Action-based security rules for railway control systems

Action-Based Security Rules for Railway Control Systems

Rocco De Nicola[1,3], Simone Soderi[2,3]

[1] IIT – CNR Pisa Italy
rocco.denicola@iit.cnr.it
[2] IMT School for Advanced Studies Lucca, Lucca, Italy
simone.soderi@imtlucca.it
[3] Cybersecurity National Laboratory, CINI - Roma, Italy

Abstract. This paper presents an *action-based* methodology for securing railway signalling systems, building upon the TS 50701 framework. In TS 50701, zones represent groups of assets that share common security requirements, while conduits denote controlled communication channels that interconnect zones and enforce defined security policies. Railway systems described within this framework comprise wayside and onboard components, interconnected by a Data Communication System (DCS). We propose an attacker model centred on inter-zone conduits that specifies enforceable rule templates for each conduit. These templates define requirements for source authentication, integrity, freshness, and semantic consistency, thereby constraining permissible behaviours that can be implemented at boundary monitors. Through qualitative security analysis, we demonstrate how these rules address specific threats and trace how security degradations may propagate to safety-critical effects. By formalising zones and conduits as terms in a process description language, system properties can be expressed as sequences of observable actions. This formalisation enables the use of Action-Based Temporal Logic (ACTL) to verify whether security properties are guaranteed, which constitutes our long-term research goal.

Keywords: Railway signalling · TS 50701 · Process Description Languages · Temporal Logic · Cybersecurity Assessment · Safety

1 Introduction

Railway signalling has evolved into a distributed, software-intensive system in which control logic and traffic management exchange critical information across heterogeneous networks.

The progressive digitalisation of railway signalling has increased exposure to cyber threats across operational technology domains. IXL, RBC, ATS/OCCs, and lineside equipment exchange information over heterogeneous networks and protocols; misconfiguration or malicious manipulation of these systems can degrade availability or integrity and, in extreme cases, create conditions that stress safety margins [26,8].

In this setting, cybersecurity measures must be implemented to enable operators to monitor and intervene at both the interfaces between *zones* and along the *conduits* that connect them, as prescribed by TS 50701:2021 (which will be replaced in mid-2026 by the IEC 63452 standard) and related guidance [3,10]. While modelling systems in terms of zones and channels is important, it is equally crucial to examine whether a gap exists between these architectural artifacts and the cybersecurity requirements applicable to safety-critical railway systems.

The industry guidelines defined by TS 50701 structure System under Consideration (SuC) cybersecurity by creating logical elements called *zones* and *ducts*. Meanwhile, ENISA details a zoning/ducting methodology for the railway sector, providing concrete architectural models and risk management practices [3,10].

In the reference architecture of the European Rail Traffic Management System / European Train Control System (ERTMS / ETCS), the functions are partitioned between subsystems *trackside* and *onboard*. Trackside comprises the *Interlocking* (IXL) with train detection, the *Lineside Electronics Units* (LEU) driving balises, the *Radio Block Centre* (RBC), and the *Global System for Mobile Communications–Railway* (GSM-R). Onboard, the *European Train Control System* (ETCS) equipment supervises train movement using odometry and balise updates via the Driver Machine Interface (DMI); Automatic Train Operation (ATO) over ETCS can be added to execute driving profiles under ETCS supervision. At Level 2[1], the RBC issues Movement Authorities (MAs) over the radio link while eurobalises provide position reference; at Level 1, movement authorities are conveyed at fixed points through eurobalises/loops. The Operations Control Centre (OCC) hosts Automatic Train Supervision (ATS), which plans traffic and interfaces with IXL and RBC to coordinate routing and movement authority delivery across the corridor [9].

Accordingly, this paper adopts an *action-based* perspective, defining abstract zones and exposing observable actions, namely commands, indications, and authority updates. Security requirements are then expressed over admissible action traces using Action-Based Temporal Logic (ACTL) [6]. We propose enforceable action-based rules on the conduits among railway systems to prevent malicious manipulation of commands, indications, and movement authorities, aligning these controls with TS 50701. The choice is pragmatic: action-level properties align with how rail operators monitor and gate traffic on conduits, and compose with established formal results for signalling (e.g., interlocking verification and model-based environments) without imposing heavyweight verification on the entire system [19,12].

Grounded in this zoning-and-conduits view, the objective here is to model *possible attacks* as *action-based* behaviours and to express enforceable security requirements in a logic like ACTL. On the verification side, formal analyses have matured for signalling safety, e.g., compositional verification of interlock-

[1] ETCS levels define the supervision/authority mechanism: Level 0 means no ETCS; Level 1 means intermittent balise/loop-based with lineside signals; Level 2 means continuous radio via an RBC with balise position reference; Level 3 implements radio-only moving block with train-integrity supervision.

ings and dedicated verification environments, but there remains a gap between architectural zoning and enforceable *behavioural* security constraints [19,12].

Our contribution is an *action-based* security specification that (i) models, as LTS, the TS 50701 zones and conduits of the SuC comprising wayside, onboard, and the DCS; (ii) defines a three-tier attacker model centred on inter-zone conduits (with explicit consideration of compromised endpoints) and aligned with railway threat catalogues; and (iii) derives a compact set of ACTL-style rules that constrain admissible behaviours on critical conduits. The proposed rules are phrased in terms of observable actions and can be enforced at gateways; a brief analysis discusses how security degradations may propagate into safety concerns.

The rest of the paper is organised as follows. Section 2 positions this work within the context of railway cybersecurity, zoning/conduits practice, and action-based reasoning while stressing the role of TS 50701 in coordinating security and safety and the use of formal methods for specification and verification. Section 3 defines the SuC and its zoning/conduits. Section 4 introduces the attacker model. Section 5 presents the action-based modelling of an abstract railway system using a simple process description language. Section 6 reports on security analysis. Section 7 offers concluding remarks.

