Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the Environment, Transport, Energy and Communications DETEC

Federal Office of Transport FOT
Safety Division

Safety incidents on ETCS Level 2 lines in Switzerland on April 16th and June 27th 2019

Date:	16.04.2020
To:	SIS ERA
Copy to:	SPR, fz, st, su

File reference: BAV-503.233-2/1/1

A detailed analysis of two incidents is currently on-going involving the Swiss Federal Railways (SBB), the Swiss Federal Office of Transport (FOT) and the suppliers of the On-Board-System (OBS) and the Radio Block Centre (RBC). A notification to ERA was sent on the 12th of July 2019.

The following description outlines the main events common to both incidents:

1) During maintenance activities important odometer parameters were configured incorrectly. Neither the applied process nor the OBS revealed the error.
2) As a consequence, the ETCS OBS experienced a substantial loss in precision of the distance measurement functionality.
    - The reported confidence interval of the positions of the trains did not meet the given performance requirements and exceeded the threshold permanently by a large factor outside the acceptable tolerance according to Subset-41 §5.3.1.1.
    - Even in the light of this implausible sensor measurement data leading to the growth of the confidence interval, there was no adequate reaction from the OBS.
3) The train continued movement in Full Supervision (FS) mode and accepted and confirmed a Conditional Emergency Stop (CES) although the train had already passed the emergency stop location.
    - As a result, the Movement Authority (MA) was shortened by the OBS to the emergency stop location.
    - The train braked until standstill without trip reaction.
4) After the train reported its MA as shortened, trackside issued a new MA which allowed the train to closely approach the virtual signal, situated 75m after the emergency stop location. Since the actual train front end was already beyond this virtual signal at this moment, no movement was allowed at all.

Federal Office of Transport FOT
Colin Bonnet
3003 Bern
Location: Mühlestrasse 6, 3063 Ittigen
Tel. +41 58 463 8996, Fax +41 58 464 1248
colin.bonnet@bav.admin.ch
https://www.bav.admin.ch/

5) The estimated and max safe front ends were located beyond the virtual signal and therefore beyond the End of Authority (EoA). This resulted in the expected OBS behaviour:
    - The supervision of the EoA by max safe front end resulted in allowed speed “Release Speed” (operator’s choice in Switzerland).
    - On the on-board Driver Machine Interface (DMI), the safe speed indication was shown as zero. The Release Speed was indicated with 20km/h.
    - The on-board DMI showed that there was no more distance to the target (EoA).
    - The on-board DMI indicated an empty planning area.
6) The train was set in motion again and continued moving in Release Speed.
7) This movement was still not allowed (see 4), therefore the train was expected to trip as soon as the min safe front end passed the EoA. However, the train continued moving without performing a trip reaction. The trip reaction was not performed because the min safe front end had still not passed the EoA at the virtual signal due to an unexpected large deviation of the train positioning function, as indicated in step 1.
    - In case the passing of the EoA would have been correctly supervised with the min safe front end by the OBS, a trip reaction would have been the consequence.
    - In case the driver would have been aware of the fact that the train is moving in Release Speed under full responsibility of the driver and beyond its authorisation, the driver would not have set the train into motion again.
    - The train was hence moving without any authorisation in FS mode outside of a valid MA.
    - The train OBS still considered its position to be before the EoA, i.e. the train would accept a next CES for a stop location at or before the virtual signal.
8) Moving away from its MA without relevant authorisation, the train cleared routes and switches. Now it was possible for the interlocking to use the track for new routes over the other leg of a cleared switch. Since the OBS (see 7) still reported to be inside its MA, this MA was extended over the newly set route, and the extension was communicated to the train.

