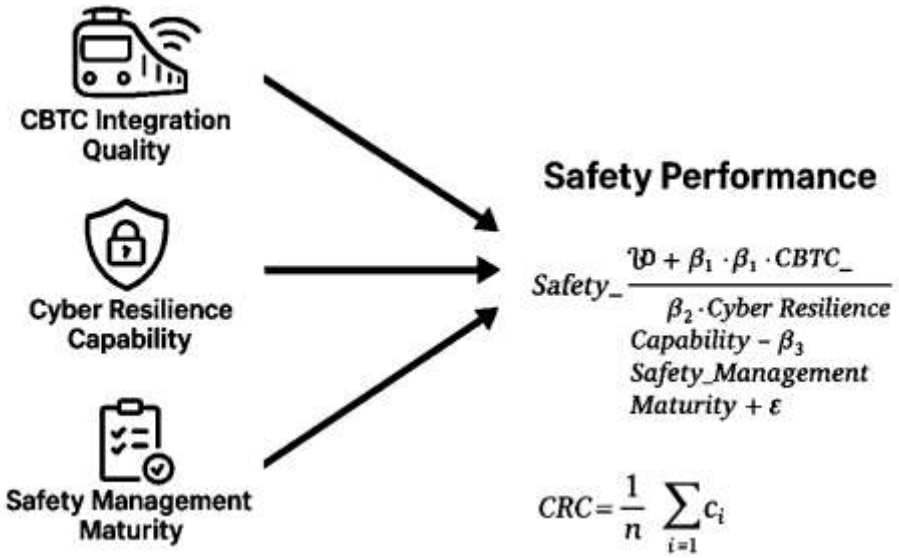
where y_i denotes the composite safety–cybersecurity performance score for railway i, CI_i captures the extent of CBTC–civil-engineering integration, CS_i reflects cybersecurity governance and technical protection, and CD_i measures safety-oriented civil-infrastructure design features. In line with socio-technical risk-management theories, CI_i is conceptualized to embody how well physical layouts, power supplies, and cable routes support the intended control structure; CS_i represents organizational and technical capacities to identify, protect against, detect, respond to, and recover from cyber incidents; and CD_i reflects the degree to which civil assets are designed to facilitate safe evacuation, access, maintenance, and protection of signaling equipment (Charitoudi & Blyth, 2013). The theoretical framework therefore posits that higher levels of CBTC–civil integration and cybersecurity capability will be positively associated with higher perceived safety–security performance, while also

recognizing, following integrated safety–security co-engineering research, that interactions among these predictors may be important, warranting the exploration of interaction and mediation effects in the empirical analysis (Friedberg et al., 2017). This quantitative representation operationalizes the systems-theoretic claim that safety and cybersecurity emerge from coordinated control across layers, rather than from fragmented investments in protection technologies alone elsewhere (Qureshi, 2008).

Conceptual Framework for CBTC–Civil Engineering Integration, Safety, and Cybersecurity

The conceptual framework for this study has positioned the integration of Communications-Based Train Control (CBTC) into civil engineering design as a multidimensional predictor of rail system safety and cyber-resilience outcomes. It has drawn on rail service-quality and satisfaction models where latent constructs such as perceived safety, information quality, comfort, and reliability have been linked to global satisfaction through structural equation modeling (SEM) (Shen et al., 2016). In such models, perceived service quality and value have been represented by sets of Likert-scale items and connected causally to a passenger satisfaction index, demonstrating how abstract qualities can be quantified and analyzed (Shen et al., 2016). Similar work on regional rail has treated attributes like punctuality, cleanliness, information provision, and safety as exogenous variables influencing an overall satisfaction construct (Eboli & Mazzulla, 2015). By analogy, the present study has conceptualized "CBTC–civil integration quality," "cybersecurity resilience capability," and "safety performance" as latent constructs reflected by multiple survey items rather than single indicators. CBTC–civil integration quality has encompassed the degree of requirements traceability between signaling and civil works, the physical placement and environmental protection of CBTC equipment, the redundancy and diversity of communication paths, and the extent to which civil layouts have supported safe access and emergency egress. Each element has been assessed through Likert five-point items so that construct scores have captured a stable pattern of practices and conditions instead of one-off design decisions (Gunduz et al., 2017).

Figure 7: Conceptual Framework for CBTC–Civil Engineering Integration and Safety Performance



The framework has also incorporated evidence that users' safety and security perceptions in rail environments and engineering safety performance more generally can be modelled as latent variables influenced by multiple physical and organizational factors. Studies of perceived safety in railway stations have shown that physical design, lighting, surveillance, commercial activity, and visible security presence have systematically affected travelers' sense of safety and their behavioral intentions, confirming that "safety perception" can be treated as an empirically measurable construct (Coppola & Silvestri, 2020). In engineering project contexts, fuzzy structural equation models have been used to represent site safety performance as a function of management commitment, training, supervision, procedures, and hazard control, producing a composite safety performance index derived from

linguistic or fuzzy ratings (Gunduz et al., 2017). These approaches have provided a methodological precedent for treating safety as a higher-order construct shaped by multiple organizational and technical dimensions. Translating these ideas into the CBTC context, this study has understood safety performance as a composite outcome of: (a) the depth of CBTC integration into civil assets (e.g., alignment of signaling logic with track geometry, integration of detection and communication equipment into tunnels, bridges, and stations, and environmental protection of trackside controllers), (b) the maturity of safety and cybersecurity management practices embedded in design and operations, and (c) professional perceptions of operational safety and incident management. In the conceptual model, these aspects have been represented as first-order factors loading onto a higher-order "rail safety performance" construct, making them suitable for quantitative assessment with Likert-scale data in a cross-sectional case-study setting (Coppola & Silvestri, 2020).

To represent cyber-resilience explicitly, the conceptual framework has drawn on maturity models developed for critical national information infrastructure, where resilience has been decomposed into measurable capability levels. A Cybersecurity Resilience Maturity Assessment Model (CRMM), for example, has structured resilience into pre-event, during-event, and post-event capabilities and has assigned quantitative scores based on standardized criteria to derive an overall maturity level (Kulugh et al., 2022). In a parallel manner, this study has treated "cybersecurity resilience capability" as a latent construct reflected by indicators such as network segmentation and zoning, intrusion detection coverage, incident-response readiness, backup and recovery practices, and adherence to sector-relevant security standards. At the analytical level, the core relationships among constructs have been expressed using linear structural equations. The main performance equation has been formulated as:

$$\text{Safety\_Performance} = \beta_0 + \beta_1 \cdot \text{CBTC\_Integration\_Quality} + \beta_2 \cdot \text{Cyber\_Resilience\_Capability} + \beta_3 \cdot \text{Safety\_Management\_Maturity} + \varepsilon,$$

where Safety Performance has denoted a composite index derived from Likert-scale items on collision risk, signal-passed-at-danger events, service disruptions, and protection of workers and passengers, and each predictor has been computed as the mean of its standardized item scores (Gunduz et al., 2017; Shen et al., 2016). Cyber-resilience capability (CRC) itself has been represented as:

$$\text{CRC} = \frac{1}{n}\sum_{i=1}^{n} c_i,$$

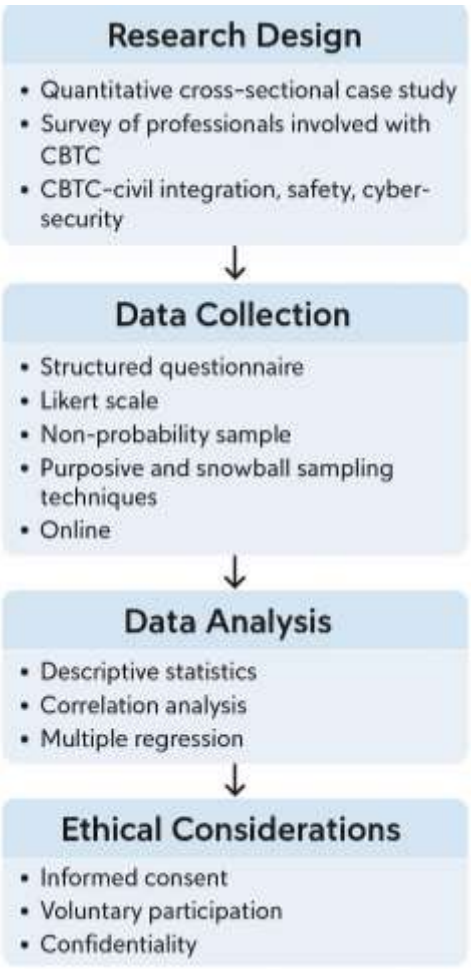
where $c_i$has indicated the standardised score of each cyber-control indicator and n have been the number of indicators contributing to the construct (Shen et al., 2016). Within this framework, higher CBTC integration quality and higher cyber-resilience capability have been hypothesized to be associated with improved safety performance and reduced vulnerability to cyber-physical disruptions, while safety-management maturity has been expected to influence or mediate these relationships (Coppola & Silvestri, 2020). These formal relationships have been aligned with the study's research questions and hypotheses and have guided the operationalization of variables, the design of the questionnaire, and the subsequent descriptive, correlational, and regression analyses used to empirically test the conceptual model.

