UIC RAIL SYSTEM DEPARTMENT

Common safety barrier definitions to improve safety and interoperability

September 2022

INTERNATIONAL UNION
OF RAILWAYS

ISBN 978-2-7461-3210-8

1. INTRODUCTION

Today the demand for better railways drives the accelerated introduction of digital systems. That, in turn, accelerates the introduction of digital safety management systems. But as different railway organisations are digitizing at different speeds, Babylonian confusions emerge for the digital future of railway safety. The UIC created a work group on safety barriers to design a set of rules and definitions to combat confusion.

The work group has discussed many aspects of safety management and safety barriers including existing and proposed legislation, safety management systems, barrier models and various hierarchical arrangements of barriers. It has settled on a number of common definitions for safety barriers to support improvement in safety and interoperability globally.

The work group members believe that these definitions pave the way for consistent mutual understanding about safety barriers in the exchange of information and data between railway undertakings, infrastructure managers and their subsidiaries. We believe that the rules and definitions help because:

- Opportunities are created for shared understanding up to the point of interoperability between safety management systems;
- (digital) railway safety (knowledge) models can be harmonized by using shared principles;
- Experiences from different railway undertakings may be exchanged more easily, both by humans and by computers; and
- The rules provide a foundation for international supply chains for digital safety management systems that ensures fair competition.

CONTENTS

2. APPROACH TO DEFINITIONS FOR BARRIERS

The railways have incorporated many measures to ensure safety. The railways use systematic methods to assess and ensure that these measures work as expected. Those measures that require attention whilst trains are in operation are called safety barriers: the measures that railway undertakings, infrastructure managers or their subsidiaries have to conscientiously install, operate and/or maintain as a safety business process. Safety barriers come in many shapes and forms; varying from relatively simple components (such as a locking pin) to sprawling technical systems (such as axle-box overheating detector networks) and human-technical systems (such as the dead-man's switch). It is because of this variety that rules are required about how to describe barriers. In this document a small set of rules, classes and types of barriers are provided that are necessary to justify that a (set of) technical or non-technical element(s) represent a safety barrier. They are described by:

- RULES, which are key statements that explain how safety barriers should be understood and defines and links key concepts, and
- DEFINITIONS, where several concepts are clarified.

To ensure interoperability, the document provides the rules and definitions to be as generic as possible. This makes it possible for any railway undertakings, infrastructure managers or their subsidiaries to (re)label their safety measures as safety barriers with minimal disruption. In light of that objective, the current work abstains from classifications or sub-classifications and:

a. any reference to how important a safety barrier is in relation to others;

b. any reference to the justification for the existence of the safety barrier;

c. any reference as to how well the safety barrier (should be) working; and

d. any reference to the linkage and hierarchy that safety barriers may have in relation to each other.

3. SAFETY BARRIER FOR THE RAILWAY: RULES

The following are the rules that define safety barriers. Words in upper-case represent key concepts. Key concepts are either defined in these rules (§3) or listed separately (in §4). Lower-case words follow dictionary definitions for which additional descriptions are deemed unnecessary.

- a SAFETY BARRIER has the PURPOSE to control a HAZARD by preventing, or recovering LOSS-OF-CONTROL or mitigating the effects of HAZARDOUS EVENTS; a SAFETY BARRIER is an embedded SYSTEM for whom an organisation or a person within that organisation is RESPONSIBLE; the SYSTEM achieves its PURPOSE via HUMAN ELEMENTS, ORGANISATIONAL ELEMENTS and/or TECHNICAL ELEMENTS
- SAFETY BARRIERS are sub-divided in 3 sub-classes:
    a. PREVENTION SAFETY BARRIERS preventing PRECURSOR-EVENTS
    b. RECOVERY SAFETY BARRIERS that directly prevent LOSS-OF-CONTROL, and
    c. MITIGATION SAFETY BARRIERS mitigating post-critical events.
- SAFETY BARRIERS can only be VALID as PREVENTION- or RECOVERY SAFETY BARRIERS if they can stop the chain-of-events leading to the LOSS-OF-CONTROL, they otherwise can only be MITIGATION barriers.
- a SAFETY BARRIER may be ACTIVE or PASSIVE
    a. a PASSIVE BARRIER is always in place and achieves its PURPOSE via its placement and/or CHARACTERISTICS
    b. an ACTIVE BARRIER achieves its PURPOSE after activation of a decision making process that:
        i. DETECTS that a HAZARDOUS EVENT may be in progress,
        ii. DECIDES whether (and perhaps even how) to intervene, and
        iii. ACTS to intervene.
- To include a SAFETY BARRIER in a risk analysis and/or a safety case it has to:
    a. be managed with CRITICAL BARRIER ACTIVITIES recorded in the SMS-BUSINESS PROCESSES and
    b. VALIDATION should be presented and recorded in the SMS-BUSINESS PROCESSES.

