Inspection Report

Subject: Software Module Requirement Specification of Turnout Safety Module

Date	2016-09-29

1. Introduction

This document reviews the [1] software module requirement specification document based on the ISO/IEC/IEEE 29148:2011 standard [2]. The following nine paragraphs review the inspected document following one criteria of the above mentioned standard at a time. The abbreviations and nominations used here are defined in [1].

2. Necessity

All the given requirements and specifications are necessary to describe the whole functionality.

3. Implementation details

[REQ-TSM-02-9] and [REQ-TSM-02-10] requirements cover requirements about storing heartbeat messages, which are inner properties of the TSM not seen from outside components. The communication model described in [REQ-TSM-04-01] also defines none necessary constraints on the implementation.

4. Ambiguous parts

In section 3.1. the expression "much longer" is not defined. The term "braking" is also ambiguous in this context.
In section 3.4. the term "short" periodic message is not defined. In section 5.2. the term between any two occupied section is not defined well. It could be two sections, which are not in one line.
In section 5.4. the term "reliable" could be ambiguous. (In what way is the communication channel reliable, which metrics describe it?)
In section 7.1 the term "pass" a turnout and a section is not defined. It can mean passing the whole train or just a defined part of the train. The nomination "x<<y" can be ambiguous too: it can refer that x is a magnitude smaller or x is negligible compared to y. (And in section 3.1. there is also a misspelling – tree instead of three.)

5. Consistency

In section 3.1. there is an inconsistency in the numbering of use cases. Use case UC3 should get greater number than, in which it is included (UC6). Inconsistency between the definition of unsafe situation (section 3.1.) and the requirements (section 5.): the requirements do not handle the unsafe situations, which are related to the improper direction of the turnouts. E.g. if a train is on the straight section, and the turnout is in divergent direction, there is an unsafe state, the section shall be disabled.
Inconsistent requirement numbering, section 5.1-5.2. uses [REQ-TSM-0x-y] format, but section 5.3-5.5. uses [REQ-TSM-0x-0y] format for one digit numbers. [REQ-TSM-02-14] is not

consistent with [REQ-TSM-02-19], former say that distributed decision may happen, latter say shall.

6. Completeness

In section 3.1. the review does not define, whether a train can occupy only one section at a time or two neighboring sections. The definition of unsafe situations is incomplete, as the trains can collide on a turnout as well, not only on sections. Section 3.4. is incomplete, unacceptable risk and harm terms are not defined.

In section 3.1. the review does not cover how the movement permissions should be granted when turnout direction changes happen. Section 1. does not cover, what should happen, if a train is on a dead end. [REQ-TSM-03-02] does not specify what should happen in case of more than one message is coming per second. [REQ-TSM-05-01] does not list of the parameters for communicating with other modules and does not specify the lower and upper limits of the heart beat frequency. [REQ-TSM-02-9] does not specify, that how should a TSM get the current local time.

7. Singularity

In section 5. the review merges together the case of straight and divergence states in one sentence multiple times, which can harm singularity and can also be ambiguous. [REQ-TSM-02-10] requirement covers 3 different things: storing the heartbeat messages, handling new heartbeat messages and starting decision protocols.

8. Feasibility

Section 3. does not inspect whether the function of a disabled section can be implemented in the train braking systems. In [REQ-TSM-02-7] requirement the term "high enough" is too general and nothing ensures that it is feasible. Based on the review it cannot be decided, whether [REQ-TSM-03-01] is feasible.

9. Traceability

In section 5.2 the third paragraph does not have an ID. [REQ-TSM-02-8], [REQ-TSM-02-15], [REQ-TSM-02-18] and [REQ-TSM-05-01] cover some sub requirements listed in more points without ID. The concrete numbers in [REQ-TSM-02-11], [REQ-TSM-03-01] and [REQ-TSM-03-02] cannot be derived from higher level requirements. [REQ-TSM-04-01] does not refer to the document where the publish/subscribe model is defined.

10. Verifiability

In [REQ-TSM-02-9] it is not defined how the clocks of different TSM-s should be synchronized and how that could be verified.

11. References

[1] Software and Systems Verification Ltd. - Software Module Requirement Module: Turnout Safety Module Specification v0.13 2016-09-22

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