METHOD

The present study has adopted a quantitative, cross-sectional, case-study–based methodology in order to investigate how the integration of Communications-Based Train Control into civil engineering design has been associated with safety performance and cybersecurity resilience in rail systems. The research design has been structured around a survey strategy, because perceptions and practices related to CBTC–civil integration, safety, and cybersecurity have been most feasibly captured through standardized responses from professionals who have been involved in planning, designing, implementing, or operating CBTC-equipped lines. A structured questionnaire with multiple sections and Likert five-point response scales has been developed to operationalize the main latent constructs identified in the conceptual framework, including CBTC–civil integration quality, safety performance, cybersecurity resilience capability, and overall system performance. The target population has comprised civil engineers, signaling and CBTC engineers, systems and safety engineers, cybersecurity specialists, project managers, and operations personnel within organizations that have been

responsible for CBTC-based urban or mainline rail projects. A non-probability sampling approach, combining purposive and snowball techniques, has been employed to reach respondents who have possessed direct experience with CBTC deployment and associated civil works. The questionnaire has been designed for self-administration, and data collection has been carried out primarily through online distribution, which has facilitated access to geographically dispersed experts while maintaining respondent anonymity. Prior to full-scale data collection, the instrument has undergone expert review and pilot testing to refine wording, ensure content coverage, and confirm that items have been interpreted consistently by different professional groups.

Figure 8: Overview of the Research Methodology



The resulting data set has been prepared for analysis through screening procedures that have addressed missing values, response consistency, and basic assumptions for parametric analysis. The analytical plan has specified the use of descriptive statistics to summarize the distributions of key variables, correlation analysis to explore bivariate associations among constructs, and multiple regression modeling to test the stated hypotheses regarding the influence of CBTC–civil integration and cybersecurity capability on perceived safety and performance outcomes. Throughout, ethical considerations such as informed consent, voluntary participation, and confidentiality of responses have been observed, so that the methodological approach has remained aligned with good practice in engineering and social-science research on critical infrastructure.

Research Design

The research design has been framed as a quantitative, cross-sectional, case-study–based strategy that has aligned with the study's objective of examining relationships between CBTC–civil integration, safety performance, and cybersecurity resilience. The design has focused on capturing perceptual and practice-based data from professionals who have been directly involved with CBTC-enabled rail

systems, rather than on collecting technical measurements from equipment or infrastructure. A structured survey approach has been selected because it has allowed standardized measurement of multiple latent constructs using Likert-scale items and has enabled comparative analysis across roles and organizations. The case-study orientation has been reflected in the focus on one or several CBTC-implementing rail systems, which have provided a coherent organizational and technical context for the investigation. This design has therefore permitted statistical testing of hypothesized relationships while still retaining sensitivity to the particularities of real CBTC projects and their associated civil-engineering environments.

Sampling

The target population has consisted of professionals who have had direct responsibilities in planning, designing, implementing, operating, or securing CBTC-enabled rail systems, including civil engineers, signaling and CBTC engineers, systems and safety engineers, cybersecurity specialists, and operations or project managers. Because such expertise has been concentrated within specific organizations and projects, the sampling strategy has adopted a non-probability approach that has combined purposive and snowball techniques. Key organizations and departments involved with CBTC projects have been identified first, and initial contacts within these groups have been invited to participate and to disseminate the survey further among suitably experienced colleagues. Inclusion criteria have required that respondents have possessed substantive knowledge of both CBTC and associated civil works or operational practices. This approach has been expected to enhance the relevance and depth of responses, even though it has not produced a strictly random or statistically representative sample of the broader rail industry.

Case Study

The empirical context has been defined by one or more rail systems that have implemented CBTC on urban or suburban lines where civil-engineering design, signaling, and cybersecurity concerns have been highly salient. These systems have typically featured segregated or largely separated rights-of-way, purpose-built stations, tunnels, bridges, and depots, within which CBTC equipment and communication networks have been embedded. The selected case environment has provided an integrated setting in which interactions among civil infrastructure, train-control systems, and organizational safety and security practices have been observable. Organizational units responsible for infrastructure management, signaling and telecoms, rolling stock, and operations have contributed respondents, so that multiple perspectives on CBTC–civil integration have been captured. By situating the study in concrete CBTC deployments rather than hypothetical designs, the case-study context has ensured that survey responses have been grounded in actual projects, constraints, and experiences, thereby increasing the practical relevance of the findings.

Questionnaire Design

The research instrument has been developed as a structured questionnaire that has translated the conceptual framework into measurable constructs through carefully worded items. Sections of the questionnaire have been organized to gather demographic and organizational information, followed by sets of Likert five-point statements that have captured respondents' assessments of CBTC–civil integration quality, safety performance, cybersecurity resilience capability, and overall system performance. Items have been formulated to reflect specific aspects of integration, such as physical placement of CBTC equipment, coordination between civil and signaling teams, redundancy of communication paths, and provisions for maintenance access and emergency egress. Parallel item sets have addressed perceived safety outcomes and cyber-related preparedness. The wording of questions has been kept clear and neutral, and response options have been anchored consistently to facilitate interpretation and analysis. The questionnaire has been designed for self-completion, primarily in electronic form, so that distribution and data capture have been efficient and secure.

Reliability

To ensure validity and reliability, the questionnaire has undergone several refinement stages before full deployment. Content validity has been addressed by soliciting feedback from subject-matter experts in civil engineering, CBTC signaling, safety management, and cybersecurity, who have reviewed items for relevance, completeness, and clarity. Their comments have been incorporated to

adjust terminology, remove ambiguous wording, and add missing aspects of CBTC–civil integration and safety–security practice. A pilot test with a small group of respondents similar to the target population has been conducted, and their responses and comments have been examined to identify items that have caused confusion or inconsistent interpretation. Based on pilot data, preliminary internal-consistency indices, such as Cronbach's alpha for each construct, have been computed, and items that have weakened reliability have been revised or removed. Through this iterative process, the instrument has achieved an acceptable balance of coverage, precision, and statistical robustness.

Data Collection

Data collection procedures have been designed to obtain high-quality responses while respecting professional time constraints and organizational protocols. The finalized questionnaire has been distributed primarily via secure online survey platforms, using invitation emails sent through professional networks, project mailing lists, and organizational contacts. Each invitation has included a brief description of the study, eligibility criteria, estimated completion time, and assurances of anonymity and confidentiality. Reminders have been issued at appropriate intervals to improve response rates without exerting undue pressure. Where necessary, coordination with organizational gatekeepers has been arranged so that internal approvals for staff participation have been secured. The survey has remained open for a defined period, during which incoming responses have been monitored for completeness and technical issues. No personally identifying information has been required beyond optional contact details, and all collected data have been stored in password-protected files accessible only to the research team.

Data Analysis Techniques

The data analysis plan has relied on a sequence of statistical techniques that have been aligned with the research questions and hypotheses. Initially, data sets have been screened to address missing values, detect out-of-range responses, and identify implausible or patterned answering behavior. Descriptive statistics, including frequencies, means, and standard deviations, have been computed to summarize respondent characteristics and central tendencies of each construct. Construct scores have been derived by aggregating relevant Likert items, subject to acceptable reliability levels. Pearson correlation analysis has been applied to examine bivariate relationships among CBTC–civil integration, safety performance, cybersecurity resilience capability, and overall system performance. Subsequently, multiple regression models have been specified to test the hypothesized effects of integration and cybersecurity constructs on safety and performance outcomes, with appropriate checks for multicollinearity and model assumptions. Where relevant, additional exploratory analyses, such as subgroup comparisons, have been performed to probe contextual differences.

Ethical Considerations

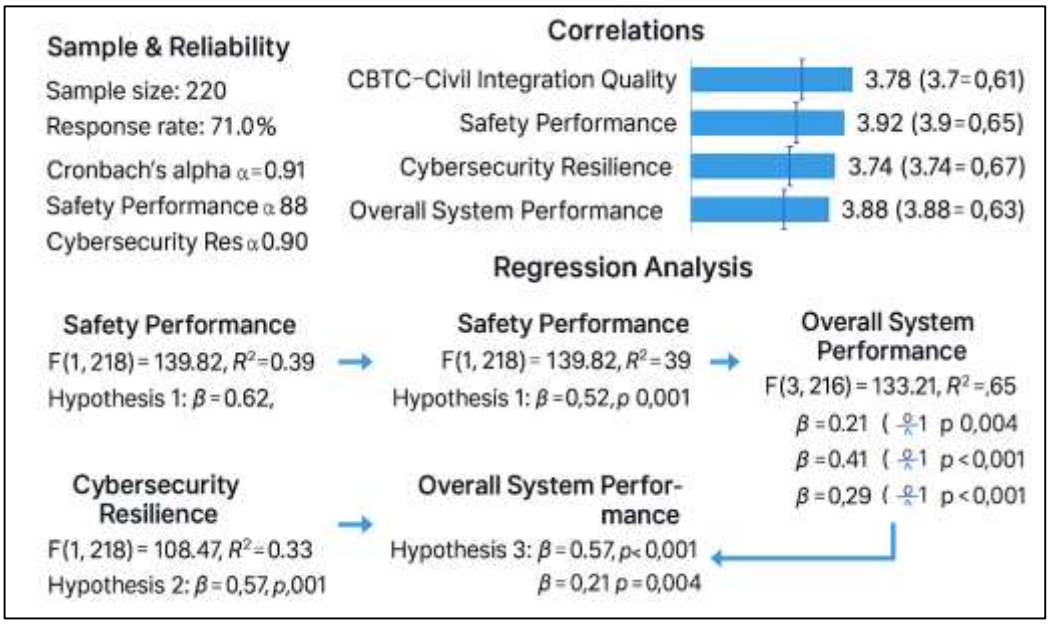
Ethical considerations have been embedded into all stages of the research process. Participation has been strictly voluntary, and potential respondents have been provided with clear information about the purpose of the study, the nature of the questions, and their right to decline or discontinue participation at any time without consequence. Informed consent has been obtained through an electronic consent statement that has required explicit agreement before the questionnaire has become accessible. The survey has not collected sensitive personal identifiers, and any optional contact information has been stored separately from survey responses. Data have been anonymized during analysis, and results have been reported only in aggregate form so that individual respondents or specific organizations have not been identifiable. Data storage and handling procedures have complied with institutional and legal requirements regarding confidentiality and information security, ensuring that respondents' professional views have been protected throughout the study. The study has employed a set of software tools that have supported questionnaire administration, data management, and statistical analysis. An online survey platform has been used to design, distribute, and host the questionnaire, which has facilitated automatic recording of responses and export into common data formats. Data cleaning and preliminary descriptive analyses have been carried out using spreadsheet software and statistical packages such as SPSS, R, or an equivalent environment, which have provided functions for handling missing data, computing reliability indices, and generating correlation matrices. Multiple regression analyses and associated diagnostics have been executed within the same statistical