4. SAFETY BARRIER FOR THE RAILWAY: KEY DEFINITIONS

The definitions for capitalized concepts in the rules are the following:

- PURPOSE: the intended effect of the fully functioning SYSTEM that prevents a HAZARD from occurring
- HAZARD: a process or condition that could potentially lead to harm and/or damage
- PRECURSOR EVENTS: events leading to LOSS-OF-CONTROL
- HAZARDOUS EVENTS: events leading to harm or damage
- SYSTEM: a set of elements (HUMAN ELEMENTS, ORGANISATONAL ELEMENTS and/or TECHNICAL ELEMENTS) that is coherently organized and interconnected in a pattern or structure to produce a characteristic effect: the PURPOSE
- RESPONSIBLE: an organisation or representative of an organisation that bears the responsibility for the correct functioning of the SAFETY BARRIER
- HUMAN ELEMENTS: system elements pertaining to activities performed by humans
- ORGANISATIONAL ELEMENTS: system elements pertaining to organisational instruments (such as management and oversight)
- TECHNICAL ELEMENTS: hardware- and/or software system elements
- CHARACTERISTICS: the key features of an object that facilitate the SAFETY BARRIER to achieve its PURPOSE
- LOSS-OF-CONTROL: the point where the HAZARD is no longer controlled and HAZARDOUS EVENTS can lead to harm or damage
- DETECT: sensing, through measurement or observation
- DECIDE: taking an appropriate decision to intervene by humans or automation logic
- ACT: the intervention in the chain-of-events by humans and/or technical systems
- VALID: justifiably used as a safety measure
- CRITICAL BARRIER ACTIVITIES: a set of activities that an organisation performs to maintain the SAFETY BARRIER
- SAFETY MANAGEMENT SYSTEM - BUSINESS PROCESS: the collection of activities performed by an organisation to maintain safety
- VALIDATION: the processes for gathering evidence that the SYSTEM will achieve its PURPOSE when it is called upon

5. DESCRIBING SAFETY BARRIERS

The work group proposes a consistent format for describing a safety barrier to provide transparency.

A SAFETY BARRIER description requires at least the following elements:

a. the name of the SAFETY BARRIER, its PURPOSE and the HAZARD it controls

b. to which subclass it belongs (PREVENTION, RECOVERY or MITIGATION) and how it achieves its PURPOSE

c. whether it is PASSIVE or ACTIVE type and how it achieves its PURPOSE

d. a clear description of the SYSTEM, how it functions and how it achieves its PURPOSE, including:

   i. for ACTIVE barriers: a full description of the SAFETY BARRIER and how it DETECTS, DECIDES and ACTS;

   ii. for PASSIVE barriers: a full description of the barrier CHARACTERISTICS; and in conjunction

   iii. a clear explanation of distinct HUMAN ELEMENTS, ORGANISATIONAL ELEMENTS and TECHNICAL ELEMENTS in the SYSTEM;

e. e. how proof is collected through VALIDATION to assure that the barrier SYSTEM achieves its PURPOSE.

The work group suggests enriching the description of the barrier with information that is locally relevant, e.g. to the railway undertaking, infrastructure manager, their subsidiaries, suppliers or national regulators. This additional information is wholly discretionary and could be placed in annexes. The work group suggests adding information on the following categories:

a. the CRITICAL BARRIER ACTIVITIES (e.g. maintenance and training),

b. the relevant SAFETY MANAGEMENT SYSTEM - BUSINESS PROCESSES (e.g. oversight and planning)

c. a description of the VALIDATION process (e.g. inspection or testing procedures)

d. information about the justification for installing the SAFETY BARRIER (e.g. standardisation or cost-benefit analysis)

e. the relative importance of the SAFETY BARRIER in relation to other SAFETY BARRIERS (e.g. critical versus auxiliary)

f. the linkage or hierarchy in which SAFETY BARIERS form a network (e.g. BowTie or Hazard Log)

g. further sub-classifications used in the railway undertaking or its software systems (e.g. human barriers and procedural barriers)

h. information about the efficiency of the SAFETY BARRIER.

