Software Module Requirement Specification

Module: Turnout Safety Module

Version	0.13
Date	2016-09-22
Company	Software and Systems Verification Ltd.
Responsible	Zoltan Micskei

NOTE: This document is an example specification part of the home assignment of the Software and Systems Verification (VIMIMA01) course at BME. It is deliberately simplified and contains errors.

1 Version History

Name	Date	Change	Version
Z. Micskei	2016-08-16	Initial structure	0.1
Z. Micskei	2016-08-18	Introduction, purpose and overview	0.2
D. Darvas	2016-08-18	Review of railway terminology	0.3
A. Hajdu	2016-08-19	Added rules for safety logic	0.4
Z. Micskei	2016-08-19	Added description of neighboring	0.5
Z. Micskei	2016-08-22	Added SysML model fragments	0.6
Z. Micskei	2016-08-23	Added detailed requirements	0.7
D. Darvas	2016-08-29	Review of document	0.8
Z. Micskei	2016-09-02	Finalizing after review	0.9
A. Hajdu	2016-09-06	Some changes in the terminology	0.10
Z. Micskei	2016-09-19	Resolving TODOs in the document	0.11
D. Darvas	2016-09-19	Updated figures	0.12
Z. Micskei	2016-09-22	Added assumptions and constraints	0.13

2 TABLE OF CONTENTS

3 INTRODUCTION

This document defines the requirements and interfaces for the Turnout Safety Module (TSM) of the Railway Interlocking System (RIS). The document describes the high-level functionality of the module, which should be the basis for the subsequent detailed design, implementation and validation phases.

The structure of the document is based on the ISO/IEC/IEEE 29148:2011 standard [1] and adheres to the guidelines of the IEEE 830-1998 [2] standard.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

The intended audience of the document includes the following roles:

- Representatives of the customer,
- Developers responsible for implementing and testing the module,
- Test engineers responsible for the validation of the module.

The rest of this section provides an overview about the context of the module and its high-level functionality. The subsequent sections describe the detailed requirements.

3.1 PURPOSE

This section describes the context of TSM and its purpose in RIS.

RIS TSM is part of the Railway Interlocking System (RIS). RIS is responsible for planning the routes of the trains and controlling the trackside equipment (e.g. signals, turnouts) to prevent any unsafe situation during the passage of trains. RIS is composed of several communicating modules, e.g. Signaling Subsystem, Train Control Module, Route Planner Module or the Turnout Safety Module.

Section A railway track is divided into sections. A section is much longer than the breaking distance of the trains. At most one train should occupy a given section at any time. The occupancy of the section is monitored by RIS. RIS can only monitor whether a given section is occupied or free, but it cannot detect the speed or direction of the train on the section. In the context of RIS the status of a section means its occupancy.

Turnout A turnout is a mechanical installation enabling trains to be guided from one track to another. A turnout is connected to three sections on its three sides. The sides, and hence the sections are named as follows (see Figure 1):

- facing,
- straight,
- divergent.

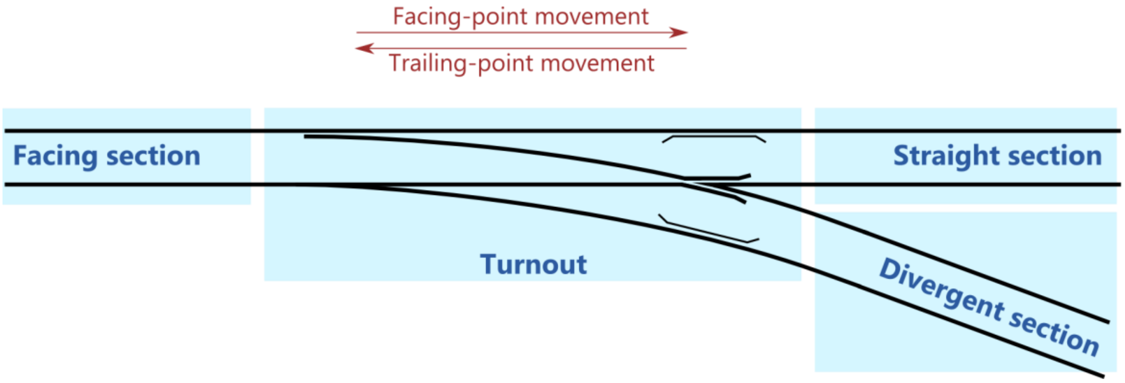

Figure 1. Naming conventions for a turnout

The turnout can be set into one of these directions:

- Straight: the facing section is connected to the straight section,
- Divergent: the facing section is connected to the divergent section.