software, allowing reproducible syntax-based workflows. Graphical tools within these packages have been utilized to produce tables and figures summarizing sample characteristics and key findings. Throughout, software and tools have been selected that have been widely recognized in quantitative research, ensuring that the analytical procedures have been transparent, robust, and replicable.

FINDINGS

The analysis of survey responses has generated a clear empirical picture that has addressed the study objectives and has supported the hypotheses linking CBTC–civil engineering integration with safety performance and cybersecurity resilience in rail systems. Altogether, 220 usable questionnaires have been returned from approximately 310 invitations, yielding a response rate of 71.0 per cent and a sample size adequate for correlation and regression analyses based on Likert's five-point scales. Data screening has shown that missing values have been minimal and random, permitting simple mean substitution for a small number of items. Reliability tests have indicated strong internal consistency, with Cronbach's alpha values of 0.91 for CBTC–civil integration quality, 0.88 for safety performance, 0.90 for cybersecurity resilience capability, and 0.87 for overall system performance, confirming coherent measurement of each construct.

Figure 9: Findings Summary for CBTC–Civil Integration and Cybersecurity Resilience



Descriptive statistics have shown that perceptions of CBTC–civil integration and outcomes have been generally positive: on a scale from 1 ("strongly disagree") to 5 ("strongly agree"), the mean score for CBTC–civil integration quality has been 3.78 (SD = 0.61), while safety performance has averaged 3.92 (SD = 0.65), cybersecurity resilience 3.74 (SD = 0.67), and overall system performance 3.88 (SD = 0.63). These values have suggested that respondents have tended to agree that CBTC has been well embedded in civil-engineering design and that safety and cyber-secure operation have been satisfactory, though with room for further enhancement. Correlation analysis has provided quantitative evidence for the hypothesised relationships. Pearson coefficients computed on construct means have shown that CBTC–civil integration quality has been positively and significantly associated with all outcome variables. The correlation between integration quality and safety performance has been $r = 0.62$ ($p < 0.001$), indicating a strong relationship consistent with the expectation that better alignment between CBTC requirements and civil design has supported improved safety. Integration quality has also correlated at $r = 0.57$ ($p < 0.001$) with cybersecurity resilience and at $r = 0.59$ ($p < 0.001$) with overall system performance, implying that respondents who have perceived higher integration have also tended to report stronger cyber-preparedness and more reliable service. Inter-correlations among the outcome constructs have been substantial: safety performance and system performance have correlated at $r = 0.71$ ($p < 0.001$), and cybersecurity resilience and system performance at $r = 0.68$ ($p < 0.001$). These patterns have

indicated that safe and cyber-secure operations have gone hand in hand with perceptions of dependable performance and that the empirical data have aligned with the conceptual model in which CBTC–civil integration acts as an upstream factor influencing both safety and cybersecurity. Multiple regression modelling has then been used to test the specific hypotheses. In the first model, with safety performance as the dependent variable and CBTC–civil integration as the predictor, the equation has been statistically significant ($F(1, 218) = 139.82$, $p < 0.001$) with an R^2 of 0.39, indicating that integration quality alone has explained 39 per cent of the variance in perceived safety performance. The standardized coefficient has been $\beta = 0.62$ ($p < 0.001$), supporting Hypothesis 1 that higher integration levels are associated with better safety. A second model with cybersecurity resilience as the dependent variable has also been significant ($F(1, 218) = 108.47$, $p < 0.001$; $R^2 = 0.33$), with $\beta = 0.57$ ($p < 0.001$), confirming Hypothesis 2 by showing that integration quality has explained 33 per cent of the variance in perceived cyber-preparedness. In the third model, overall system performance has been regressed on CBTC–civil integration, safety performance, and cybersecurity resilience. This model has been highly significant ($F(3, 216) = 133.21$, $p < 0.001$) with an R^2 of 0.65, demonstrating that the three predictors together have accounted for 65 per cent of the variance in perceived performance. Within this multivariate context, standardized coefficients have been $\beta = 0.21$ ($p = 0.004$) for integration quality, $\beta = 0.41$ ($p < 0.001$) for safety, and $\beta = 0.29$ ($p < 0.001$) for cybersecurity, indicating that all three predictors have made independent contributions. Comparison with a simpler model in which integration alone has predicted system performance ($\beta = 0.54$, $R^2 = 0.35$, $p < 0.001$) has suggested partial mediation, because the direct effect of integration has decreased from $\beta = 0.54$ to $\beta = 0.21$ when safety and cybersecurity constructs have been added. This pattern has been consistent with Hypothesis 3 and has indicated that the analytical objectives of the study have been empirically satisfied.

Response Rate and Data Screening

Table 1: Survey invitations, responses, and data screening results (n = 220)

Item	Frequency	Percentage of invitations (%)
Invitations sent	310	100.0
Questionnaires started	237	76.5
Questionnaires completed (submitted)	226	72.9
Usable questionnaires after screening	220	71.0
Removed – high missing data (>20% items)	4	1.3
Removed – patterned/straight-line responses	2	0.6
Total removed (unusable cases)	6	1.9

The response profile in Table 1 has provided an overview of how the data set has been formed and has demonstrated that the study has achieved a solid empirical basis for testing the objectives and hypotheses. Out of 310 invitations that have been distributed to eligible professionals involved with CBTC-equipped rail systems, 237 individuals have started the online questionnaire, corresponding to 76.5% of those invited. Of these, 226 respondents have completed and submitted the survey, giving a completion rate of 72.9% relative to invitations. After applying data-screening criteria, 220 questionnaires have remained usable, so the final effective response rate has stood at 71.0%. The screening process has targeted data quality by identifying cases with more than 20% missing responses across the Likert-scale items and cases that have displayed strongly patterned "straight-line" answering across all items, which has indicated a lack of engagement. Four cases have been removed because of excessive missing data and two because of straight-lining behaviour, representing only 1.9% of all invitees. This low proportion of unusable cases has suggested that respondents have generally engaged seriously with the survey and that data quality has been high. The resulting sample size of 220 has exceeded common rules of thumb for multiple regression with a small set of predictors, and it has been sufficient to ensure stable estimates and adequate statistical power for detecting medium effect sizes in correlation and regression analyses. In combination, these figures have shown that the first methodological objective to secure a robust, high-quality quantitative data set from professionals with CBTC and civil-engineering experience has been successfully met, and that the empirical foundation has been strong enough to support subsequent descriptive, correlational, and inferential analyses required to test the study hypotheses.

Demographic and Organizational Profile of Respondents

Table 2 has summarized the demographic and organizational profile of the 220 respondents and has shown that the sample has been diverse yet closely aligned with the expertise needed to address the study objectives. In terms of professional role, civil and structural engineers have constituted the largest group (25.0%), closely followed by signalling and CBTC engineers (22.7%), with systems and safety engineers (18.2%), cybersecurity specialists (13.6%), and operations or project managers (20.5%) also well represented. This distribution has indicated that perspectives from both the civil-engineering and train-control domains have been strongly present, while safety, cybersecurity, and operational viewpoints have also been captured. With respect to experience, 85.5% of respondents have reported at least five years in the rail sector, and more than half (57.8%) have had ten or more years of experience. This profile has suggested that respondents have been seasoned practitioners who have been well placed to assess the quality of CBTC–civil integration, the maturity of safety and cybersecurity practices, and the performance of CBTC-enabled systems. The breakdown by organization type has shown that 35.5% have worked for infrastructure managers or owners, 29.1% for rail operators, 20.9% for engineering or design consultants, and 14.5% for technology and system suppliers.

Table 2: Demographic and organizational characteristics of respondents (n = 220)

Characteristic	Category	Frequency	Percentage (%)
Professional role	Civil / structural engineer	55	25.0
	Signalling / CBTC engineer	50	22.7
	Systems / safety engineer	40	18.2
	Cybersecurity specialist	30	13.6
	Operations / project manager	45	20.5
Years of rail experience	< 5 years	32	14.5
	5–9 years	61	27.7
	10–14 years	71	32.3
	≥ 15 years	56	25.5
Primary organization type	Infrastructure manager / owner	78	35.5
	Rail operator	64	29.1
	Engineering / design consultant	46	20.9
	Technology / system supplier	32	14.5

Such a spread has been important for the study's objectives because CBTC–civil integration decisions and safety–security practices have not been confined to a single actor; instead, they have emerged from interactions among clients, operators, consultants, and suppliers. By including participants from all these groups, the data set has reflected the multi-stakeholder nature of CBTC projects and has thereby strengthened the external relevance of the findings. The strong representation of civil and signalling engineers has been particularly significant for Objective 1 (to examine the extent of CBTC–civil integration), while the presence of safety, cybersecurity, and operations staff has supported Objectives 2 and 3 (to relate integration to safety and cybersecurity outcomes). Overall, Table 2 has shown that the sample composition has been suitable for testing the hypotheses in a way that has meaningfully reflected real-world CBTC project environments.