2 Related Works and Background

The cybersecurity literature for railways spans signalling systems, onboard communications, and enterprise interfaces. Comprehensive surveys document threats, assets, and defence-in-depth strategies across both operational and information-technology domains [26,8]. In the rest of this paper, the term *asset* refers to any equipment that constitutes a railway system, whether installed on the ground or on board, or the communication system between them. Sector guidance codifies security engineering via *zones* and *conduits* in CENELEC TS 50701 [3] (from now onward we refer to it simply as TS 50701) complemented by ENISA's zoning-and-conduits security architecture specific to railways [10]. Within Communication-Based Train Control (CBTC), the security of DCS has been analysed with emphasis on wireless jamming and integrity risks [25], while intra-vehicular architectures have been evaluated with respect to performance and security [21]. Model-based development of ATO for CBTC illustrates how engineering choices shape the attack surface of control loops [7]. Broader infrastructure-focused overviews situate cybersecurity controls across wayside and enterprise networks [22]. Recent studies examine risks and mitigations in DCS [13], availability of Industrial Control Systems (ICS) attack datasets from railway cyber ranges [27], and threats to Federated Learning (FL) pipelines used in railway AI workloads [28].

On the assurance front, Formal Methods (FM) have a long tradition in the railway domain. In this context, the contributions by Alessandro Fantechi and collaborators have been particularly significant. A position paper by Alessandro reflects on twenty-five years of FM adoption and open challenges [12]; a systematic mapping study covering 1989–2020 quantifies techniques, tools, and targets

(with Interlocking, IXL, as the core system) [14]; and an empirical evaluation assesses the usability of mainstream FM tools for signalling-system design [15]. At the level of concrete verification results, compositional verification has been advanced for large interlocking systems [19]. At the same time, prior milestones include verified modelling of signalling rules [20], model-driven development and verification for train control [23], and formal development and verification of distributed railway control in [18].

Table 1 summarises representative contributions by *study focus* and *methodology*, covering: CBTC/DCS analyses [25,21], surveys and guidance [26,8,3,24,10], FM perspectives, mappings, and tool evaluations [12,14,15], compositional verification and verified modelling [19,20,18], model-driven control [23], infrastructure overviews and DCS risk studies [22,13], ICS datasets and covert-channel evidence [27], and FL attack/defence work for rail AI [28]. This synthesis motivates the paper's contribution: action-based security rules stated over PA/LTS at zone/conduit interfaces, aligned with TS 50701 and informed by CBTC/DCS realities.

Table 1: Representative related works: study focus and methodology.

Citation	Study focus	Methodology
[26]	Rail threats, assets, defence-in-depth	Survey; taxonomy
[25]	CBTC DCS security (jamming, integrity)	Analysis; security considerations
[12]	FM in railways; challenges	Position/survey
[19]	Compositional verification of IXL	Compositional model checking
[14]	Mapping of FM in rail (1989–2020)	Systematic mapping study
[15]	FM tools for signalling	Empirical tool evaluation
[22]	Railway infrastructure cybersecurity overview	Practitioner/standards overview
[1]	Cybersecurity–safety co-engineering	Conceptual framework
[27]	ICS attack dataset (rail cyber-range)	Dataset; attack simulation
[13]	DCS risks, vulnerabilities, mitigations	Risk review; mitigation map
[28]	FL poisoning threats and defences in railway AI	Analytical & experimental study

Up to now, safety aspects and cybersecurity for railway systems have been considered mainly as separate concerns. TS 50701 provides a common framework to unify safety and security in railway systems. By structuring cybersecurity around zones and conduits, it enables the separation of concerns, the precise placement of controls, and the reuse of the same artefacts for both risk assessment and safety assurance. These structures serve as anchors to link security

rules with operational safety objectives—for example, enforcing restrictive behaviours under uncertainty or attack. Adopting TS 50701 terminology ensures traceability from architecture to enforceable rules, while ENISA's complementary guidance adds patterns and documentation practices. Together, they support the co-engineering of safety and security as integral elements of resilient railway systems [3,10].

Building on this, we adopt a process-algebraic approach that enables compositional descriptions of components interacting through observable actions. This enables the compositional description of components that interact through *observable actions*. We take TS 50701 as the starting point for specifying the behaviour and expressing security properties of railway systems. Signalling subsystems and zones (e.g., interlocking, RBC, ATS/OCC, lineside equipment) can be modelled as interacting labelled transition systems that emit or consume domain actions (e.g., commands, indications, authority updates). Conduits are modelled as channels and used to synchronise selected actions and impose policy constraints. This perspective permits us to describe

- *Behavioural specifications*: Behaviours are phrased over sequences of observable actions (e.g., only authenticated, fresh commands affect an interlocking state; movement authority application requires corroboration under disturbance)
- *Required properties*: Properties are specified in terms of ACTL [4], an action-based temporal logics that provide a natural language for expressing security rules over the labelled transition system induced by the composed processes, and tools for verifying correctness of the behavioural specification with respect to the envisaged property [11].

In this way, security requirements can be articulated and possibly verified where they can be observed and enforced, i.e., at zone and conduit boundaries, while remaining compatible with established FM practice on IXL and related subsystems.

3 System Model: Architecture, Zones and Conduits

The SuC is the *entire railway signalling system architecture*, comprising wayside, onboard, and the DCS that interconnect them. Wayside includes IXL, RBC (where applicable), ATS/OCC, LEU, and balises, as well as train detection (e.g., axle counters or track circuits). Onboard comprises ETCS/ATP/ATO, including odometry and the DMI. The DCS covers wired operational backbones, radio bearers for train–ground communication (e.g., GSM–R/FRMCS), time distribution, segmentation and filtering devices, security gateways, central logging and monitoring, and controlled maintenance access. Figure 1 sketches this architectural context. In particular, the figure shows how the local railway signalling networks at each station, which control the various train movement systems,

