ETCS Case Study EM: Treatment of Emergency Messages

Johannes Faber

October 27, 2004

Informal description

In this case study we consider the treatment of emergency messages as required for ERTMS/ETCS level 3.
In level 3 the currently existing national trackside systems for the detection of train speed, location and integrity are not used anymore. Instead the current parameters for a moving train are ascertained in co-operation of the on-board ETCS unit of the train with the appropriate *radio block centre* (RBC) which controls the traffic in a well-defined area and grants *movement authorities* (MA) to trains. A main issue of ETCS level 3 is increasing of the possible traffic density. Therefore the *moving block principle* is used by which the MAs are always given up to the position known as the *safe rear end* of the preceeding train. This allows the trains to drive with a smaller distance.
If some consecutive trains are driving with a minimal distance according to the moving block principle the train control system has to guarantee that in case of an accident of the first train the other trains come to a standstill before reaching this *danger position*. For achieving this behavior in ETCS the following procedure (with reference to [FRS99], sections 4.6.3 and 4.6.4) shall be applied, cf. Fig. 1. If the first train detects an emergency situation it has to send an *emergency message* to the appropriate RBC. If a connection is not yet established between train and RBC the train tries to call the RBC. The set-up time for an emergency call amounts to at most 2 seconds. If the train is not able to connect the call, it shall retry for 30 seconds (in reference to [EIR03], sections 3.4 and 13.2.2.). The maximum end-to-end delay for the message transfer is 500 ms [FFF00]. After receiving the emergency message the RBC must, in less than 0.5 seconds, forward the emergency message to every train approaching the danger position. If needed to avoid a collision, after less than 0.5 seconds the emergency breaks of these trains are automatically applied. If not needed, the driver shall maintain the control on the train. Hence, after less then 1.5 seconds a (visual and audible) indication shall be given to the drivers of the trains. They have up to 5 seconds to acknowledge the receipt of the message. After this time the emergency brake of the train must be applied automatically. The breaking curves depending on the current train speed are also sketched in Fig. 1.

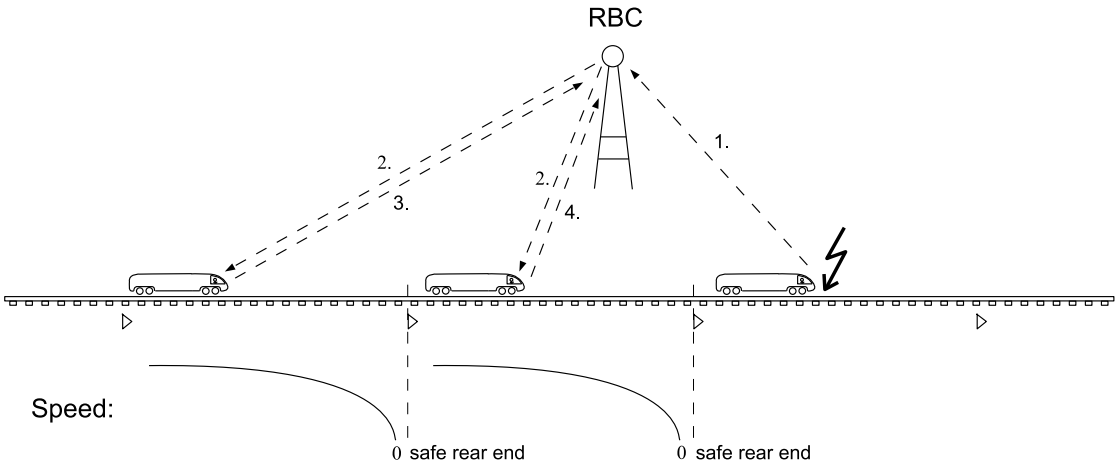

Figure 1: Three consecutive trains. If the first train sends an emergency call, the following trains have to stop before reaching the save rear end of the preceeding train.

Global safety property. In the case study we want to show that this ETCS procedure leads to a secure emergency behavior in the sense that after an emergency call of one train *no collision* of the following trains occurs.

References

[EIR03] UIC Project EIRENE Functional Requirements Specification, October 2003. EIRENE User Group Version 6.0. 1

[FFF00] Euroradio FFFIS Class 1 requirements, March 2000. UNISIG Version 2.0.0. 1

[FRS99] ERTMS/ETCS Functional Requirements Specification FRS, December 99. ECSAG Version 4.29. 1