A train approaching from the facing section is a facing-point movement, a train approaching from straight or divergent section is a trailing-point movement.

Connecting sections The railway tracks managed by RIS are divided into sections in a way that there is no section connected to sections on both sides. Therefore, a section can be either connected to a turnout and another section, or connected to a turnout and not connected to anything on the other side (i.e. a dead end). A section cannot be connected to two turnouts. Two turnouts cannot be directly connected, only through sections. There is always a section on each of the tree sides of a turnout.

Unsafe situations The following unsafe situations can occur when trains are approaching or are passing over a turnout.

- Trailing the switch: a train is approaching from the straight section to a turnout that is set to divergent direction, or a train is approaching from the divergent section to a turnout that is set to straight direction. Trailing the switch can happen only with trailing-point movement.
- Collision of trains: collision can happen if two trains arrive on the same section either by moving towards each other or a train catching up a slower or standing train.

Purpose of TSM The planner and controller modules of RIS are responsible for granting permissions to move only those trains and setting turnouts in only those directions that prevent the possibility of unsafe situations.

However, as RIS is a safety-critical system, additional safety measures are needed.

TSM is such a safety measure, which is responsible for monitoring one turnout and intervening if it detects an unsafe situation. However, the TSM is not responsible to grant movement permissions or to change the direction of the turnout.

3.2 Scope

The document describes the external interfaces and high-level functionality of the TSM modules. The document does not detail the other modules in RIS, only the messages received from these modules.

3.3 Module Overview

In RIS there is a separate TSM instance monitoring every turnout. A TSM is responsible for monitoring one turnout and the sections directly connected to the turnout.

TSM receives status messages about the direction of the monitored turnout and the occupancies of the connected sections, and decides whether the current situation results in an unsafe situation.

If an unsafe situation is detected, then the TSM intervenes by disabling the respective sections. On a disabled section no train can proceed. Note: The exact procedure for disabling a section depends on the capabilities of the actual trackside equipment, which are not detailed in this document.

For technical reasons trains cannot be stopped on a turnout, only on sections. Therefore, a turnout cannot be disabled.

Local decision Some of the unsafe situations can be detected locally, i.e. by taking into account only the direction of the turnout and the statuses of the sections connected to the turnout. For example, if (1) the turnout is in straight direction, (2) the facing section is occupied and (3) a new message is received that the straight section is occupied, then both the facing and straight sections shall be disabled.

Distributed decision For detecting more complex situations coordination between different TSM instances is required. Figure 2 depicts an example scenario. If the TSM monitoring turnout T2 receives that section S4 is occupied, then it has to check the direction of T2 and the occupancy of S5. If T2 is in straight direction and S5 is free then the result of the local decision would be to enable S4 and S5. However, if another train would occupy S8 and S7 would be free, then T3 could also decide to enable S7 and S8. If both trains would proceed, then eventually the two trains would collide. Therefore, the TSM should take into account information from other TSMs before making a final decision. This information is exchanged between TSMs using periodic heartbeat messages.

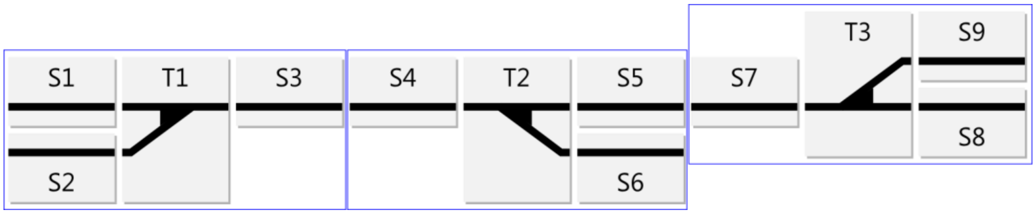

Figure 2. Example scenario

Neighbors In a distributed decision the TSM uses information about the status of its neighboring TSMs. (The status of a TSM will be defined later in the document.) A TSM can have three neighbors (in the facing, straight and divergent sides). If one of the sections of a turnout is a dead end, then it has no neighbor in that direction. On the example depicted on Figure 2, the straight side neighbor of the TSM monitoring T2 is the TSM monitoring T3, while the TSM monitoring T1 has no straight side neighbor.