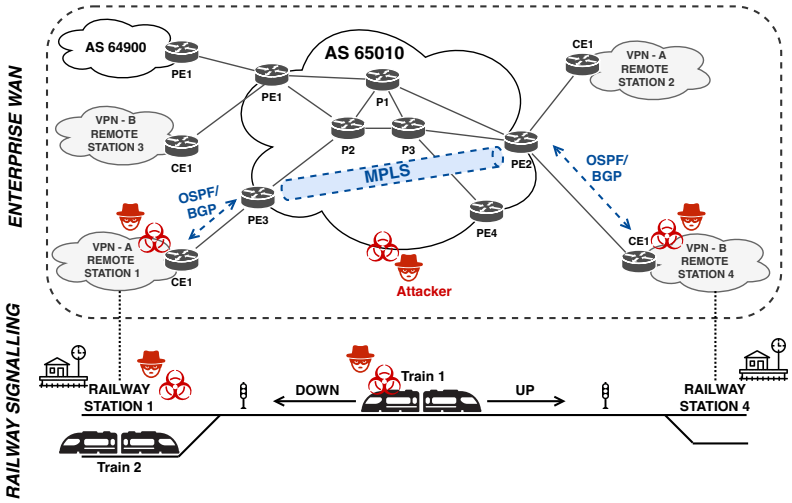

Fig. 1: SuC: railway signalling system architecture with potential attack points.

exchange information via a WAN network[2]. Our terminology for routes, signals, track segments, and points is aligned with that used in the IXL literature [19,12,26].

Zoning and conduits are the architectural primitives used to place and enforce cybersecurity controls in railway signalling, as defined in TS 50701 and aligned with ENISA guidance [3,10]. A *zone* is a set of assets with shared security requirements, exposure, trust level, and function; boundaries enumerate assets, interfaces, assumptions, and required controls. A *conduit* is the controlled communication path between zones that carries specified information flows and enforces policy (identification, authentication, filtering, monitoring). In practice, conduits are realised in three recurring patterns:

- *transparent* (segmentation/forwarding only, no content inspection),
- *filtered* (boundary enforcement via stateful allow-listing, protocol mediation, or proxy/inspection in a DMZ), and
- *unidirectional* (data diode to prevent backflow).

Independent add-on controls, such as VPN/IPsec/TLS tunnelling, time-sync constraints, logging, and bandwidth or rate-limit guarantees, may be applied to any conduit pattern to fulfil confidentiality, integrity, availability, and forensic objectives [10,3].

For the SuC, typical zones include ATS/OCC, IXL, RBC, lineside I/O (LEU, balises, train detection), onboard ETCS/ATP/ATO, DCS/telecommunications,

[2] In WAN architecture, Multiprotocol Label Switching (MPLS) connects sites, Open Shortest Path First (OSPF) handles internal routing, and Border Gateway Protocol (BGP) exchanges routes between WAN domains and providers.

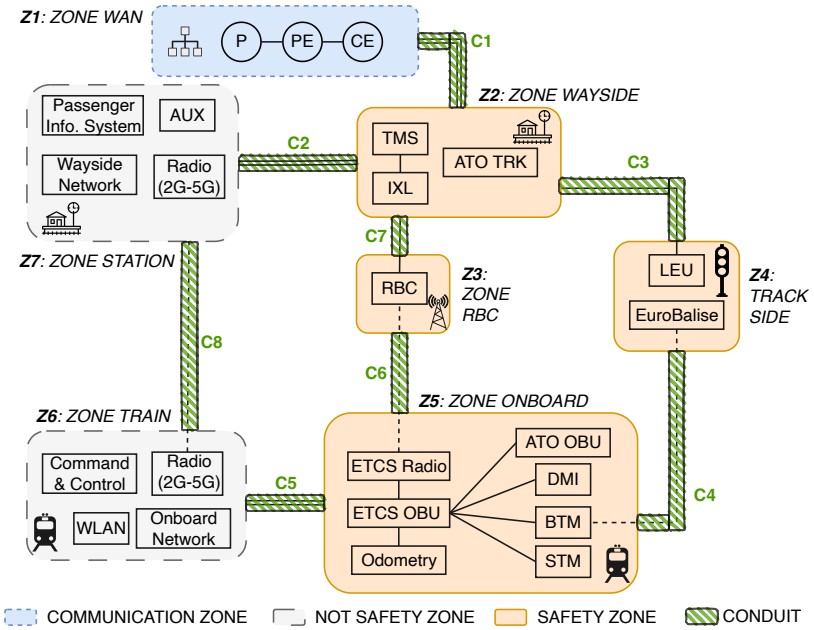

Fig. 2: Zoning and conduits of the SuC.

and support services (e.g., time and logging). Critical conduits include ATS–IXL, ATS–RBC, RBC–onboard ETCS, IXL–LEU/balises, IXL–train detection, and controlled maintenance/monitoring paths. Each conduit is documented with permitted flows (direction, endpoints, protocols), trust assumptions (identities, credentials), enforcement points (filters, proxies, diodes), and performance envelopes (latency, availability); these artefacts serve as anchors for the action-based rules developed later in the paper [3,10].

Figure 2 illustrates a zoning and conduits model for the SuC, highlighting critical conduits (e.g., Zone WAN to Zone Wayside, Zone RBC to Zone Wayside, Zone onboard to Zone Trackside, etc.) where action-based rules will be applied.

Table 2 clarifies which inter–zone exchanges are architecturally permitted and how they are controlled. In this table, each cell shows (Conduit ID, Type) with Type $\in$ {F = filtered, T = transparent, U = unidirectional}. A dash (–) denotes that inter-zone communication is *not permitted*. Thus, in the cells:

- `(Cx, F)` denotes *filtered* conduits (policy enforcement at the boundary);
- `(Cx, T)` denotes *transparent* conduits (segmentation/forwarding only);
- `(Cx, U)` denotes *unidirectional* conduits (data–diode pattern).

A dash (–) indicates that inter–zone communication is not allowed, and the diagonal is intentionally empty to denote intra–zone traffic. This representation follows the zoning–and–conduits approach in TS 50701 and the ENISA rail se-

Table 2: Zone-to-zone conduits.

Zone ID	Z1	Z2	Z3	Z4	Z5	Z6	Z7
Z1		(C1, F)	–	–	–	–	–
Z2	(C1, F)		(C7, F)	(C3, T)	–	–	(C2, F)
Z3	–	(C7, F)		–	(C6, F)	–	–
Z4	–	(C3, T)	–		(C4, U)	–	–
Z5	–	–	(C6, F)	(C4, U)		(C5, T)	–
Z6	–	–	–	–	(C5, T)		(C8, F)
Z7	–	(C2, F)	–	–	–	(C8, F)	

curity architecture, where security requirements are apportioned to zones and enforced along the conduits that connect them [3,10].

