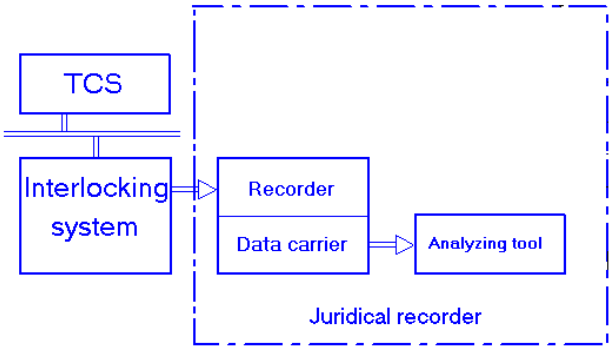
FINNISH INTERLOCKING REQUIREMENTS 2010
QUALITATIVE REQUIREMENTS
APPENDIX 2 - JURIDICAL RECORDER

CONTENTS

FIR-JR001	**1 Introduction**
FIR-JR002	**1.1 Background**
FIR-JR003	This document presents requirements for the juridical recorder, which permits juridical analysis of an interlocking system's operation.
FIR-JR004	**1.2 Purpose**
FIR-JR005	The main goal of these requirements is to provide the users of the interlocking system with services such as recording, download and display of data for efficient juridical analysis in case of an accident or other irregularity.
FIR-JR006	The purpose of juridical recording is to collect data that documents the behaviour of the interlocking system and its interactions with its subsystems or adjacent systems when an irregularity occurs.
FIR-JR007	The function of demonstrating the behaviour of the interlocking system shall be fulfilled by means of a juridical recorder.
FIR-JR008	**1.3 Scope**
FIR-JR009	This document includes the requirements and domain knowledge for the juridical recorder for an interlocking system.
FIR-JR010	**2 Domain knowledge**
FIR-JR011	A juridical recorder for an interlocking system is a standalone, separate unit that is part of the interlocking system. Guidelines: The diagnostic system may possibly carry out the functions of the juridical recorder.
FIR-JR012	As the following diagram shows, a juridical recorder consists of the following functional subsystems: - Recorder - Data carrier - Analysis tool (for reading data, downloading data, or performing a "playback" based on recorded data)

FIR-JR013	
FIR-JR014	The juridical recorder's data carrier shall be physically separate from the diagnostic system, even if the diagnostic system carries out some of the juridical recording functionality.
FIR-JR015	The juridical recorder is not intended for ordinary diagnostic purposes and hence shall not contain additional functions for diagnostic recording.
FIR-JR016	**3 Requirements**
FIR-JR017	**3.1 General**
FIR-JR018	The juridical recorder shall record all data it receives.
FIR-JR019	Alteration of recorded data shall be impossible.
FIR-JR020	The juridical recorder shall mark all incoming data with a time stamp accurate to within one tenth of a second.
FIR-JR021	The juridical recorder shall record data in chronological order.
FIR-JR022	When the juridical recorder receives an item of information bearing a time stamp from another system, the juridical recorder shall record the information with the time stamps of both the other system and the juridical recorder. Rationale: This requirement refers to timestamped data that the juridical recorder receives from other systems (for example the interlocking system).
FIR-JR023	The juridical recorder shall record data from all sources in the interlocking system, its subsystems or adjacent systems (including the TCS, adjacent interlocking, trackside elements, the ETCS radio block centre, and ETCS trackside equipment).
FIR-JR024	As the volume of data approaches storage capacity, the juridical recorder shall automatically delete older data to accommodate

	new data. However, the juridical recorder shall delete only data that is older than the age FIR-JR033 specifies.
FIR-JR025	It shall be possible to download the recorded juridical data (that is, create a copy) via a downloading tool, without influencing the data.
FIR-JR026	The juridical recorder shall be tamper-proof.
FIR-JR027	**3.2 RAMS requirements**
FIR-JR028	The juridical recorder shall record juridical data identically as the interlocking system transmits it, and keep it without change for the storage period specified in FIR-JR033.
FIR-JR029	The juridical recorder shall have at least the same availability as the interlocking system, as specified in the Availability Requirements document.
FIR-JR030	The juridical recorder shall be subject to the same maintenance process as the rest of the interlocking system.
FIR-JR031	**3.3 Data storage**
FIR-JR032	At any time, for the purpose of juridical analysis following an irregularity, it shall be possible to permanently store the data recorded by the juridical recorder over a pre-defined number of hours H.
FIR-JR033	The customer shall be able to specify one of the following values for H.
FIR-JR034	- 24 hours
FIR-JR035	- 48 hours
FIR-JR036	- 72 hours
FIR-JR037	- 672 hours (28 days)
FIR-JR038	Replacing the data carrier shall not interrupt the recording of data.
FIR-JR039	Manipulating (changing or erasing) the contents of the data carrier shall be impossible.
FIR-JR040	An unauthorized person shall not be able to read the contents of the data carrier.
FIR-JR041	Storage of the data carrier (outside the recorder) shall be possible with no change in content for at least five years without a power supply.
FIR-JR042	**3.4 Required juridical information**
FIR-JR043	The juridical information associated with each object or object type shall consist of two parts: - common (mandatory) information, and - additional specific information (depending on the specific application).
FIR-JR044	**3.4.1 System**
FIR-JR045	The juridical recorder shall at least record the following information about trackside elements:

FIR-JR046	- detected values
FIR-JR047	- steering values
FIR-JR048	The juridical recorder shall at least record current internal states (variables) of the interlocking system and its subsystems such as:
FIR-JR049	- every state or position of track elements
FIR-JR050	- internal diagnostic variables supporting failure detection (the nature of these variables will depend on the design of the interlocking system)
FIR-JR051	- all states (such as standby, running, not running) of the components of the interlocking system, its subsystems and adjacent systems
FIR-JR052	- all states of the communication links between the interlocking system, its subsystems and adjacent systems
FIR-JR053	- all states of computer and communication redundancy available in the interlocking system or its subsystems
FIR-JR054	- the identity of the interlocking system, its subsystems and adjacent systems.
FIR-JR055	The juridical recorder shall record at least the following information about the power supply: (also applies to distributed systems without a central power supply)
FIR-JR056	- power supply voltages present
FIR-JR057	- failures in the power supply.
FIR-JR058	**3.4.2 Commands and statuses**
FIR-JR059	The juridical recorder shall record all commands that the interlocking system receives (including those from the TCS, maintenance system, RBC, or adjacent interlockings).
FIR-JR060	The juridical recorder shall record all statuses of commands that the interlocking system executes or rejects.
FIR-JR061	The information about a command shall consist of:
FIR-JR062	- command identification (type, required operation);
FIR-JR063	- time of issuance;
FIR-JR064	- identification of the person who issued the command;
FIR-JR065	- identification of the source system (such as TCS, diagnostic system, local control panel, RBC or adjacent interlocking);
FIR-JR066	The juridical recorder shall record all status information that the interlocking system sends (to recipients such as the TCS, maintenance system, RBC or adjacent interlocking).
FIR-JR067	The information about a status shall consist of:
FIR-JR068	- event identification (type, unique identifier);
FIR-JR069	- time of event;
FIR-JR070	- identification of the source causing the event;
FIR-JR071	- identification of the destination for the status information (such as to the TCS, maintenance system, RBC or adjacent

	interlocking).
FIR-JR072	**3.4.3 Safety override commands**
FIR-JR073	The juridical recorder shall record any:
FIR-JR074	- safety override command that the interlocking system receives (such as those from the TCS or the maintenance system);
FIR-JR075	- status of a safety override commands that the interlocking system executes or rejects;
FIR-JR076	- acknowledgment of a safety override command that the interlocking system receives. The result can be:
FIR-JR077	- "accepted";
FIR-JR078	- "rejected";
FIR-JR079	- other safety related information. (to be defined - needs feedback from the railways)
FIR-JR080	The information about the interlocking system's acknowledgment of a safety override command shall consist of:
FIR-JR081	- time of issuance;
FIR-JR082	- time of execution (if the result is "accepted");
FIR-JR083	- reason of rejection (if the result is "rejected");
FIR-JR084	- identification of the source of the result;
FIR-JR085	- identification of the initial safety override command.
FIR-JR086	The information about a safety override command shall consist of:
FIR-JR087	- command identification (type, required operation);
FIR-JR088	- time of issuance;
FIR-JR089	- identification of the person who issued the command;
FIR-JR090	- identification of the source system (such as the TCS, maintenance system or a local control panel).
FIR-JR091	**3.5 Failures**
FIR-JR092	A failure, breakdown or shutdown of the interlocking system shall not lead to failure, breakdown or shutdown of the juridical recorder.
FIR-JR093	A failure or breakdown of the juridical recorder shall not lead to failure or breakdown of the interlocking system.
FIR-JR094	As the basis for informing the user of any breakdown of the juridical recorder, the juridical recorder shall regularly inform an adjacent system (such as the TCS, maintenance system or diagnostic system) that it is functioning.
FIR-JR095	The juridical recorder shall operate as long as any part of the interlocking system is in operation.
FIR-JR096	The juridical recorder shall continue to operate when the interlocking system goes into a degraded mode or returns to normal operating mode.
FIR-JR097	If the interlocking system shuts down for any reason, the recorder shall operate at least five minutes after the interlocking

	system has stopped and resume operation 10 seconds before the interlocking system starts again.
FIR-JR098	**3.6 Access to the juridical recorder**
FIR-JR099	The system giving access to the juridical recorder shall provide for at least the following classes of access rights:
FIR-JR100	Juridical recorder administrator;
FIR-JR101	User.
FIR-JR102	The system giving access to the juridical recorder shall allow combination of several access rights.
FIR-JR103	The juridical recorder shall only permit local access.
FIR-JR104	All access to the juridical recorder shall be recorded.
FIR-JR105	Every record of access to the juridical recorder shall at least contain:
FIR-JR106	- Name or identification of the natural person who accessed the system;
FIR-JR107	- Type of access/what kind of user;
FIR-JR108	- The time and date of access;
FIR-JR109	- Reason for access.
FIR-JR110	**3.7 Hardware**
FIR-JR111	The supplier shall provide a tool allowing an authorised user to select, read and download all or parts of the data recorded by the juridical recorder.
FIR-JR112	Displayed and downloaded data shall be understandable and every event recorded shall include a written description in complete words (not just internal codes or states).
FIR-JR113	The supplier shall provide a tool that is able to show a "play back" of railway operations, based on the recorded data.
FIR-JR114	The supplier shall make a proposal concerning the hardware for juridical recording.
FIR-JR115	The juridical recorder shall record all data on a data carrier.
FIR-JR116	The data carrier shall be removable from the recorder.
FIR-JR117	The juridical recorder shall allow connection of at least two independent fixed data carriers for recording of juridical data.
FIR-JR118	It shall be physically impossible (for example, due to a mechanical lock) for an unauthorized person to remove the data carrier.
FIR-JR119	The supplier shall provide spare data carriers.
FIR-JR120	The supplier shall guarantee the supply of spare data carriers during the operational lifetime of the interlocking system.
FIR-JR121	The design and construction of all involved elements - including the communication interfaces between the interlocking system, juridical recorder and data carrier, and the tools for reading or downloading data from the data carrier - shall preclude corruption of juridical data during transfer.