3.3.1 Functions of the Module

The main functionality of the module can be summarized as follows (see Figure 3).

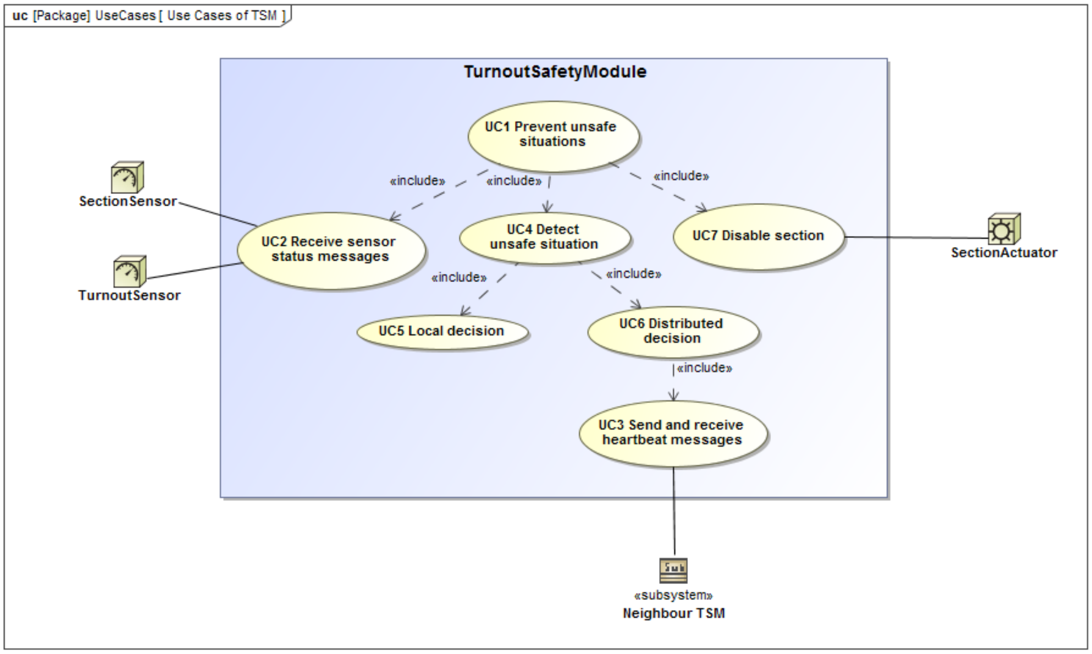

Figure 3. Main use cases of the module

- *UC1 Prevent unsafe situations*: this is the main functionality of TSM that is achieved with the help of the other use cases.
- *UC2 Receive sensor status messages*: receive status messages about direction of turnouts and occupancy of sections.
- *UC3 Send and receive heartbeat messages*: TSMs report their own status using periodic heartbeat messages and update the status of neighboring TSMs based on their heartbeat messages.
- *UC4 Detect unsafe situations*: run a detection protocol that has two phases (local and distributed).
- *UC5 Local decision*: detection of unsafe situations based only on the direction of the turnout and the occupancy of its three connected sections.
- *UC6 Distributed decision*: detection of unsafe situations based on communication received from neighboring TSM instances.
- *UC7 Disable section*: if an unsafe situation is detected then TSM disables some sections identified by the detection.

3.3.2 Interfaces of the Module

TSM is connected logically to other modules of RIS. TSM can be connected to at most three neighboring TSM instances. TSM uses the following functionality from these modules (Figure 4).