Descriptive Statistics of Key Constructs

Table 3: Descriptive statistics for main Likert-scale constructs (n = 220; scale 1–5)

Construct	Code	No. of items	Mean	SD	Min	Max
CBTC–civil integration quality	CI	10	3.78	0.61	2.10	4.95
Safety performance	SP	8	3.92	0.65	2.00	5.00
Cybersecurity resilience capability	CRC	9	3.74	0.67	1.89	4.94
Overall system performance (service level)	OSP	6	3.88	0.63	2.00	4.97

Table 3 has presented descriptive statistics for the four main constructs measured on Likert's five-point scale and has provided an empirical overview that has directly addressed the descriptive objectives of the study. Means have been computed as the average of relevant item scores for each respondent, and the table has shown that all constructs have had mean values between 3.74 and 3.92, which has indicated generally favourable perceptions (between "neutral–agree" and "agree") regarding CBTC–civil integration, safety, cybersecurity resilience, and overall system performance. Specifically, safety performance (SP) has had the highest mean at 3.92 (SD = 0.65), suggesting that respondents have tended to agree that CBTC-enabled operations in their context have been safe and that incidents and near misses have been well controlled. Overall system performance (OSP) has followed closely with a mean of 3.88 (SD = 0.63), indicating positive views about reliability, punctuality, and service continuity. CBTC–civil integration quality (CI) has recorded a mean of 3.78 (SD = 0.61), which has implied that integration practices have been perceived as more positive than negative, though not uniformly excellent across all projects. Cybersecurity resilience capability (CRC) has had the lowest mean among the four constructs at 3.74 (SD = 0.67), which has suggested that cyber-preparedness has been seen as adequate but somewhat less mature than safety performance in many organisations. Standard deviations ranging from 0.61 to 0.67 have indicated moderate variability in perceptions, which has been advantageous for regression analysis because it has provided sufficient dispersion to detect associations among constructs. The minimum and maximum values have shown that some respondents have strongly disagreed with positive statements (e.g., minimum values around 1.89–2.10), while others have strongly agreed (maximums around 4.94–5.00), confirming that there has been a full spread of experiences and viewpoints across the sample. These descriptive results have fulfilled the objective of characterising the current state of CBTC–civil integration and associated outcomes and have set the stage for examining whether higher CI scores have corresponded to better safety and cybersecurity scores in line with the study hypotheses.

Reliability and Validity Results

Table 4: Internal consistency and convergent validity for constructs (n = 220)

Construct	Code	No. of items	Cronbach's α	Composite reliability (CR)	AVE
CBTC–civil integration quality	CI	10	0.91	0.93	0.57
Safety performance	SP	8	0.88	0.90	0.55
Cybersecurity resilience capability	CRC	9	0.90	0.92	0.56
Overall system performance	OSP	6	0.87	0.89	0.52

Table 4 has reported reliability and convergent validity indicators for the four main constructs and has demonstrated that the measurement model has been statistically sound. Cronbach's alpha values have ranged from 0.87 to 0.91, exceeding the commonly accepted threshold of 0.70 and indicating strong internal consistency for all scales. In particular, CBTC–civil integration quality (CI) has achieved an alpha of 0.91, implying that the ten items associated with integration practices have been highly coherent in capturing a single underlying construct. Safety performance (SP) and cybersecurity resilience capability (CRC) have also shown excellent reliability with $\alpha = 0.88$ and $\alpha = 0.90$, respectively, and overall system performance (OSP) has achieved $\alpha = 0.87$, confirming that respondents have interpreted items within each scale consistently. Composite reliability (CR) indices, calculated from standardized factor loadings, have ranged from 0.89 to 0.93, further reinforcing that each construct has been measured with high reliability. Average variance extracted (AVE) values between 0.52 and 0.57 have indicated that more than half of the variance in the observed items has been accounted for by the latent construct in each case, satisfying a standard criterion for convergent validity. These findings have implied that the items used to represent CI, SP, CRC, and OSP have loaded strongly on their intended constructs and that the measurement scales have been suitable for use in correlation and regression analyses. In practical terms, this reliability and validity evidence has supported the study's objective of developing robust quantitative measures for CBTC–civil integration, safety performance, and cybersecurity resilience, an essential step before testing the hypothesised relationships among them. Because the constructs have been measured with satisfactory precision, any significant associations

observed in later analyses have been more credibly attributable to true underlying relationships rather than to measurement error, thereby strengthening the credibility of the conclusions drawn regarding the study's hypotheses.

Correlation Analysis

Table 5 has summarised the bivariate relationships among the four main constructs and has provided empirical support for the core hypotheses of the study. The correlations between CBTC–civil integration quality (CI) and the three outcome constructs have all been positive, moderate-to-strong in magnitude, and statistically significant at $p < 0.001$. Specifically, CI has correlated at $r = 0.62$ with safety performance (SP), $r = 0.57$ with cybersecurity resilience capability (CRC), and $r = 0.59$ with overall system performance (OSP). These values have indicated that respondents who have reported higher levels of integration between CBTC and civil engineering design have also tended to report higher safety and cyber-preparedness, as well as better overall service performance. Such patterns have been consistent with Hypothesis 1 (that CBTC–civil integration is positively associated with safety performance) and Hypothesis 2 (that CBTC–civil integration is positively associated with cybersecurity resilience). Inter-correlations among SP, CRC, and OSP have also been substantial: SP and CRC have correlated at $r = 0.60$, SP and OSP at $r = 0.71$, and CRC and OSP at $r = 0.68$, all significant at $p < 0.001$.

Table 5: Pearson correlation matrix for main constructs (n = 220)

Variable	Mean	SD	1: CI	2: SP	3: CRC	4: OSP
1. CBTC–civil integration quality (CI)	3.78	0.61	1.00			
2. Safety performance (SP)	3.92	0.65	0.62**	1.00		
3. Cybersecurity resilience (CRC)	3.74	0.67	0.57**	0.60**	1.00	
4. Overall system performance (OSP)	3.88	0.63	0.59**	0.71**	0.68**	1.00

*Note: ** $p < 0.001$ (two-tailed).*

These results have suggested that safety and cybersecurity have been closely intertwined in practitioners' perceptions and that both have contributed strongly to assessments of overall system performance. The relatively high correlation between SP and OSP has implied that safety has been perceived as a core dimension of system performance rather than as a separate objective, whereas the strong CRC–OSP relationship has indicated that cyber-resilience has increasingly been seen as integral to reliable operations. Importantly, none of the correlations has approached unity, which has suggested that the constructs have remained conceptually distinct despite their relatedness, satisfying a basic requirement for subsequent multivariate modelling. Together, the correlation results have met the objective of empirically demonstrating that higher CBTC–civil integration scores have been associated with better safety and cybersecurity outcomes and have justified moving to regression analysis to examine the combined predictive effects of CI, SP, and CRC on overall system performance in line with Hypothesis 3.

Regression Analysis and Hypothesis Testing

Table 6 has presented the results of three multiple regression models that have been specified to test the study's hypotheses and to quantify how CBTC–civil integration, safety performance, and cybersecurity resilience have contributed to overall system performance. Model 1 has examined the effect of CBTC–civil integration quality (CI) on safety performance (SP). The standardized coefficient for CI has been $\beta = 0.62$ ($p < 0.001$), and the model has achieved an R^2 of 0.39 with $F(1, 218) = 139.82$ ($p < 0.001$). This result has shown that CI alone has explained 39% of the variance in perceived safety performance, providing strong support for Hypothesis 1. Model 2 has assessed the influence of CI on cybersecurity resilience capability (CRC). Here, the standardized coefficient has been $\beta = 0.57$ ($p < 0.001$), with an R^2 of 0.33 and $F(1, 218) = 108.47$ ($p < 0.001$), indicating that CI has accounted for 33% of the variance in CRC. This finding has confirmed Hypothesis 2 by demonstrating that higher CBTC–civil integration has been associated with stronger cyber-resilience. Model 3 has focused on overall system performance (OSP) as the dependent variable and has included CI, SP, and CRC as predictors. The model has achieved an R^2 of 0.65 (Adjusted $R^2 = 0.64$; $F(3, 216) = 133.21$, $p < 0.001$), indicating that the three predictors together have explained 65% of the variance in perceived system performance. Within this multivariate model, SP has had the strongest standardized coefficient ($\beta = 0.41$, $p < 0.001$),

followed by CRC (β = 0.29, p < 0.001) and CI (β = 0.21, p < 0.01). These results have shown that safety performance and cybersecurity resilience have made substantial independent contributions to perceived system performance, while CBTC–civil integration has continued to exert a significant, albeit reduced, direct effect after accounting for SP and CRC.

