Dagstuhl Seminar 07241
Tools for the Model-based Development of Certifiable, Dependable Systems
Case Study *Railway Level Crossing*

Hardi Hungar, Michaela Huhn, Oliver Lemke, Axel Zechner

June 10-15, 2007

Version 1.0 - 11.05.2007

Abstract

The *Railway Level Crossing* case study provides an opportunity to illustrate development processes and techniques on a small, but still realistic, stand-alone dependable system. The case study was taken from the OPRAIL project (2004-2006, sponsored by the bmbf).

By suggesting a joint example we hope to focus discussions, inspire comparisons, and accelerate the awareness of agreed solutions, opposite approaches and open issues in the seminar.

Picture removed for
licensing reasons

1 Railway Level Crossing

The German railroad network comprises about 50,000 level crossings. One safety action induced by national laws is to limit the maximum speed on railway lines with level crossings to 160 kilometers per hour. But the major safety measure is to equip the level crossings with safety and signaling technology which has to be developed in accordance to European railway standards [1, 2, 3]. These norms recommend a catalogue of system and software development techniques to achieve the higher safety integrity levels SIL 3 and SIL 4 with their specific requirements concerning reliability, availability, maintainability and safety.

2 System structure

A very simple[1] level crossing is composed of at least five parts to be managed by the control system under design: A gate prevents road traffic from entering the crossing when a train is in a safety-critical distance to the crossing. It can be raised and lowered (see Figure 1). Additionally, the road is secured by a set of lights consisting of a red and a yellow lamp with the known meaning. A supervision signal with one lamp indicates the train driver the status of the safeguarding equipment: Iff the signal is blinking the protective system is working and the train crossing is secured. Activation and deactivation sensors for the level crossing are installed before and after the level crossing and detect the approaching, respectively departing train.

In the case study the developer might restrict him/herself to the software design of the control component, appropriate dependable hardware components for the set of lights, the signal, and the gates may be assumed.

3 Normal Operation

When the automated level crossing system is set up correctly and in operation and no failure occurred so far, all lights are off and the gate is open. Then the system is in the so-called *unsaved mode*.

As long as an approaching train runs over the activation sensor the sensor shall generate an occupied signal. When the last axle of the train has traversed the activation sensor it shall generate a free signal again. If

[1] Here we consider only a one way road crossing one way railway traffic.

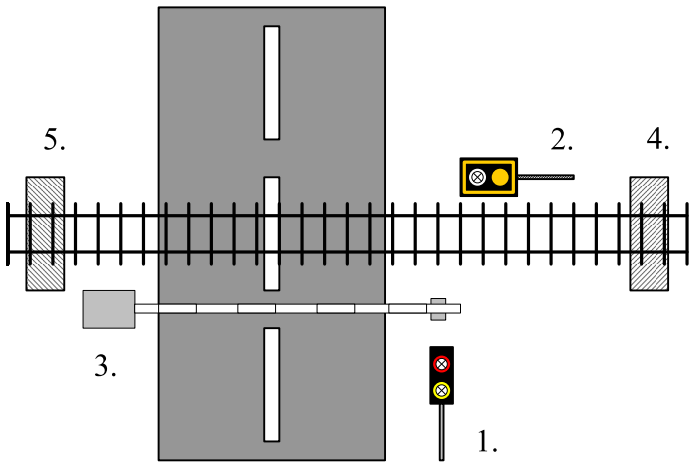

Figure 1: Railway level crossing: 1. set of lights 2. supervision signal 3. gate 4. activation sensor 5. deactivation sensor

the control unit[2] receives an occupied signal from the activation sensor in the *unsaved mode*, it will enter the *saving mode* and gives the command to turn on the yellow lamp of the set of lights. Three seconds after entering the *saving mode* the control unit has to give the command for switching off the yellow lamp and turning on the red lamp. If no failure occurs the system will enter the *saved mode* now. By entering *saved mode* the controller shall switch on the supervision signal to show signal aspect *LC1*, which means to turn on the blinking light. Twelve seconds after the system has entered the *safed mode* it must start to lower the gate. The activity of lowering or raising the gate must not last longer than six seconds from one end position to the other. When the gate has reached the lower end position within the six seconds interval the control unit will enter the mode *saved and gates closed*.

While a train or parts of it are located in the section of the train crossing the deactivation sensor has to generate an occupied signal. If the train has completely left this area the deactivation sensor shall emit a free signal. Immediately after receiving a free signal from the deactivation sensor, the control unit - still in mode *saved and gates closed* - shall switch the supervision signal to show signal aspect LC0, which means to turn off the blinking light. Inaddition, the command to switch off the red lamp of the set of lights

[2]also referred to as the system under design, protective device

is sent. After executing both actions the control unit initiates the raising of the gate. If the gates are opened within the six seconds interval the control unit traverses into *unsaved mode*.

If for unforeseeable reasons the train has passed the activiation sensor but does not reach the deactivation sensor within 240 seconds, the control unit reacts as in the previous case, i.e. it traverses from *saved and gates closed* to the *unsaved mode* after switching off the supervision signal and the red lamp and opening the gate.

4 Failure Mode

If the system once is in *failure mode* it must rest in that state until maintainance is accomplished. In *failure mode* the signal must always show signal aspect LC0.

If raising of the gate takes more than 6 seconds and the upper end position isn't reached in thatinterval the system shall consider the state of the gate as *unknown* and the system shall enter *failure mode*.

If during lowering of the gate the system is in *saved mode* and the system doesn't acknowledge that the lower end position is reached within the six seconds interval it must stay in *saved mode* until the unit receives a free signal from the deactivation sensor. After that the system shall proceed with the same actions requered for reaching the *unsaved mode* but instead it will finally enter the *failure mode*.

In case of failure of a lamp of the set of lights the system must immediately enter *failure mode*.

References

[1] CENELEC. EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Saftey (RAMS). European Norm., 1999.

[2] CENELEC. EN 50128: Railway Applications - Communications, Signalling and Processing Systems - Software for Railway Control and Protection Systems. European Norm., 2001.

[3] CENELEC. EN 50129: Safety related electronic systems for signalling. European Norm., 2003.