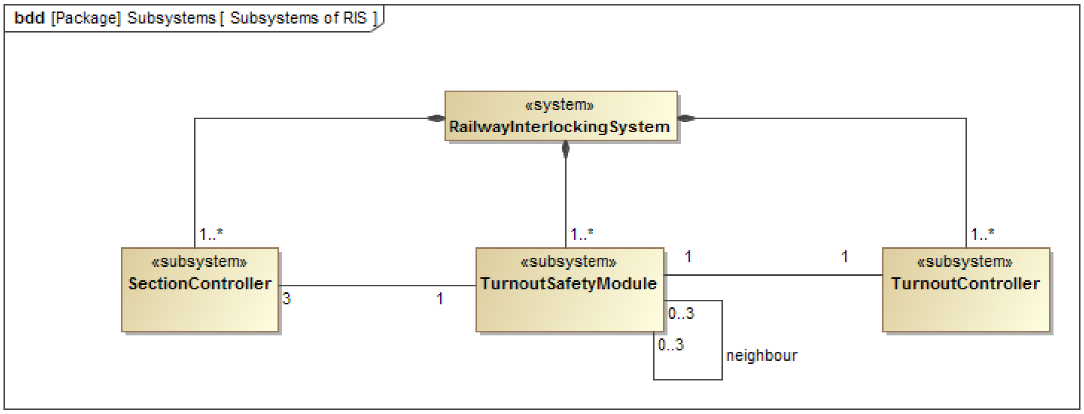

Figure 4. Modules connecting to TSM

- *Turnout Controller*: reporting the change of the direction of a given turnout.
- *Section Controller*: reporting the change in the occupancy of a given section, and making possible to enable or disable a section.
- *TSM*: receiving periodic messages reporting the status of the neighbor.

3.4 Definitions

This list contains definitions from ERA Glossary [4] and ETCS SUBSET-23 [5].

Term	Definition
DIVERGENT	The side of a turnout that is non-straight from the facing side.
FACING	The side of the turnout that a passing train always touches.
FREE	A track section which is not occupied.
HEARTBEAT	Short periodic messages that report on the status of an entity.
INTERLOCKING SYSTEM	A system that prevents the unsafe movements of trains.
OCCUPIED	A track section having any part of a train on it.
ROUTE	A sequence of connected sections and turnouts where each turnout is set in the direction of the section contained in the route.
SAFETY	Freedom from unacceptable risk of harm.
SECTION	A division of track for tracking occupation.
STRAIGHT	The side of the turnout, which is straight from the facing side.
TURNOUT	A mechanical installation enabling railway trains to be guided from one track to another.

4 REFERENCES

[1] IEEE Standards Association. Systems and software engineering – Life cycle processes – Requirements engineering, ISO/IEC/IEEE 29148:2011, 2011.

[2] IEEE Standards Association. IEEE Recommended Practice for Software Requirements Specifications, IEEE Std. 830-1998, 1998.

[3] IETF. Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, 1997.

[4] European Railway Agency. Glossary of railway terms. 8/11/2010. URL: http://www.era.europa.eu/document-register/pages/glossary-of-railway-terms.aspx

[5] European Railway Agency. ERTMS/ETCS Glossary of Terms and Abbreviations, SUBSET-23, 2015.

5 Specific Requirements

This section contains the detailed requirements of TSM.

5.1 External Interfaces

Signals [REQ-TSM-01-1] In communicating with other modules TSM shall use the signals depicted on Figure 5.

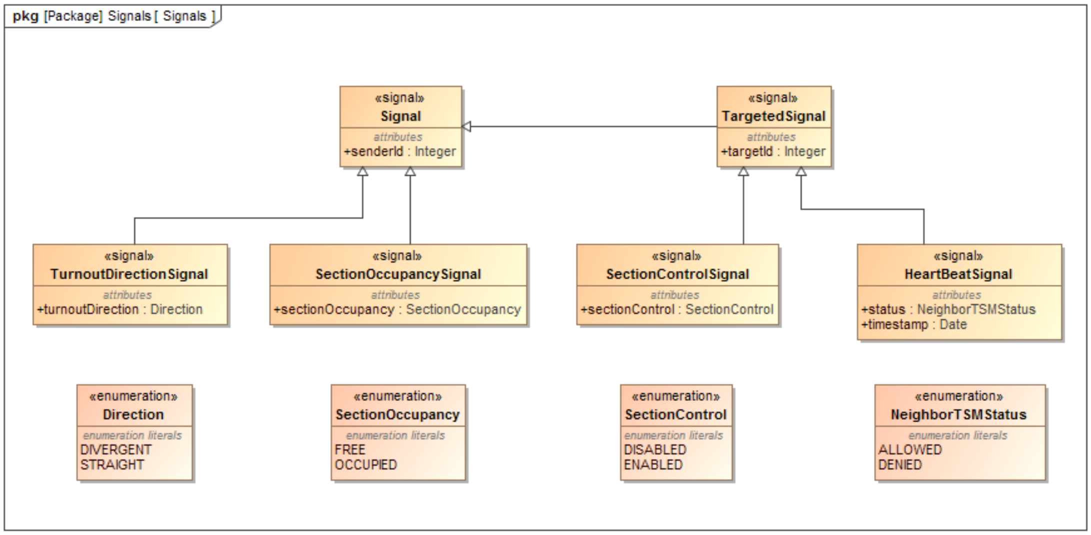

Figure 5. Signals used by TSM

- *TurnoutDirectionSignal*: a signal reporting on the direction of a turnout.
- *SectionOccupancySignal*: a signal reporting on the occupancy of a section.
- *SectionControlSignal*: a signal enabling or disabling a section.
- *HeartBeatSignal*: a signal reporting on the status of a neighbor TSM.