The matrix highlights a small number of security–relevant exchanges. Between Z1 (WAN) and Z2 (wayside), C1 is filtered to constrain exposure at the perimeter. Z2–Z7 (wayside–station) is likewise filtered (C2), reflecting the heterogeneity of station assets. Z2–Z4 (wayside–trackside) includes a transparent conduit (C3) used for deterministic lineside I/O, while Z4–Z5 (trackside–onboard) is unidirectional (C4), reflecting that balise/BTM flows are one–way by design. RBC–onboard (Z3–Z5) is filtered (C6) to protect the radio–borne movement authority exchange, and Z2–Z3 (wayside–RBC) is filtered (C7) to restrict control and configuration paths. The onboard–train backbone (Z5–Z6) is transparent (C5) to preserve performance within the vehicle, whereas Z6–Z7 (train–station) is filtered (C8) to control platform WLAN/maintenance connectivity. All other pairs are explicitly disallowed (–) to reduce lateral movement opportunities and to simplify assurance arguments.

This structure prepares the ground for the attacker model in the next section. Each conduit class implies distinct threats and feasible controls: transparent conduits prioritise determinism and thus are more exposed to eavesdropping, replay, or injection unless endpoints authenticate and protect their traffic; filtered conduits can be targeted via credential abuse, policy gaps, or device misconfiguration; unidirectional conduits block backflow but may still be susceptible to spoofed low–side inputs or timing/availability manipulation. By enumerating *which* inter–zone exchanges exist (C1–C8), *how* they are mediated (F/T/U), and *which* pairs are prohibited, Table 2 provides the precise scope of attacker capabilities and the action–based rules (Section 5) to be enforced.

4 Attacker Model and Threats

The SuC is the *entire railway signalling system architecture* (wayside, onboard, and the DCS interconnecting them). By adopting the zone–conduit perspective from TS 50701, we assume the adversary primarily targets inter-zone conduits to influence behaviour across zones; endpoint exposures are considered whenever they provide leverage over conduit traffic.

The attacker is modelled in three tiers to capture plausible attacks while keeping mitigations implementable at zone/conduit enforcement points.

Tier A (conduit-only): The attacker can manipulate traffic only on the conduits in Table 2, e.g., by eavesdropping, injecting, replaying, reordering, or selectively dropping packets; flooding or jamming radio bearers; or disturbing time synchronisation used for correlation and gating.

Tier B (endpoint-assisted): The attacker may additionally compromise selected wayside or onboard assets to originate seemingly legitimate traffic or to modify boundary configurations, e.g., by exploiting remote maintenance channels or misusing credentials.

Tier C (privileged): The attacker can leverage insider knowledge or supply-chain access to alter policies or credentials, potentially gaining broader access to the system.

In Section 5, we instantiate formal rules for Tier A. The same ACTL properties can be extended to Tiers B–C by modelling endpoint compromise as the capability to perform authenticated yet policy-inconsistent actions or to alter enforcement. Such deviations are detected through source validation, freshness checks, corroboration (i.e., independent consistency checks), and change-control constraints. This approach keeps the rules concise and enforceable at conduits while remaining sensitive to endpoint compromise, as recommended in TS 50701 and ENISA guidance [3,10].

Without assuming broken cryptography, the attacker can eavesdrop on mis-segmented or transparent paths, inject, replay, reorder, or selectively drop packets; flood or jam radio bearers; tamper with boundary devices through credential abuse or misconfiguration; disrupt time synchronisation used for correlation and gating; and misuse remote maintenance channels. These capabilities are bound to the permitted conduits in Table 2: filtered conduits (e.g., C1, C2, C6, C7, C8) are exposed to policy bypass and misconfiguration; transparent conduits (e.g., C3, C5) favour determinism but admit observation and injection unless endpoints protect their exchanges; unidirectional conduits (e.g., C4) block backflow yet remain susceptible to spoofed low-side inputs or timing/availability manipulation.

The following threat classes refine attacker capabilities by mapping them to the specific inter-zone conduits of the SuC (Table 2). Next, we outline representative ways in which an adversary may alter control or indication flows, or degrade their timeliness, to create unsafe preconditions during degraded operation. Each item identifies the affected conduit(s) (C1–C8) and, where relevant, provides a possible compromised-endpoint to highlight that authenticated yet policy-inconsistent traffic remains a realistic vector [26,8].

Perimeter control paths (C1, C2). Manipulation of TMS–IXL directives or IXL–TMS indications on filtered conduits (e.g., injection, replay, reordering). *Example (C2, Z7–Z2):* a compromised station Human Machine Interface in Z7 emits valid-looking directives into Z2 over the filtered path C2.

Train–ground movement authorities (C6) and RBC integration (C7). Spoofing or replay in the RBC–onboard exchange and misconfiguration of wayside–RBC interfaces. *Example (C7, Z2–Z3):* a wayside engineering workstation in Z2 is reused to push configuration to RBC in Z3 using stolen session material.

Trackside indications and lineside I/O (C4, C3). Interference with balise/BTM one-way flows or deterministic lineside signals, causing false position/occupancy cues. *Example (C3, Z2–Z4):* firmware-modified lineside I/O in Z4 emits plausible but false indications accepted into Z2 across the transparent conduit C3.

Onboard backbones and controllers (C5). Exploitation of transparent onboard networks to influence trainborne decisions via control-frame injection or replay. *Example (C5, Z6–Z5):* malware on the onboard backbone in Z6 injects frames toward ETCS/ATP/ATO in Z5.

Maintenance and station connectivity (C8, Z6–Z7). Lateral movement by means of filtered maintenance links toward operational zones. *Example (C8, Z6–Z7):* abuse of temporary maintenance connectivity from Z7 to Z6 to produce data or pivot toward operational assets.