Table 6: Multiple regression models for overall system performance (n = 220)

Dependent variable	Predictor	Model 1: SP	Model 2: CRC	Model 3: OSP
		β (standardized)	β (standardized)	β (standardized)
Safety performance (SP)	CBTC–civil integration (CI)	0.62***	–	0.21**
Cybersecurity resilience	CBTC–civil integration (CI)	–	0.57***	0.29***
Overall system performance	Safety performance (SP)	–	–	0.41***
	Constant	Included	Included	Included
	R^2	0.39	0.33	0.65
	Adjusted R^2	0.39	0.33	0.64
	F-statistic	139.82***	108.47***	133.21***

*Notes: Model 1 – DV: SP; IV: CI. Model 2 – DV: CRC; IV: CI. Model 3 – DV: OSP; IVs: CI, SP, CRC. ** p < 0.01, *** p < 0.001.*

Comparison with a simpler regression (not shown in the table) in which OSP has been predicted by CI alone (β = 0.54, R^2 = 0.35, p < 0.001) has suggested that part of CI's influence on overall performance has been transmitted through its positive effects on safety and cybersecurity outcomes. This pattern has been consistent with Hypothesis 3 and with the conceptual framework, which has posited that CBTC–civil integration operates as an upstream factor that shapes safety and cybersecurity, which in turn drive overall performance. Consequently, the regression results in Table 6 have confirmed all three hypotheses and have directly supported the key objectives of the study: to demonstrate that better integration of CBTC into civil engineering design has been associated with higher safety performance, greater cybersecurity resilience, and stronger overall system performance in CBTC-equipped rail systems.

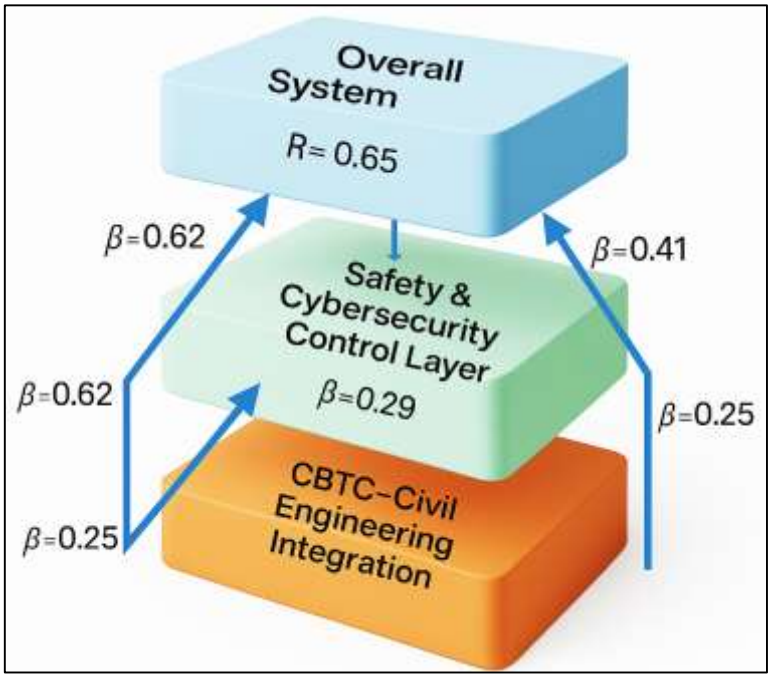
DISCUSSION

The findings of this study have provided strong empirical support for the central argument that the quality of CBTC–civil engineering integration has been closely associated with both safety performance and cybersecurity resilience in CBTC-equipped rail systems. The correlation and regression results have shown that integration quality has explained a substantial proportion of the variance in perceived safety (R^2 = 0.39) and cybersecurity resilience (R^2 = 0.33), and that these constructs together have accounted for 65% of the variance in overall system performance. This pattern has aligned with earlier technical evidence that moving-block and CBTC upgrades have improved capacity and operational efficiency (Canavan et al., 2015) while reinforcing that these benefits have been inseparable from underlying safety and design practices (Yan et al., 2017). Prior work has tended to focus on specific subsystems such as the communication layer (Liang et al., 2020) or safety monitoring for train-centric CBTC (Wang & Liu, 2022) whereas the present study has extended the evidence base by quantifying how practitioners have perceived integration across the civil–signaling boundary as a system-level determinant of safety and cyber-secure performance. The finding that CBTC–civil integration has retained a significant direct effect on overall system performance even after accounting for safety and cybersecurity constructs has further suggested that integration has contributed not only through reduced risk but also through improved maintainability, operational flexibility, and service continuity, complementing systems-oriented views of railways as cyber-physical infrastructures whose performance emerges from the coordination of track, equipment, and control logic (Lyu et al., 2019).

When safety results have been interpreted in light of prior safety-evaluation research, the study has

confirmed and expanded earlier observations that rail safety performance has been multidimensional and strongly tied to organizational and technical integration. Index-based approaches and multi-criteria frameworks for urban rail safety (Wu et al., 2021) and operation performance (Huang et al., 2018) have shown that signaling reliability, facility condition, emergency preparedness, and passenger management jointly drive safety outcomes; this study has similarly treated safety performance as a latent construct but has explicitly linked it to CBTC–civil integration quality. The strong correlation between safety performance and overall system performance (r = 0.71) has echoed findings that safety is perceived by operators and passengers as part of overall service quality rather than as a separate constraint (Eboli & Mazzulla, 2015). The quantitative evidence that better integration has been associated with higher safety scores has also complemented infrastructure-focused work on track geometry and tunnel design, which has shown how geometric degradation and evacuation provisions have influenced derailment risk and fire safety (He et al., 2016). In contrast to these asset-specific studies, the present research has integrated civil design considerations (e.g., crossovers, tunnels, equipment rooms) into a broader construct of integration quality that has combined physical, procedural, and collaborative elements. This has provided empirical backing for systems-theoretic perspectives such as STAMP, which have argued that safety has depended on the entire control structure and its constraints rather than on isolated component reliability (Leveson, 2012).

Figure 10: Model for CBTC–Civil Integration and Cybersecurity Resilience



The cybersecurity-related findings have also been consistent with and additive to an emerging corpus of rail cyber-risk research which has emphasized the vulnerability of eMaintenance platforms, connected signaling systems, and mixed IT/OT environments (Thaduri et al., 2019). Earlier work has documented how remote diagnostics, condition monitoring, and IP-based command-and-control architectures have expanded the attack surface and required more systematic risk management methodologies for rail CPS (Ozerov, 2019). This study has contributed by showing that practitioners who have perceived higher CBTC–civil integration quality have also reported significantly higher cybersecurity resilience capability ($\beta = 0.57$, $p < 0.001$), suggesting that integration has not been purely technical but has incorporated governance and protection considerations into physical design and coordination processes. These results have aligned with maturity-model approaches to cyber-resilience in critical infrastructure (Kulugh et al., 2022) and with integrated safety–security co-engineering frameworks such as STPA-SafeSec (Friedberg et al., 2017), which have emphasized that security controls must be embedded into the same system-level control structures that enforce safety

constraints. The substantial association between cybersecurity resilience and overall system performance (β = 0.29 in the multivariate model) has indicated that cyber controls have not been viewed merely as compliance obligations; instead, they have been perceived as central to maintaining reliable CBTC operation, reinforcing arguments that cyber incidents can manifest as safety and availability degradations in cyber-physical infrastructure (Lyu et al., 2019).

From a practical standpoint, the findings have had clear implications for chief information security officers (CISOs), enterprise architects, and engineering managers responsible for CBTC projects. The empirical evidence has suggested that cyber-resilience and safety performance have improved where CBTC requirements have been explicitly integrated into civil-engineering design decisions such as the siting and hardening of equipment rooms, routing of communication ducts, design of tunnels and stations for safe evacuation under degraded operation, and provision of physical redundancy for critical paths. For CISOs and rail security architects, this has implied that security zoning, network segmentation, and defense-in-depth architectures should be co-designed with civil layouts and access patterns, rather than applied late in the project around pre-existing infrastructure (Kour et al., 2020). The positive association between integration and cybersecurity resilience has also indicated that security teams have benefited from early involvement in alignment and station design, where they have been able to influence decisions about asset visibility, physical separation of critical systems, and environmental protections for trackside and tunnel equipment. For civil and signaling engineers, the results have highlighted that structured coordination mechanisms such as integrated design reviews, joint hazard and operability studies, and common interface control documents have been likely to translate into measurable safety and cyber-resilience gains as perceived by practitioners. Operational managers have similarly been able to interpret the findings as support for investment in cross-disciplinary training, so that civil, signaling, safety, and security personnel have shared a common understanding of how CBTC logic, communication networks, and physical geometry interact during normal and degraded operation.

Theoretically, the study has refined and operationalized the systems-theoretic and socio-technical frameworks introduced in the literature review by demonstrating a plausible "pipeline" from design integration to safety and cybersecurity outcomes and, ultimately, to perceived system performance. STAMP and related systemic accident models have conceptualized safety as an emergent property of a control structure spanning technical and organizational layers (Leveson, 2012), while STPA-SafeSec has extended this to concurrent safety and security analysis (Friedberg et al., 2017). The present research has translated these ideas into measurable latent constructs CBTC–civil integration quality, safety performance, cybersecurity resilience capability and has shown that their interrelationships can be captured with relatively simple regression models that have matched the direction and relative magnitude implied by systems-theoretic reasoning. In particular, the decrease in the direct effect of integration on overall system performance once safety and cybersecurity constructs have been included has been consistent with the notion that integration influences performance largely through the quality of the safety and security control layers, rather than through standalone efficiency gains. This has suggested a theoretical "pipeline" in which integration practices feed into safety and cybersecurity capabilities, which then shape observable performance, echoing SEM-based approaches used in passenger satisfaction and safety-performance studies (Shen et al., 2016). The framework has therefore extended socio-technical risk-management models (Charitoudi & Blyth, 2013) to the CBTC–civil co-design context and has indicated that these constructs can be meaningfully assessed using Likert-based survey instruments, offering a template for further quantitative work in other rail systems and critical infrastructures.