Ports [REQ-TSM-01-2] TSM shall provide the ports depicted on Figure 6.

[REQ-TSM-01-3] TSM shall not respond to other signals that are not defined on Figure 6.

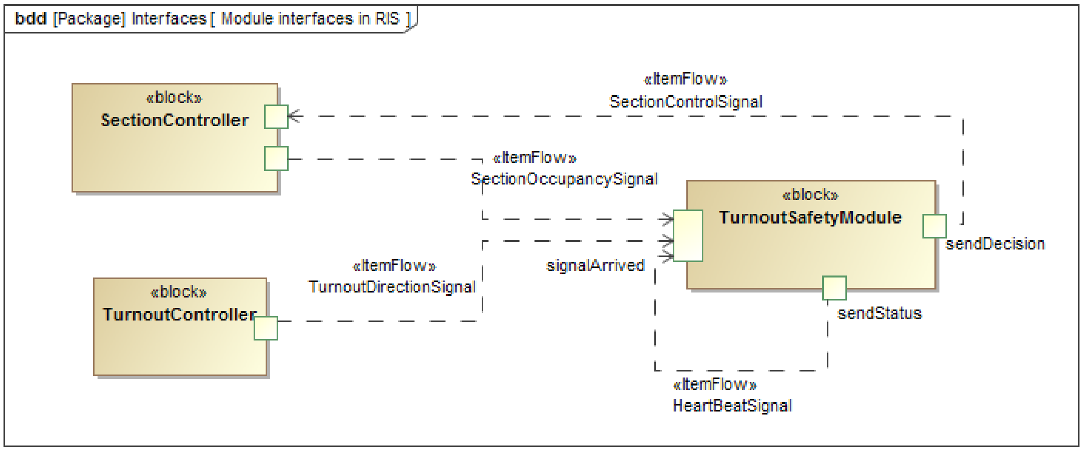

Figure 6. Ports and information flow of TSM

- *SectionContoller*: TSM receives SectionOccupancySignal from SectionContoller when the occupancy of the section managed by the SectionContoller is changed. TSM sends SectionControlSignal to SectionContoller to enable or disable the section managed by the SectionContoller.
- *TurnoutController*: TSM receives TurnoutDirectionSignal from TurnoutController when the direction of the turnout managed by the TurnoutController is changed.
- *TurnoutSafetyModule* TSM sends periodically HeartBeatSignal to its neighboring TSMs to inform them about its status. TSM receives HeartBeatSignal from its neighboring TSMs with their status information.

5.2 Functions

[REQ-TSM-02-1] TSM shall prevent unsafe situations.

[REQ-TSM-02-2] In order to achieve this objective TSM shall ensure that there is always at least one free section between any two occupied sections, where at least one of the occupied sections is enabled.

5.2.1 Receiving sensor status messages

[REQ-TSM-02-3] TSM shall receive status messages from the monitored turnout and the sections connected to the turnout.

[REQ-TSM-02-4] TSM shall store the latest received status for the turnout and each section. Older statuses may be stored.

[REQ-TSM-02-5] If the received status is different from the previously stored status, then a new decision protocol shall be started.

5.2.2 Heartbeat messages

[REQ-TSM-02-6] TSM shall periodically notify all of its neighboring TSMs about its status in heartbeat messages.

[REQ-TSM-02-7] The frequency of the heartbeats shall be configurable. The frequency of the heartbeat should be high enough to allow detection and handling of unsafe situations.

The status of a TSM can be allowed or denied. The status of a TSM is defined separately in all three neighbor sides (e.g. facing status is the status reported to the facing side neighbor).

[REQ-TSM-02-8] TSM shall report its status according to the following rules.

- Facing status: denied if facing section is occupied or turnout is in straight/divergent direction and straight/divergent section is occupied. Otherwise allowed.
- Straight/divergent status: denied if straight/divergent section is occupied, or facing section is occupied and the turnout is in straight/divergent direction. Otherwise allowed.