Graphical description

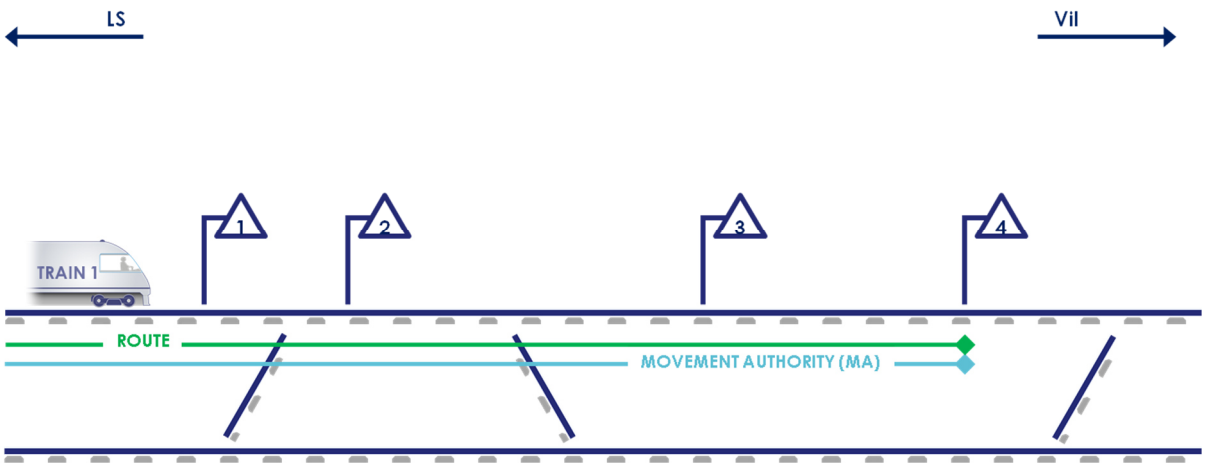

Figure 1

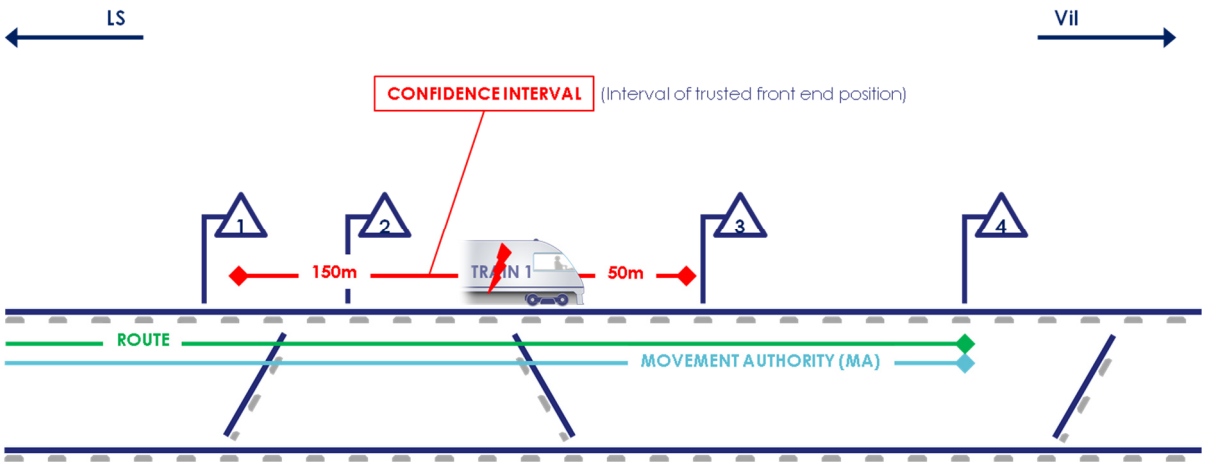

Figure 2

- Train 1 runs from LS to VIL. (set route is indicated in green, MA is indicated in blue). All signals have release speed (Figure 1)
- Train 1 shows a large confidence interval (indicated in red) (Figure 2)
- Section between Signal 2 and 3 is occupied by train 1, min SFE remains in front of Signal 2 (Figure 2/3)