On-path Denial of Service (DoS) via intentional interference. forcing the underlying radio connection to drop and re-establish (e.g., via jamming or network-induced release) *Example (C6, Z2–Z3):* targeted RF interference against GSM–R/FRMCS drops the EuroRadio session, delaying MAs until the onboard times out into a restrictive profile.

These scenarios are consistent with prior studies and with good-practice threat catalogues [26,8]. Since these attacks can potentially produce *authenticated* traffic, additional safeguards are necessary. The rules presented in the following section address this challenge by requiring freshness, corroboration, and approved change-control witnesses before any action can modify the zone state.

5 Action-Based Security Rules for Railway Systems

Building on the threat model established above, this section presents our approach to specifying security-aware operational rules using process description languages. First, we provide a set of enforceable rules, and then we discuss how process description languages can be used to describe railway systems by modelling them as sets of interacting processes performing conditioned actions. These descriptions are expressed as terms that model systems exposing *typed, observable actions*, representing commands and configuration requests, indications and status reports, movement-authority updates, authentication and freshness outcomes, as well as error or timeout signals.

Conduits control selected actions and apply policy according to their classification: filtered, transparent, or unidirectional. The formal rules are defined over process descriptions (*behaviour*), allowing only actions that satisfy *source*, *integrity*, *freshness*, *semantic consistency* to affect zone state. Let us remark that

by *semantic consistent* systems we refer to systems exchanging *content- and context-based* validated messages; i.e., messages with admissible temporal ordering and rates, topology and route compatibility, and with value ranges consistent with the operational context.

Examples of *semantically consistent* behaviour include: (i) only authenticated and fresh TMS directives are allowed to change IXL state on perimeter conduits; (ii) RBC messages are applied only if they conform to the authorised route model and current topology; and (iii) when a lineside device (e.g., noisy balise/track-circuit events), do not act on consistently with the rest of the system; hold the update unless an independent source (e.g., onboard odometry or a redundant sensor) confirms it within the allowed time window. These requirements are constraints on admissible sequences of observable actions (action traces) and can be directly formalised in ACTL. For readability, we present them textually here and omit the explicit formulae. It is worth noting that transforming the following textual descriptions into ACTL formulas remains a non-trivial task that warrants further investigation. Interested readers are encouraged to consult relevant literature on formal methods and temporal logic verification, starting from [4,19,12].

5.1 Rules For Securing Railway Signalling Systems

A concise set of enforceable rules is associated with the conduits identified in Table 2; each rule names the conduit and its corresponding control points. The rules align with TS 50701 and ENISA guidance on zoning and conduit enforcement [3,10,8]; they are organised according to the main operational contexts within the SuC: perimeter and wayside control paths, lineside interfaces, onboard networks, train–ground radio and RBC integration, and maintenance and station connectivity.

Perimeter and wayside control paths:

- **C1 (filtered, Z1–Z2):** TMS-to-IXL directives are applied only if the session is authenticated by both peers, messages are fresh, and the requested route change is *semantically consistent* with current topology and locking state. Otherwise, messages are discarded, and the last safe state is recovered from the log.
- **C2 (filtered, Z7–Z2):** Station-to-wayside exchanges (e.g., operator consoles, auxiliary services) are restricted by an allow-list of endpoints and protocols; write operations are authorised after dual control.

Lineside interfaces:

- **C3 (transparent, Z2–Z4):** Deterministic lineside I/O is accepted only from provisioned endpoints and within *contextual validation windows* (e.g., temporal ordering/rate limits and route context). Out-of-window sequences are quarantined and require secondary confirmation.

– **C4 (unidirectional, Z4–Z5):** Trackside to onboard flows (e.g., balise/BTM) are one-way. Onboard processing performs the balise's messages' integrity checks and kinematic/model consistency checks against odometry data. In the presence of interferences, the expected telegram cannot be received (the onboard system has a database with all the balises for each track), authority updates are suspended until validation succeeds or a restrictive fallback is entered.

Onboard networks:

– **C5 (transparent, Z6–Z5):** The onboard backbone carries ETCS/ATP/ATO control and telemetry. Only authenticated channels are accepted; *semantic/temporal consistency* constraints are enforced on control sequences; anomalies (replay, reordering) trigger degraded mode (i.e., restricted, fail-safe operation with conservative speed supervision and reduced automation) and local logging.

Train–ground radio and RBC integration:

– **C6 (filtered, Z3–Z5):** RBC-to-onboard exchanges must satisfy origin, integrity, and freshness; movement authority changes are applied only if reconciled with the current track-occupancy model and the route authorised by IXL; inconsistent or stale items are rejected and logged.
– **C7 (filtered, Z2–Z3):** Wayside-to-RBC control/configuration paths are restricted to authenticated sessions, with protocol allow-listing and rate limits; configuration changes require signed artefacts and out-of-band approval; failure to validate reverts the SuC to the last approved configuration.

Maintenance and station connectivity:

– **C8 (filtered, Z6–Z7):** Train–station connectivity (e.g., WLAN, maintenance uplinks) denies write paths into safety-related zones by default; temporary enablement follows a break-glass procedure with time-bound access, session recording, and post-hoc verification.

Across all conduits, the *restrictive-under-uncertainty* principle applies: if origin, freshness, or semantic consistency cannot be established within specified budgets, affected actions are ignored and the system transitions to a safe degraded mode; alarms and evidence are recorded for forensic analysis.

5.2 Modelling a Simple Railway System

In this subsection, we begin an initial abstract formalisation of railway systems by modelling zones and conduits as interacting processes. Zones, representing trains, tracks, and stations, are rendered as processes that expose typed actions (e.g., commands, indications, authority updates). Conduits, on the other hand, are rendered as processes that control message exchange between zones and enforce the appropriate policy (filtered, transparent, or unidirectional). The

overall system is described as the parallel composition of these processes. A distinct component is the MA, which models the electronically issued permissions by the control system (e.g., RBC/IXL) and determines how far a train may proceed and under which constraints. Such constraints may include limits on authority, permitted speeds/gradients, and timing or conditional data, to ensure onboard protection.