[REQ-TSM-02-9] The heartbeat message shall include a timestamp containing the current local time of the sending TSM.

[REQ-TSM-02-10] TSM shall store the last received heartbeat message for each neighbor. The heartbeat messages shall be stored separately for each neighboring TSM. A new heartbeat message overwrites any existing heartbeat message for the given direction. If the status in the new heartbeat message is different from the stored one, then a new decision protocol shall be started.

[REQ-TSM-02-11] If a heartbeat message is not received from a neighboring TSM for four heartbeat periods, then the neighboring TSM shall be considered faulty and its status should be handled as denied. If a new heartbeat message is received from a previously faulty neighboring TSM, then a new decision protocol shall be started.

5.2.3 Decision protocol

[REQ-TSM-02-12] TSM shall use the following decision protocol to detect unsafe situations.

[REQ-TSM-02-13] The decision protocol shall decide for every section connected to turnout monitored by TSM whether it shall be enabled or disabled.

[REQ-TSM-02-14] The decision protocol starts with a local decision, and may continue with a distributed decision.

5.2.3.1 Local Decision

[REQ-TSM-02-15] TSM shall use the following rules for the local decision.

- If the turnout is in the straight/divergent direction and divergent/straight section is occupied then the divergent/straight section shall be disabled.
- If facing and straight/divergent section is occupied and the turnout is in straight/divergent position, then both sections should be disabled.
- Otherwise the decision is to enable the section.

[REQ-TSM-02-16] If there is an occupied section that is enabled after the local decision, TSM shall start the distributed decision.

5.2.3.2 Distributed Decision

The purpose of the distributed decision is to confirm that the neighboring section will be free when the train will move in that direction.

[REQ-TSM-02-17] The distributed decision shall ensure that there is always at least one free section between any two occupied sections where a route exists between the occupied sections.

[REQ-TSM-02-18] TSM shall use the following rules for the distributed decision.

- If the facing section is occupied and the neighboring TSM on the facing side is denied, then the facing section shall be disabled.
- If the facing section is occupied and the turnout is in straight/divergent position and the neighboring TSM on the straight/divergent side is denied, then the facing section shall be disabled.
- If the straight/divergent section is occupied and neighboring TSM on the straight/divergent side is denied, then the straight/divergent section shall be disabled.
- If the straight/divergent section is occupied and the turnout is in straight/divergent position and the neighboring TSM on the facing side is denied, then the straight/divergent section shall be disabled.
- Otherwise the decision is to enable the section.

[REQ-TSM-02-19] The result of the decision protocol is the combination of the results of the local and distributed decision in a way that if at least one of the decisions decided to disable the section, then it shall be disabled, otherwise it shall be enabled.

5.3 NON-FUNCTIONAL REQUIREMENTS

[REQ-TSM-03-01] The duration of the decision protocol shall in all cases be lower than 0.5 seconds.

[REQ-TSM-03-02] TSM shall be able to handle at least 1 incoming status messages per second when deployed in a production environment. The capabilities of a production environment are described in the RIS System Requirements Specification.

5.4 DESIGN CONSTRAINTS

[REQ-TSM-04-01] TSM shall use the common communication method and technique employed in RIS. RIS uses the publish/subscribe communication model.

[REQ-TSM-04-02] Although RIS's communication method aims to be reliable, TSM shall prepare for lost communication messages.

5.5 SOFTWARE SYSTEM ATTRIBUTES

[REQ-TSM-05-01] The module shall store the following configuration attributes:

- ids of sections and turnout monitored by TSM,
- parameters for communicating with other modules,
- heartbeat frequency.

6 VERIFICATION

This specification will be verified by an external assessor team.

The verification of the module will be performed using code reviews, unit and integration tests.

7 APPENDICES

7.1 ASSUMPTIONS AND DEPENDENCIES

The requirements of TSM are based on the following assumptions.

Definitions:

- t_train_turnout = time required for a train to pass a turnout
- t_train_section = time required for a train to pass a section
- t_message = full roundtrip time of any status, heartbeat or control message

Timing assumptions:

- t_train_turnout << t_train_section
- t_message << t_train_turnout

7.2 ACRONYMS AND ABBREVIATIONS

Acronym	Meaning
RIS	Railway Interlocking System
TSM	Turnout Safety Module