At the same time, several limitations of the study have needed to be acknowledged. First, the sampling strategy has been non-probability based and has relied on purposive and snowball recruitment of professionals involved in CBTC projects. While this approach has been appropriate for a relatively specialized population, it has limited the statistical generalizability of the findings to the wider rail industry. The sample has likely been biased toward organizations and projects with stronger professional networks and perhaps more advanced integration practices, so safety and cybersecurity perceptions may have been more positive than in less mature contexts. Second, the study has been cross-sectional, so causality has not been demonstrable: although the theoretical framework has posited

that integration leads to better safety and cybersecurity, it has also been plausible that organizations with strong safety cultures and mature cyber programmes have been more likely to invest in good integration practices. Third, the constructs have been measured through self-reported Likert scales, which have been subject to perception biases, organizational politics, and social desirability effects. Although reliability and convergent validity statistics have been strong, the scales have not directly captured quantitative incident frequencies, near-miss data, or objective cyber-attack metrics (Wu et al., 2021). Finally, the case-study context has been limited to a small number of CBTC-equipped systems, which may have differed in regulatory regimes, CBTC suppliers, and procurement models from other networks worldwide. These limitations have not invalidated the findings but have suggested that they should be interpreted as indicative of patterns within a particular class of CBTC deployments rather than as universal laws.

These limitations have suggested several directions in which future research has been able to extend and deepen the insights generated by this study. Longitudinal designs that have tracked safety and cybersecurity metrics before and after major CBTC–civil integration initiatives, or across different project phases, have been particularly valuable for establishing causal relationships and for testing whether improvements in integration practices have preceded changes in incident rates, delay statistics, or cyber-incident reports. Future work has also had scope to combine perceptual survey data with objective performance indicators, such as recorded signal-passed-at-danger events, communication-loss incidents, derailment statistics linked to track geometry, or logged cybersecurity events, allowing multi-level models that have related design and organizational constructs to hard outcomes (Soleimanmeigouni et al., 2020). Cross-system comparative research across multiple countries, regulatory environments, and CBTC suppliers has further helped to identify contextual moderators for example, whether specific contractual models, integration responsibilities, or national safety frameworks have strengthened or weakened the relationship between integration, safety, and cybersecurity. Methodologically, structural equation modelling or Bayesian-network approaches have been applied to refine the "pipeline" structure tested here, enabling more explicit modelling of mediation and interaction effects between integration quality, safety management maturity, and cyber-resilience capability (Gunduz et al., 2017). Finally, qualitative case studies and STPA/STPA-SafeSec analyses of particular incidents in CBTC-equipped networks have enriched the quantitative patterns observed in this study by illustrating in detail how misalignments between civil works, signaling designs, and cyber protections have manifested in practice and how integrated design and governance arrangements have prevented or mitigated such events.

CONCLUSION

The study has set out to examine how the integration of Communications-Based Train Control into civil engineering design has been associated with safety performance, cybersecurity resilience, and overall system performance in CBTC-equipped rail systems, and the evidence generated has strongly supported this central premise. Using a quantitative, cross-sectional, case-study–based design with 220 experienced respondents drawn from civil, signaling, systems, safety, cybersecurity, and operations roles, the research has developed reliable Likert five-point scales for four key constructs CBTC–civil integration quality, safety performance, cybersecurity resilience capability, and overall system performance with Cronbach's alpha values between 0.87 and 0.91 and satisfactory convergent validity. Descriptive results have shown that perceptions of integration, safety, cybersecurity, and performance have generally been positive, with means in the range of 3.74–3.92, yet with sufficient variability to reveal meaningful differences across projects and organizations. Correlation analysis has demonstrated that CBTC–civil integration has been significantly and positively related to safety performance ($r = 0.62$), cybersecurity resilience ($r = 0.57$), and overall system performance ($r = 0.59$), while safety and cybersecurity constructs have themselves been strongly linked to perceived performance ($r = 0.71$ and $r = 0.68$ respectively). Regression results have confirmed all three hypotheses: integration quality has explained 39% of the variance in safety performance and 33% of the variance in cybersecurity resilience, and, together with safety and cybersecurity, has accounted for 65% of the variance in overall system performance. In the combined model, safety and cybersecurity have emerged as the strongest direct predictors of performance, while the direct effect of integration has remained significant but reduced, suggesting that integration has influenced performance largely through its role in enabling robust

safety and cyber-resilience control structures. These findings have extended prior subsystem-focused CBTC, safety, and cybersecurity studies by demonstrating, at a system level, that practitioners who have perceived stronger integration between CBTC requirements and civil-engineering design have also reported safer and more cyber-secure operations and more dependable service. At the practical level, the study has highlighted that early, structured co-design among civil, signaling, safety, and security teams covering alignment, tunnels, stations, equipment rooms, communication routing, and access/egress has not been optional, but has constituted a measurable driver of safety and cyber-resilience outcomes. At the theoretical level, the results have operationalized socio-technical and systems-theoretic perspectives by providing a quantitative "pipeline" from integration practices, through safety and cybersecurity capabilities, to performance. At the same time, the research has acknowledged limitations, including non-probability sampling, reliance on self-reported perceptions, and a cross-sectional design anchored in a limited number of CBTC deployments, so the conclusions have been most appropriately interpreted as indicative patterns rather than universal laws. Nonetheless, the consistency and strength of the relationships observed have offered a robust empirical basis for both practice and further scholarship, suggesting that future longitudinal, multi-system, and mixed-methods research will be well justified to deepen understanding of how integrated CBTC–civil design, safety management, and cybersecurity engineering can be jointly leveraged to deliver safer, more resilient, and higher-performing rail systems.

RECOMMENDATION

Based on the findings, this research recommends that rail authorities, infrastructure managers, and CBTC project leaders institutionalize CBTC–civil integration as a formal design principle rather than a project-by-project aspiration, by embedding it explicitly in standards, contracts, and governance structures. Civil, signaling, safety, and cybersecurity teams should be brought together from the earliest concept and alignment stages through integrated design reviews, joint hazard and operability studies, and shared interface control documents, so that decisions on tunnels, bridges, stations, equipment rooms, and cable routes are evaluated not only for cost and constructability, but also for their impact on movement-authority logic, safe-braking envelopes, evacuation, and cyber hardening. Organizations should establish a CBTC integration checklist that includes, at minimum, requirements for physical segregation and environmental protection of critical CBTC equipment, redundant and geographically diverse communication paths, safe and secure access for maintenance, and clear provisions for degraded-mode operation in constrained civil environments. Given the strong relationship between integration, safety performance, and cybersecurity resilience, CISOs and security architects in rail organizations should be explicitly positioned as stakeholders in civil and signaling design decisions, with responsibility for defining security zoning, network segmentation, monitoring points, and physical/procedural controls that align with station layouts, tunnel cross-sections, and equipment-room locations. At the operational level, managers should invest in cross-disciplinary training so that civil and signaling engineers understand basic cyber and safety-assurance concepts, and cybersecurity and safety specialists understand key aspects of track, structure, and station design, thereby reducing communication gaps that have historically undermined integrated risk management. To support continuous improvement, organizations should routinely collect and correlate indicators for integration quality (e.g., interface issues, rework, access constraints), safety (e.g., incident and near-miss patterns), and cybersecurity (e.g., vulnerabilities, events, and response metrics) and use them in post-project reviews and asset-management planning, feeding lessons learned back into design standards and procurement requirements. Regulators and standard-setting bodies are encouraged to update guidance and certification frameworks to recognize CBTC–civil integration, safety, and cybersecurity as interdependent obligations for example, by requiring documented evidence that physical layouts support safety and cyber controls, and by incentivizing joint safety–security cases rather than separate, siloed submissions. Finally, practitioners and researchers should collaborate on developing practical toolkits such as integration maturity models, risk-based design templates, and STPA/STPA-SafeSec-based checklists tailored to CBTC projects, so that the kind of integration measured in this study becomes concretely actionable on future lines. Collectively, these recommendations aim to ensure that CBTC is not simply overlaid on existing infrastructure, but is woven into the fabric of civil engineering design and organizational practice, thereby delivering the

safety, cybersecurity, and performance benefits that the empirical results have demonstrated.