In the following, we describe the main steps to define the operational model:

1. **Define zones and conduits (TS 50701):** Identify the SuC and partition it into functional zones (e.g., Z1 WAN, Z2 wayside with IXL/TMS, Z3 RBC, Z4 trackside, Z5 onboard, Z6 train, Z7 station). Enumerate conduits (C1–C8) and classify them as filtered, transparent, or unidirectional; record permitted flows, identities, and performance budgets.
2. **Translate operations into a set of process terms:** Model each zone as a process with typed actions (command, indication, authority, auth_ok, fresh_ok, error/timeout). Model each conduit as a synchronisation/middleware process that enforces the conduit's policy and exposes the resulting observable actions.
3. **Compose processes and restrict action visibility:** Compose zone and conduit processes in parallel, while taking into account their interaction with MA and possibly restricting internal actions to reflect policy scoping and configuration, following the zoning artefacts of TS 50701.

The terms listed in Example 1 illustrate simplified process definitions for key zones and conduits, as well as the overall system composition. In this initial modelling, we use only three basic process algebra operators, namely the one for action sequentialization, and those for nondeterministic and parallel composition:

Action Prefixing `Act --> P` for indicating a process performing action Act and then behaving like P.

Nondeterministic Choice `P + Q` for indicating alternative behaviour of a process, possibly based on some conditions.

Parallel Composition `P || Q` for indicating the parallel composition of processes.

Most of the process description languages proposed contain additional operators, such as those for hiding or relabeling actions, enforcing synchronisation, and others. Here, for the sake of simplicity, we limit ourselves to this basic set of operators that are present in essentially all proposed languages. We refer the reader to [5] for a bird's-eye overview of these languages and for detailed references.

We concentrate on five zones (`TMS, IXL, RBC, ONB, TRKS`) and on four conduits connecting them (`C_TI, C_IR, C_RO, C_CO`) where the two letters after `C_` are the initials of the two connected zones. The behaviour of the five zones is the following:

– TMS plans traffic and requests route settings,

- IXL enforces the establishment of safe routes and reports the track status.
- RBC computes and transmits MAs consistently with the IXL topology and occupancy, as well as the TMS plan, over EuroRadio.
- ONB (the onboard ETCS) collects information from MA, supervises speed and braking against its constraints, and reports train status upstream to support subsequent TMS/IXL/RBC decisions;
- TRKS models trackside equipments, such as Eurobalise, that send encoded messages (typically referred to as telegrams) to the onboard train signalling system.

Below, we provide two simple models of railway systems using a basic process description language.

Example 1:

```
TMS   = send_TI --> TMS + error --> TMS )
IXL   = recv_TI --> (policy_tt --> apply_route --> send_IR
        --> IXL) + (policy_ff --> reject --> IXL)

RBC   = (recv_IR --> MA_update --> RBC) +  (send_RO --> RBC)
ONB   = MA_read --> (consistency_TT --> apply_ma --> ONBOARD)
        + (consistency_FF --> ONBOARD)

C_XY  = authenticate --> freshness --> filter_cmd --> C_XY

SYS  = (TMS || IXL || RBC || ONBOARD || C_TI || C_IR || C_RO
       || MA)
```

In this system, `TMS` issues a traffic instruction (`send_TI`); `IXL` receives it (`recv_TI`), checks whether the required policies are respected. If compliant, it applies the route (`apply_route`) and sends a report (`send_IR`); otherwise it rejects the request. Subsequently, `RBC` consumes the interlocking report (`recv_IR`) to update the movement authority (`MA_update`). Finally, `ONB` reads the MA (`MA_read`) and applies it only if the consistency check is successful. All communication conduits (`C_TI`, `C_IR`, `C_RO`) enforce `authenticate`, `freshness`, and `filter_cmd`. The main system `SYS` composes all processes in parallel and synchronises on matching send/recv actions.

As a further example, we focus on three zones—`RBC`, `ONB`, and `TRKS`—and on the balise–BTM conduit `C4` (modelled as `C_BTM`, unidirectional `TRKS`→`ONB`). `RBC` updates and issues MAs from interlocking reports; `TRKS` emits balise telegrams; `ONB` receives both inputs (radio for MA, `C_BTM` for telegrams), checks consistency, and applies the MA if the checks are successful, otherwise it holds the state or enters a fail-safe fallback on timeout.

Example 2:

```
RBC   = (recv_IR--> MA_update --> RBC) + (send_RO --> RBC)
ONB   = MA_read --> ( consistency_TT --> apply_ma--> ONB)
        + (consistency_FF -->  ONB)
        + timeout --> fallback --> ONB
```

```
TRKS  = send_EB --> TRKS
C_BTM = recv_EB --> send_CO --> C_BTM
ONB   = recv_CO --> (consistency_TT --> apply_ma
          --> ONBOARD) + (consistency_FF --> ONBOARD)
SYS   = (RBC || ONB || Trackside || C_BTM)
```

According to the above description, `RBC` performs `MA_update` after `recv_IR` (or `send_RO`). `ONB` then reads the MA (`MA_read`) and applies it only if `consistency_TT` holds, otherwise it idles, and a `timeout` will trigger a `fallback`. Separately, `TRKS` produces an Eurobalise messages event that is received by `C_BTM` on the unidirectional `C_BTM` path (`recv_EB`) and forwarded to `ONB`. `C_BTM` abstracts conduit C4. After receipt, `ONB` uses a consistency predicate to decide whether to `apply_ma`. As in Example 1, `SYS` composes all processes in parallel and synchronises on matching action names at conduit boundaries.

6 Security Analysis

The analysis maps the rule catalogue to the threat classes and enforcement points established by zoning and conduits (C1–C8). Enforcement is placed at zone boundaries so that only actions satisfying *source*, *integrity*, *freshness*, *semantic consistency*, and *corroboration* can affect zone state; violations trigger restrictive behaviour, alarms, and evidence capture, in line with TS 50701 and ENISA guidance.

Perimeter and wayside control paths

C1: bind signalling information to enumerated TMS identities, enforce mutual authentication and freshness, and require topology consistency before any route is affected; on mismatch or timeout, take no action and log the event.

C2: enforce default-deny for writes toward Z2. Segregate read/write paths, require dual control and time-limited sessions for any write to safety-related functions, and allowlist protocols; block any non-allowlisted ingress.