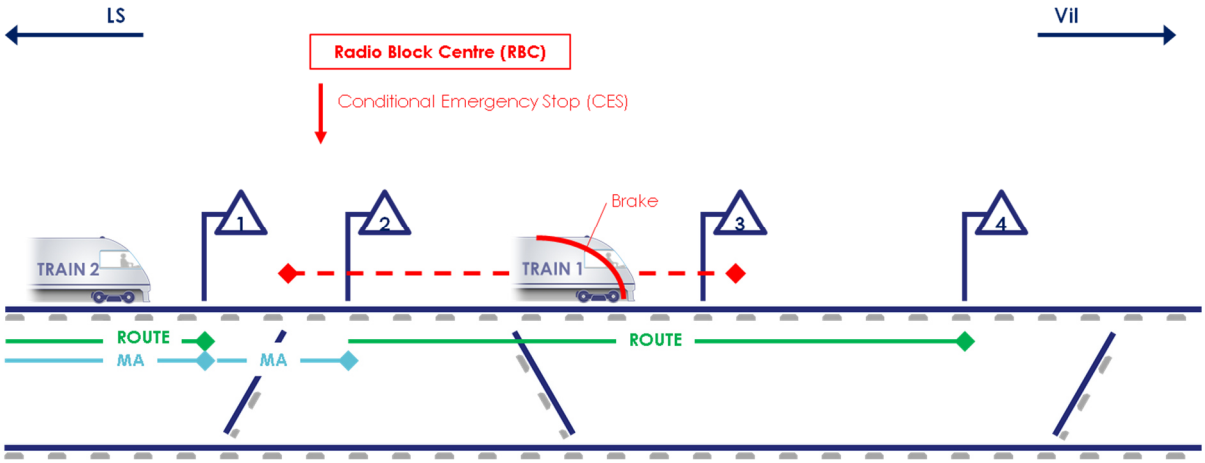

Figure 3

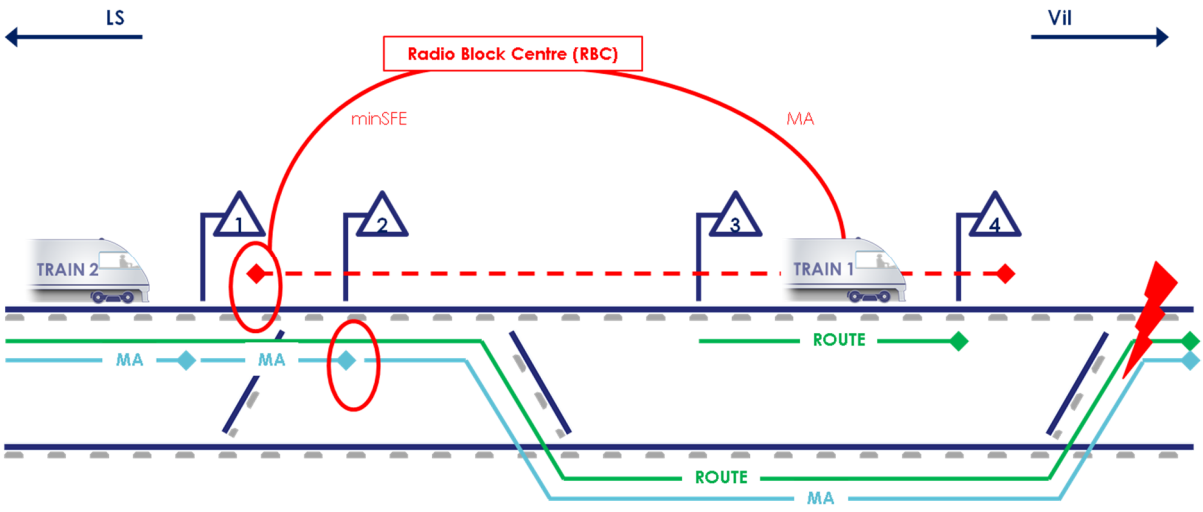

Figure 4

- Due to the function “signal stop evaluation” (1), a new MA of train 1 is sent with EoA at signal 2 (Figure 3)
- Train 1 proceeds (with RS), min SFE remains in front of signal 2. No trip occurs.
- Train 2 approaches signal 1 (Figure 3)
- Route for train 2 is set (to pass by train 1) (Figure 4)
- From RBC point of view train 1 (due to minSFE) is still in front of signal 2 (Figure 4)
- The MA based on the route set for train 2 is assigned to train 1 which leads to a critical situation (Figure 4)
- (1): by passing a signal and the occupation of the section, a CES is sent to the train at a location 75m in advance. If the CES is considered, a new MA with a EoA at this signal is sent to the train (Figure 4)

The above described chain lead ultimately to a reaction of the RBC to issue a MA to the train that had gathered a significant inaccuracy in its position.

In both incidents all systems and sub-systems individually behaved according to the UNISIG specifications. Nevertheless, in combination with human error on maintenance and Release Speed recognition, the two incidents clearly showed that a safety critical situation can occur.

Though a sufficiently safe technical solution should come from the OBS and/or the DMI, besides other measures the supplier of the RBC has been requested expressly by FOT and supported by SBB to add functionality to the RBC.

This requested functionality within the RBC should monitor the confidence intervals of the various ETCS Level 2 OBS in operation in accordance with the threshold defined by the Operator. If the confidence interval of a given ETCS Level 2 OBS would exceed this threshold, the RBC should initiate an adequate reaction to maintain the overall system safety.

This functionality is to be understood as an additional sanity check for the positioning of moving trains. All parties agree that depending on the performance of the positioning capabilities of the OBS this eventually can lead to reductions in operational performance, until UNISIG performance requirements are adequately achieved by all ETCS Level 2 OBS.

Additional short term preventive measures should be:

- a review of the maintenance procedures for ETCS Level 2 OBS to ensure that incorrect odometer data are identified before train release and,
- a restricted use of Release Speed handling combined with clear instruction and application of the operational scenarios where Release Speed is available.

In case you have further questions please feel free to contact the undersigned