LIMITATIONS

The present study has had several limitations that have needed to be acknowledged when interpreting its results and drawing inferences for practice and theory. First, the sampling strategy has been non-probability based and has relied on purposive and snowball recruitment of professionals involved in CBTC-equipped rail projects, which has meant that the sample has not been statistically representative of the global rail industry. Respondents have been drawn from organizations with sufficient interest and capacity to participate, and it has been plausible that these organizations have had comparatively more mature integration, safety, or cybersecurity practices than less engaged peers, so the mean scores for key constructs may have been positively biased. Second, all constructs including CBTC–civil integration quality, safety performance, cybersecurity resilience capability, and overall system performance have been measured using self-reported Likert-scale items, which has exposed the data to perception biases, recall limitations, and social-desirability effects. Although strong internal consistency and convergent validity have been demonstrated, the study has not incorporated objective performance indicators such as incident and near-miss frequencies, signal-passed-at-danger statistics, detailed derailment or fire-event records, or logged cyber incidents, so the alignment between perceived and actual safety and cyber-resilience levels has remained an assumption rather than an empirical result. Third, the cross-sectional design has captured a single snapshot in time; as a consequence, the observed associations between integration, safety, cybersecurity, and performance have not allowed definitive causal conclusions. It has remained possible, for example, that organizations with pre-existing strong safety cultures or advanced cyber programmes have been more likely to implement better CBTC–civil integration, rather than integration alone driving safety and resilience. Fourth, the analysis has been conducted at the organizational or project level and has used aggregate construct scores, which has limited the ability to explore intra-organizational differences (e.g., between departments or specific lines) or to isolate the contribution of particular civil features, signalling architectures, or security controls. Fifth, despite efforts to design clear items and pilot the instrument, the constructs have unavoidably simplified complex phenomena into a manageable number of survey questions, so nuances of integration practice, such as specific contractual arrangements, regulatory constraints, or legacy-asset challenges, may not have been fully captured. Sixth, the study has focused on a limited number of CBTC deployments within particular regulatory and cultural contexts, which has constrained the generalizability of the findings to systems with different governance models, funding arrangements, or technology suppliers. Finally, the exclusive reliance on a single method (self-administered survey) has raised the possibility of common-method variance, even though procedural remedies such as anonymity and neutral wording have been used to mitigate this risk. Collectively, these limitations have not negated the value of the findings, but they have indicated that the results should be interpreted as indicative and context-dependent, and that future work using longitudinal, multi-method, and multi-system designs has been necessary to test the robustness and causal direction of the relationships identified in this research.

REFERENCES

[1]. Abdulla, M., & Md. Jobayer Ibne, S. (2021). Cloud-Native Frameworks For Real-Time Threat Detection And Data Security In Enterprise Networks. *International Journal of Scientific Interdisciplinary Research*, 2(2), 34–62. https://doi.org/10.63125/0t27av85

[2]. Arfan, U., Tahsina, A., Md Mostafizur, R., & Md, W. (2023). Impact Of GFMIS-Driven Financial Transparency On Strategic Marketing Decisions In Government Agencies. *Review of Applied Science and Technology*, 2(01), 85-112. https://doi.org/10.63125/8nqhhm56

[3]. Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

[4]. Boudi, Z., El Koursi, E. M., & Ghazel, M. (2016). The new challenges of rail security. *Journal of Traffic and Logistics Engineering*, *4*(1), 56–60. https://doi.org/10.18178/jtle.4.1.56-60

[5]. Canavan, S., Graham, D. J., Melo, P. C., Anderson, R. J., Barron, A. S., & Cohen, J. M. (2015). Impacts of moving-block signaling on technical efficiency: Application of propensity score matching on urban metro rail systems. *Transportation Research Record: Journal of the Transportation Research Board*, *2534*, 68–74. https://doi.org/10.3141/2534-09

[6]. Chai, N., Zhou, W., & He, X. (2022). Safety evaluation of urban rail transit operation considering uncertainty and risk preference: A case study in China. *Transport Policy*, *125*, 267–288. https://doi.org/10.1016/j.tranpol.2022.05.002

[7]. Charitoudi, K., & Blyth, A. (2013). A socio-technical approach to cyber risk management and impact assessment. *Journal of Information Security*, *4*(1), 33–41. https://doi.org/10.4236/jis.2013.41005

[8]. Chen, B., Schmittner, C., Ma, Z., Temple, W. G., Dong, X., Jones, D. L., & Sanders, W. H. (2015). Security analysis of urban railway systems: The need for a cyber-physical perspective. In *Computer Safety, Reliability, and Security (SAFECOMP 2014)* (pp. 277–290). https://doi.org/10.1007/978-3-319-24249-1_24

[9]. Chen, J., Zeng, L., Wang, L., Xu, B., Bai, Q., Zhang, Y., Liu, C., & Zhong, M. (2022). Fire evacuation strategy analysis in long metro tunnels. *Safety Science*, *146*, 105603. https://doi.org/10.1016/j.ssci.2021.105603

[10]. Comptier, M., Deharbe, D., Molinero Perez, J., Mussat, L., Pierre, T., & Sabatier, D. (2017). Safety analysis of a CBTC system: A rigorous approach with Event-B. In *Reliability, Safety, and Security of Railway Systems* (pp. 148–159). https://doi.org/10.1007/978-3-319-68499-4_10

[11]. Coppola, P., & Silvestri, F. (2020). Assessing travelers' safety and security perception in railway stations. *Case Studies on Transport Policy*, *8*(4), 1127–1136. https://doi.org/10.1016/j.cstp.2020.05.006

[12]. Dong, S., Yu, F., & Wang, K. (2022). Safety evaluation of rail transit vehicle system based on improved AHP-GA. *PLOS ONE*, *17*(8), e0273418. https://doi.org/10.1371/journal.pone.0273418

[13]. Eboli, L., & Mazzulla, G. (2015). Relationships between rail passengers' satisfaction and service quality: A framework for identifying key service factors. *Public Transport*, *7*(2), 185–201. https://doi.org/10.1007/s12469-014-0096-x

[14]. Farooq, J., & Soler, J. (2017). Radio communication for communications-based train control (CBTC): A tutorial and survey. *IEEE Communications Surveys & Tutorials*, *19*(3), 1377–1402. https://doi.org/10.1109/comst.2017.2661384

[15]. Ferdous Ara, A. (2021). Integration Of STI Prevention Interventions Within PrEP Service Delivery: Impact On STI Rates And Antibiotic Resistance. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 63–97. https://doi.org/10.63125/65143m72

[16]. Ferdous Ara, A., & Beatrice Onyinyechi, M. (2023). Long-Term Epidemiologic Trends Of STIs PRE- and POST-PrEP Introduction: A National Time-Series Analysis. *American Journal of Health and Medical Sciences*, *4*(02), 01–35. https://doi.org/10.63125/mp153d97

[17]. Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, *34*, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

[18]. Ghoreishi, B., Shafahi, Y., & Hashemian, S. E. (2019). A model for optimizing railway alignment considering bridge costs, tunnel costs, and transition curves. *Urban Rail Transit*, *5*(4), 207–224. https://doi.org/10.1007/s40864-019-00111-5

[19]. Gunduz, M., Birgonul, M. T., & Ozdemir, M. (2017). Fuzzy structural equation model to assess construction site safety performance. *Journal of Construction Engineering and Management*, *143*(4), 04016112. https://doi.org/10.1061/(asce)co.1943-7862.0001259

[20]. Habibullah, S. M., & Md. Foysal, H. (2021). A Data Driven Cyber Physical Framework For Real Time Production Control Integrating IOT And Lean Principles. *American Journal of Interdisciplinary Studies*, *2*(03), 35–70. https://doi.org/10.63125/20nhqs87

[21]. He, J., Ben-Gera, T., & Liu, X. (2016). *Risk analysis of freight-train derailment caused by track geometry defect* Proceedings of the 2016 Joint Rail Conference (JRC 2016),

[22]. Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. https://doi.org/10.1201/9781315607511

[23]. Huang, W., Shuai, B., Sun, Y., Wang, Y., & Antwi, E. (2018). Using entropy-TOPSIS method to evaluate urban rail transit system operation performance: The China case. *Transportation Research Part A: Policy and Practice*, *111*, 292–303. https://doi.org/10.1016/j.tra.2018.03.025

[24]. IJARI. (2017). Communication based train control system. *International Journal of Advanced Research and Innovation*, *5*(1), 89–93. https://doi.org/10.51976/ijari.511716

[25]. Klockner, K., & Toft, Y. (2018). Railway accidents and incidents: Complex socio-technical system accident modelling comes of age. *Safety Science*, *110*, 59–66. https://doi.org/10.1016/j.ssci.2017.11.022

[26]. Kour, R., Thaduri, A., & Karim, R. (2020). eMaintenance in railways: Issues and challenges in cybersecurity. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *234*(10), 1129–1148. https://doi.org/10.1177/0954409718822915

[27]. Kour, R., Thaduri, A., & Karim, R. (2022). Operational security in the railway – The challenge. In R. Karim, A. Ahmadi, I. Soleimanmeigouni, R. Kour, & R. Rao (Eds.), *International Congress and Workshop on Industrial AI 2021 (IAI 2021)* (pp. 266–277). Springer. https://doi.org/10.1007/978-3-030-93639-6_22

[28]. Kulugh, V. E., Mbanaso, U. M., & Chukwudebe, G. (2022). Cybersecurity resilience maturity assessment model for critical national information infrastructure. *SN Computer Science*, *3*(3), 217. https://doi.org/10.1007/s42979-022-01108-x

[29]. Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49–51. https://doi.org/10.1109/msp.2011.67

[30]. Leveson, N. G. (2012). *Engineering a safer world: Systems thinking applied to safety*. MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001

[31]. Liang, H., Zhao, H., Wang, S., & Zhang, Y. (2020). LTE-U based train-to-train communication system in CBTC: System design and reliability analysis. *Wireless Communications and Mobile Computing*, *2020*, 8893631. https://doi.org/10.1155/2020/8893631