Lineside interfaces

C3 (transparent): boundary monitors enforce contextual validation windows (ordering, rate limits) and dual-sensing policies (e.g., axle counter vs. track circuit) before indications can influence IXL logic; out-of-window sequences are quarantined pending confirmation.

C4 (unidirectional): onboard processing accepts trackside telegrams only after performing integrity checks and cross-checks with odometry. If a disturbance is detected, authority updates are blocked, or a restrictive fallback is entered.

Onboard networks

C5: Only authenticated channels are accepted on the transparent onboard backbone; sequencing and timing guards detect replay/reordering. When anomalies are observed, trainborne logic shifts to degraded mode and records local evidence, limiting the impact of injections originating from a compromised train network segment.

Train–ground radio and RBC integration

C6: EuroRadio authentication and integrity-bound content-level attacks to cryptographic compromise; feasible on-path effects are availability losses (delay/drop/jam). In this case, the rules budget timeouts and enforce restrictive-under-uncertainty, requiring any Movement Authority to be reconciled with the route/occupancy model before application.

C7 (wayside–RBC management): Strict change control (signed artefacts, out-of-band approval, rollback to last-known-good) prevents unauthorised configuration drifts that could yield authenticated yet policy-inconsistent behaviour.

Maintenance and station connectivity

C8: Write paths into safety-related zones are denied by default. Temporary enablement follows a time-bound, dual-control "break-glass" procedure with full session recording and post-hoc verification, limiting lateral movement opportunities through service conduits. Break-glass grants tightly scoped emergency access that two authorised operators must co-approve and that is fully recorded and reviewed.

Monitoring, evidence, and time coherence. All enforcement points produce structured logs (including identities, sequence numbers, policy decisions, and timing) to support incident response and assurance. Time synchronisation bounds (used for freshness and correlation) are monitored; exceeding them triggers conservative treatment of affected actions. These practices are consistent with TS 50701 artefacts and ENISA good practices.

Security–safety propagation. Security degradations primarily manifest as loss, delay, or manipulation of control/indication flows. If unmitigated, these degradations can increase headways, create route-setting inconsistencies, or stress braking margins. By biasing behaviour toward restrictive modes under uncertainty, requiring corroboration before effectual actions, and reconciling authorities with the interlocking model, the proposed rules reduce exposure time and limit unsafe preconditions, complementing established safety verification and operational procedures.

7 Conclusions

This paper presents an *action-based* methodology that aligns TS 50701 zoning and conduits with process algebraic modelling to derive conduit-specific, enforceable security rules at the observable interfaces of the railway signalling architecture (wayside, onboard, and the Data Communication System). An attacker model grounded the rule design in realistic exposure. At the same time, the *restrictive-under-uncertainty* principle and *semantic consistency* requirements addressed the residual risk of authenticated-but-policy-inconsistent traffic. The result is a set of deployable controls implementable at zone boundaries that complements established safety-oriented verification by constraining admissible behaviours before they influence safety logic.

The approach assumes correct time synchronisation and uncompromised trust anchors for authentication and integrity, and does not quantify operational performance under sustained denial-of-service attacks. Despite these limitations, the methodology is portable across ETCS/CBTC deployments and amenable to incremental adoption because rules bind to existing zoning artefacts and boundary devices.

This work is just an initial step towards providing a formal modelling of railway systems specified according to TS 50701 specification style. Much remains to be done, and should be seen as an invitation to other researchers to join forces with us to:

1. provides a complete algebraic model of zones and conduits using the full expressive power of process algebras;
2. instantiate ACTL properties over the action alphabet and verify them with LTS-based toolchains like KandISTI [2] CADP/MCL [16] or mCRL2 [17];
3. validate the rules against configuration baselines and operational logs;
4. align the rule set to evolving standardisation (e.g., the transition from TS 50701 toward IEC 63452), while integrating runtime monitors with SOC/SIEM workflows for continuous assurance.

We hope this research helps the ongoing effort to bring formal methods and safety–security co-engineering together in the railway field. We also hope it encourages young researchers to explore these topics, ideally working with us and with Alessandro. This goal honours the legacy of Alessandro , whose work showed how careful and precise modeling and checking can ensure that complex, critical systems work correctly.

References

1. Bajan, P.M., Boyer, M., Dubois, A., Letailleur, J., Mantissa, K., Sobieraj, J., Tlig, M.: Proposal of cybersecurity and safety co-engineering approaches on cyber-physical systems. In: Computer Safety, Reliability, and Security: 41st International Conference, SAFECOMP 2022, Munich, Germany, September 6–9, 2022, Proceedings. p. 175–188. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-14835-4_12
2. ter Beek, M.H., Gnesi, S., Mazzanti, F.: From EU projects to a family of model checkers - from kandinsky to kandisti. In: Nicola, R.D., Hennicker, R. (eds.) Software, Services, and Systems - Essays Dedicated to Martin Wirsing on the Occasion of His Retirement from the Chair of Programming and Software Engineering. Lecture Notes in Computer Science, vol. 8950, pp. 312–328. Springer (2015). https://doi.org/10.1007/978-3-319-15545-6_20
3. CENELEC: TS 50701:2021 Railway applications – Cybersecurity. Technical specification, European Committee for Electrotechnical Standardization (Jul 2021)
4. De Nicola, R., Fantechi, A., Gnesi, S., Ristori, G.: An action-based framework for veryfying logical and behavioural properties of concurrent systems. Computer Networks and ISDN Systems **25**(7), 761–778 (1993). https://doi.org/10.1016/0169-7552(93)90047-8