6. EXAMPLES OF SAFETY BARRIER DESCRIPTIONS AND EXPLANATIONS

Example 1: Hot axle box detectors

Name & Purpose	Hot axle box detectors: the purpose is to prevent 1. train fires (due to high temperatures in bearings) and 2. train derailment (due to locked axles)
Subclass and Type	Hot axle box detector systems are active prevention barriers: they perform trackside measurements of the temperature of wheel bearings of passing trains to detect abnormal overheating wheel bearings and report to a signal box where procedures are then in place to decide whether a train 1. needs to be stopped immediately and what emergency procedures should be followed 2. needs to be taken out of service after operating in degraded mode and what procedures should be followed
System descriptions	Hot Axle Box Detector: a sleeper-mounted temperature detector, which warns a signal box of an overheated bearing as it counts the passing wheels. It indicates which axle is faulty and if one axle or wheel is hotter than the others on the train. {https://safety.networkrail.co.uk/jargon-buster/habd/} The technical element is a range of sensors mounted on the outside of the rails of a track to detect the increased radiated heat emitted by a defective axle box or bearing. {https://safety.networkrail.co.uk/jargon-buster/hot-axle-box-detector/} The human element is the decision of what to do with the information from the hot axle box detector in the form of applying pre-determined acceptability criteria and procedures to intervene. Network Rail provides the organisation, in terms of procedures for axle box overheating and requirements for training of drivers and staff on how to deal with hot axle boxes. If needed they inform the train driver and the organisation responsible for the maintenance of the train (which could be a TOC, a ROSCO or a Manufacturer) to take appropriate action
Validation	Axle box overheating incidents are recorded in the ORBITA system, subsequent actions are reported in that same system with feedback from the informed party confirming that subsequent actions are delegated and followed up appropriately.

Example 2: Platform markings

Name & Purpose	Platform markings (yellow line): the purpose is to indicate that passengers should not come closer to the platform edge to prevent them: 1. falling off the platform or 2. colliding with passing trains
Subclass and Type	Platform markings are passive prevention barriers alongside the length of the platform to make passengers aware that they are standing too close to the edge of the platform.
System description	The technical element is an integrated yellow line and tactile paving at 760mm from the platform edge, when there is low risk and enough space behind the line for customers to wait. A 100 mm wide yellow line at 1400 mm when there are non-stopping passenger services over 160 kph, freight services over 70 kph, any other significant aerodynamic risk such as the wind from a passing train pulling people or objects across the platform, and sufficient space behind the line for customers to wait. Tactile paving should be installed in the standard position of 760mm from the platform edge but in a colour as similar as possible to the platform surface. {https://www.transport-network.co.uk/RSSB-research-provides-platform-for-rail-safety/15224) {https://www.networkrail.co.uk/communities/safety-in-the-community/station-safety/} The organisation can stimulate the correct use of the platform markings with practical actions including: 1. Placing awareness posters in areas frequently used by wheelchair and pushchair users, such as in lifts 2. Relocating platform furniture, ticket machines, on platform retail outlets and information screens to lower risk locations on platforms to encourage lower risk behaviour 3. Creating tailored, public address system announcements on platforms and trains that are at higher risk locations. Station staff (human element) need to be made aware of the barrier and may intervene when people are standing across the line.
Validation	Installation and maintenance procedures on platform markings are recorded as evidence that the marking are placed correctly and platform markings are a recurrent training objective for platform staff.

Example 3: Compliance of the interventions of the Maintenance Plan

Name & Purpose	Compliance with ECM Maintenance Plan The Maintenance Management System (MMS) of the Entity in Charge of the Maintenance (ECM) ensures compliance with the plan at the established time. This assures the braking distance of trains in operation on the national network (caused by a technical failure by the braking system), which is a high-level safety critical function in the Renfe's risk model.
Subclass and Type	Compliance of the interventions of the Maintenance Plan is an active prevention barrier. The barrier adds safety requirements to the maintenance management processes and monitors the maintenance tasks in order to detect and correct any type of deviation.
System descriptions	The system is a management system, an organisational system that collates a set of critical barrier activities to ensure that maintenance tasks are performed as intended. This directs human tasks in relation to maintenance, which includes, but is not limited to: ↗ Correct management of the maintenance tasks of the braking system included in the Maintenance Plan. (organisational task) ↗ Reporting about observed irregularities of the braking system tant could increase the braking distance above the allowed distance. (human task) ↗ Holding regular coordination meetings with RU. (organisational task) ↗ Compliance of the recommendations from the investigation of events related to the braking system. (organisational task) ↗ Monitoring the ECM tasks related to braking systems included in the Maintenance Plan. (organisational task) ↗ Monitoring the availability and operability of the apps for the maintenance of braking systems. (organisational task for technical system) The critical activities describe the relationship between technical (braking system), human (operational tasks and good practices) and organisational elements (management of monitoring and continuous improvement procedures). These activities are included in the MMS procedures.
Validation	The system's performance is monitored by KPI's derived from (amongst others): ↗ The number of brake failures in Renfe's rolling stock ↗ The number of mentions in drivers' logs ↗ Mentions during meetings between RU and ECM ↗ Findings of accident investigations

INTERNATIONAL UNION OF RAILWAYS
16, rue Jean Rey - 75015 Paris - France
Tel. +33 (0)1 44 49 20 20
Fax +33 (0)1 44 49 20 29
E-mail: info@uic.org

Published by: UIC Rail System Department
Director of publication: Frédéric Hénon
Cover and layout: Ludovic Wattignies
Photo credit: Adobe Stock
Printing: UIC

ISBN 978-2-7461-3210-8
Copyright deposit: September 2022

www.uic.org

#UICrail