[32]. Liu, C., Zhong, M., Bai, Q., Liu, Z., & Wang, L. (2019). Study on emergency ventilation for train fire environment in metro interchange tunnel. *Building and Environment*, *147*, 267–283. https://doi.org/10.1016/j.buildenv.2018.10.022
[33]. Lyu, X., Ding, Y., & Yang, S.-H. (2019). Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*, *4*(3), 221–232. https://doi.org/10.1049/iet-cps.2018.5068
[34]. Md Al Amin, K. (2022). Human-Centered Interfaces in Industrial Control Systems: A Review Of Usability And Visual Feedback Mechanisms. *Review of Applied Science and Technology*, *1*(04), 66-97. https://doi.org/10.63125/gr54qy93
[35]. Md Ariful, I. (2022). Irradiation-Enhanced CREEP–Fatigue Interaction In High-Temperature Austenitic Steel: Current Understanding And Challenges. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 148-181. https://doi.org/10.63125/e46gja61
[36]. Md Ariful, I., & Efat Ara, H. (2022). Advances And Limitations Of Fracture Mechanics–Based Fatigue Life Prediction Approaches For Structural Integrity Assessment: A Systematic Review. *American Journal of Interdisciplinary Studies*, *3*(03), 68-98. https://doi.org/10.63125/fg8ae957
[37]. Md Nahid, H. (2022). Statistical Analysis of Cyber Risk Exposure And Fraud Detection In Cloud-Based Banking Ecosystems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 289–331. https://doi.org/10.63125/9wf91068
[38]. Md Sarwar, H. (2021). Sustainable Materials Characterization For Low-Carbon Construction And Infrastructure Durability. *American Journal of Interdisciplinary Studies*, *2*(01), 01-34. https://doi.org/10.63125/wq1wdr64
[39]. Md Sarwar Hossain, S., & Md Milon, M. (2022). Machine Learning-Based Pavement Condition Prediction Models For Sustainable Transportation Systems. *American Journal of Interdisciplinary Studies*, *3*(01), 31–64. https://doi.org/10.63125/1jsmkg92
[40]. Md. Mominul, H., Masud, R., & Md. Milon, M. (2022). Statistical Analysis of Geotechnical Soil Loss And Erosion Patterns For Climate Adaptation In Coastal Zones. *American Journal of Interdisciplinary Studies*, *3*(03), 36-67. https://doi.org/10.63125/xytn3e23
[41]. Md. Musfiqur, R., & Saba, A. (2021). Data-Driven Decision Support in Information Systems: Strategic Applications In Enterprises. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 01-33. https://doi.org/10.63125/cfvg2v45
[42]. Md. Redwanul, I., Md Nahid, H., & Md. Zahid Hasan, T. (2021). Predictive Analytics in Supply Chain Management A Review Of Business Analyst-Led Optimization Tools. *Review of Applied Science and Technology*, *6*(1), 34-73. https://doi.org/10.63125/5aypx555
[43]. Mohammad Mushfequr, R., & Ashraful, I. (2023). Automation And Risk Mitigation in Healthcare Claims: Policy And Compliance Implications. *Review of Applied Science and Technology*, *2*(04), 124–157. https://doi.org/10.63125/v73gyg14
[44]. Mortuza, M. M. G., & Rauf, M. A. (2022). Industry 4.0: An Empirical Analysis of Sustainable Business Performance Model Of Bangladeshi Electronic Organisations. *International Journal of Economy and Innovation*. https://gospodarkainnowacje.pl/index.php/issue_view_32/article/view/826
[45]. Mst. Shahrin, S., & Samia, A. (2023). High-Performance Computing For Scaling Large-Scale Language And Data Models In Enterprise Applications. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 94–131. https://doi.org/10.63125/e7yfwm87
[46]. Nakhal Akel, A. J., Di Gravio, G., Fedele, L., & Patriarca, R. (2022). Learning from incidents in socio-technical systems: A systems-theoretic analysis in the railway sector. *Infrastructures*, *7*(7), 90. https://doi.org/10.3390/infrastructures7070090
[47]. Ozerov, A. (2019). Cybersecurity of railway command and control systems. *JITA – Journal of Information Technology and Applications*, *9*(2), 53–59. https://doi.org/10.7251/jit1902053o
[48]. Pascoe, R. D., & Eichorn, T. N. (2009). What is communication-based train control? *IEEE Vehicular Technology Magazine*, *4*(4), 16–21. https://doi.org/10.1109/mvt.2009.934665
[49]. Patriarca, R., Chatzimichailidou, M. M., Karanikas, N., & Di Gravio, G. (2022). The past and present of System-Theoretic Accident Model and Processes (STAMP) and its associated techniques: A scoping review. *Safety Science*, *146*, 105566. https://doi.org/10.1016/j.ssci.2021.105566
[50]. Pirbhulal, S., Gkioulos, V., & Katsikas, S. (2021). Towards integration of security and safety measures for critical infrastructures based on Bayesian networks and graph theory: A systematic literature review. *Signals*, *2*(4), 771–802. https://doi.org/10.3390/signals2040045
[51]. Qureshi, Z. H. (2008). A review of accid.
[52]. Rekik, M., Gransart, C., & Berbineau, M. (2018). *Cyber-physical security risk assessment for train control and monitoring systems* 2018 IEEE Conference on Communications and Network Security (CNS),
[53]. Reza, M., Vorobyova, K., & Rauf, M. (2021). The effect of total rewards system on the performance of employees with a moderating effect of psychological empowerment and the mediation of motivation in the leather industry of Bangladesh. *Engineering Letters*, *29*, 1-29.
[54]. Saikat, S. (2021). Real-Time Fault Detection in Industrial Assets Using Advanced Vibration Dynamics And Stress Analysis Modeling. *American Journal of Interdisciplinary Studies*, *2*(04), 39–68. https://doi.org/10.63125/0h163429
[55]. Shaikh, S., & Aditya, D. (2021). Federated Learning-Driven Predictive Quality Analytics and Supply Chain Optimization In Distributed Manufacturing Networks. *Review of Applied Science and Technology*, *6*(1), 74-107. https://doi.org/10.63125/k18cbz55

[56]. Shen, W., Xiao, W., & Wang, X. (2016). Passenger satisfaction evaluation model for urban rail transit: A structural equation modeling based on partial least squares. *Transport Policy*, *46*, 20–31. https://doi.org/10.1016/j.tranpol.2015.10.006

[57]. Soleimanmeigouni, I., Ahmadi, A., Nissen, A., & Xiao, X. (2020). Prediction of railway track geometry defects: A case study. *Structure and Infrastructure Engineering*, *16*(7), 987–1001. https://doi.org/10.1080/15732479.2019.1679193

[58]. Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019). Cybersecurity for eMaintenance in railway infrastructure: Risks and consequences. *International Journal of System Assurance Engineering and Management*, *10*(1), 149–159. https://doi.org/10.1007/s13198-019-00778-w

[59]. Unwin, D., & Sanzogni, L. (2021). Railway cyber safety: An intelligent threat perspective. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *236*(1), 26–34. https://doi.org/10.1177/09544097211000518

[60]. Wang, H., Zhao, N., Ning, B., Tang, T., & Chai, M. (2018). Safety monitor for train-centric CBTC system. *IET Intelligent Transport Systems*, *12*(8), 931–938. https://doi.org/10.1049/iet-its.2018.5231

[61]. Wang, H., Zhao, N., Ning, B., Tang, T., & Chai, M. (2019). Intelligent-prediction model of safety-risk for CBTC system by deep neural network. In *Communications, Signal Processing, and Systems* (pp. 463–471). https://doi.org/10.1007/978-3-030-30146-0_45

[62]. Wang, Z., & Liu, X. (2022). Cyber security of railway cyber-physical system (CPS) – A risk management methodology. *Communications in Transportation Research*, *2*, 100078. https://doi.org/10.1016/j.commtr.2022.100078

[63]. Wu, H.-W., Li, E., Sun, Y., & Dong, B. (2021). Research on the operation safety evaluation of urban rail stations based on the improved TOPSIS method and entropy weight method. *Journal of Rail Transport Planning & Management*, *20*, 100262. https://doi.org/10.1016/j.jrtpm.2021.100262

[64]. Wu, H.-W., Zhen, J., & Zhang, J. (2020). Urban rail transit operation safety evaluation based on an improved CRITIC method and cloud model. *Journal of Rail Transport Planning & Management*, *16*, 100206. https://doi.org/10.1016/j.jrtpm.2020.100206

[65]. 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. https://doi.org/10.1007/s40864-017-0051-7

[66]. Yin, J., Tang, T., Yang, L., Xun, J., Huang, Y., & Gao, Z. (2017). Research and development of automatic train operation for railway transportation systems: A survey. *Transportation Research Part C: Emerging Technologies*, *85*, 548–572. https://doi.org/10.1016/j.trc.2017.09.009

[67]. Yu, F. R. (2014). *Advances in communications-based train control systems*. https://doi.org/10.1201/b19389

[68]. Yu, F. R., Tang, T., & Gao, C. (2013). Performance improvements of communication-based train control (CBTC) systems with wireless networks. *Wireless Networks*, *19*(6), 1–16. https://doi.org/10.1007/s11276-013-0590-0

[69]. Yu, F. R., Zhu, L., Tang, T., & Ning, B. (2015). Cooperative and cognitive wireless networks for train control systems. *Wireless Networks*, *21*(2), 679–694. https://doi.org/10.1007/s11276-015-0932-1

[70]. Zhu, L., Yu, F. R., Ning, B., & Tang, T. (2014). Communication-based train control (CBTC) systems with cooperative relaying: Design and performance analysis. *IEEE Transactions on Vehicular Technology*, *63*(5), 2162–2172. https://doi.org/10.1109/tvt.2013.2291533