5. De Nicola, R.: Process Algebras. In: Padua, D.A. (ed.) Encyclopedia of Parallel Computing, pp. 1624–1636. Springer (2011). https://doi.org/10.1007/978-0-387-09766-4_450
6. De Nicola, R., Vaandrager, F.W.: Action versus state based logics for transition systems. In: Guessarian, I. (ed.) Semantics of Systems of Concurrent Processes, LITP. Lecture Notes in Computer Science, vol. 469, pp. 407–419. Springer (1990). https://doi.org/10.1007/3-540-53479-2_17
7. Di Claudio, M., Fantechi, A., Martelli, G., Menabeni, S., Nesi, P.: Model-based development of an automatic train operation component for communication based train control. In: Intelligent Transportation Systems Conference (ITSC). pp. 1015–1020. IEEE (2014). https://doi.org/10.1109/ITSC.2014.6957821
8. ENISA: Railway Cybersecurity - Good Practices in Cyber Risk Management. European Union Agency for Cybersecurity (Nov 2021)
9. European Commission, DG MOVE, M., Transport: Subsystems and constituents of the ertms. European Commission, DG MOVE, Mobility and Transport - Accessed Sep. 19, 2025, https://transport.ec.europa.eu/transport-modes/rail/ertms/what-ertms-and-how-does-it-work/subsystems-and-constituents-ertms_en
10. European Union Agency for Cybersecurity, Helmut, K., Schlehuber, C., Ooms, K., Theocharidou, M., Naydenov, R.: Zoning and conduits for railways. European Union Agency for Cybersecurity (2022). https://doi.org/10.2824/761090
11. Fantechi, A., Gnesi, S., Mazzanti, F., Pugliese, R., Tronci, E.: A symbolic model checker for actl. In: Hutter, D., Stephan, W., Traverso, P., Ullmann, M. (eds.) Applied Formal Methods — FM-Trends 98. pp. 228–242. Springer Berlin Heidelberg, Berlin, Heidelberg (1999). https://doi.org/10.1007/3-540-48257-1_14
12. Fantechi, A.: Twenty-five years of formal methods and railways: What next? In: Counsell, S., Núñez, M. (eds.) Software Engineering and Formal Methods. pp. 167–183. Springer International Publishing, Cham (2014). https://doi.org/10.1007/978-3-319-05032-4_13
13. Fernandes, T., Magalhães, J.P., Alves, W.: Cybersecurity in smart railways: Exploring risks, vulnerabilities and mitigation in the data communication services. Green Energy and Intelligent Transportation **4**(4), 100305 (2025). https://doi.org/10.1016/j.geits.2025.100305
14. Ferrari, A., Beek, M.H.T.: Formal methods in railways: A systematic mapping study. ACM Comput. Surv. **55**(4) (Nov 2022). https://doi.org/10.1145/3520480
15. Ferrari, A., Mazzanti, F., Basile, D., ter Beek, M.H.: Systematic evaluation and usability analysis of formal methods tools for railway signaling system design. IEEE Transactions on Software Engineering **48**(11), 4675–4691 (2022). https://doi.org/10.1109/TSE.2021.3124677
16. Garavel, H., Lang, F., Mateescu, R.: Compositional verification of asynchronous concurrent systems using CADP. Acta Informatica **52**(4-5), 337–392 (2015). https://doi.org/10.1007/S00236-015-0226-1, https://doi.org/10.1007/s00236-015-0226-1
17. Groote, J.F., Mousavi, M.R.: Modeling and Analysis of Communicating Systems. MIT Press (2014), https://mitpress.mit.edu/books/modeling-and-analysis-communicating-systems
18. Haxthausen, A., Peleska, J.: Formal development and verification of a distributed railway control system. IEEE Transactions on Software Engineering **26**(8), 687–701 (2000). https://doi.org/10.1109/32.879808
19. Haxthausen, A.E., Fantechi, A.: Compositional verification of railway interlocking systems. Form. Asp. Comput. **35**(1) (Jan 2023). https://doi.org/10.1145/3549736

20. Ledru, Y., Idani, A., Ben Ayed, R., Ait Wakrime, A., Bon, P.: A separation of concerns approach for the verified modelling of railway signalling rules. In: Collart-Dutilleul, S., Lecomte, T., Romanovsky, A. (eds.) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. pp. 173–190. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-18744-6_11
21. Liyanage, M., Kumar, P., Soderi, S., Ylianttila, M., Gurtov, A.: Performance and security evaluation of intra-vehicular communication architecture. In: 2016 IEEE International Conference on Communications Workshops (ICC). pp. 302–308 (2016). https://doi.org/10.1109/ICCW.2016.7503804
22. Nunes, J., Cruz, T., Simões, P.: Railway infrastructure cybersecurity: An overview. In: European Conference on Cyber Warfare and Security. vol. 23, pp. 331–340 (06 2024). https://doi.org/10.34190/eccws.23.1.2296
23. Peleska, J., Feuser, J., Haxthausen, A.E.: The model-driven openetcs paradigm for secure, safe and certifiable train control systems. In: Railway Safety, Reliability, and Security: Technologies and Systems Engineering, pp. 22–52. IGI Global Scientific Publishing (2012). https://doi.org/10.4018/978-1-4666-1643-1.ch002
24. Schlehuber, C., Benoliel, S.: CENELEC prTS 50701 (Railway applications – CyberSecurity). In: Cybersecurity in Railways. pp. 1–18. ENISA-ERA (2021)
25. Soderi, S., Masti, D., Hämäläinen, M., Iinatti, J.: Cybersecurity considerations for communication based train control. IEEE Access **11**, 92312–92321 (2023). https://doi.org/10.1109/ACCESS.2023.3309005
26. Soderi, S., Masti, D., Zacchia Lun, Y.: Railway cyber-security in the era of interconnected systems: a survey. Transaction on Intelligent Transportation Systems (2023). https://doi.org/10.1109/TITS.2023.3254442
27. Yusof, A., Liu, Y., Kang, N., Seah, C.M., Liang, Z., Chang, E.C.: Signals and symptoms: Ics attack dataset from railway cyber range (2025), https://arxiv.org/abs/2507.01768
28. Zhu, Y., Liu, C., Chen, C., Lyu, X., Chen, Z., Wang, B., Hu, F., Li, H., Dai, J., Cai, B., Wang, W.: Privacy-preserving large-scale ai models for intelligent railway transportation systems: Hierarchical poisoning attacks and defenses in federated learning. Computer Modeling in Engineering & Sciences **141**(2), 1305–1325 (2024). https://doi.org/10.32604/cmes.2024.054820