The Safety Related Software for Railway Control with Respect to Automatic Level Crossing Signaling System

Andrzej Lewiński[1] and Katarzyna Trzaska–Rycaj[2]

[1] Faculty of Transport and Electrical Engineering, Technical University of Radom, Malczewskiego 29 St, PL26600 Radom, Poland
a.lewinski@pl.radom.pl
[2] Technical School of Communication, Ułanów 3 St, PL31450 Cracow, Poland
krycaj@tk.krakow.pl

Abstract. The paper deals with design problems of correct and high reliable software for railway traffic control systems. The correct software (corresponding to formal or semi-formal criteria) has an important part in safety related (SIL4) railway control systems. The paper treats about actual state of art in design of safety related software for railway application. The proposed methods, recommended by CENELEC and UIC are introduced to example of automatic level crossing signaling system.

Keywords: Software safety and reliability, level crossing signalling systems, UML modelling, railway traffic control systems.

1 Introduction

Designing a safety-related software in railway computer systems is vitally important for correct operation of the entire railway system. Performing tasks defined by the programmer is the software's main function e.g. control of the signalling on level crossings or ensuring the safety of railway traffic. In order to ensure safety of rail communication users the software applied in railway computer systems must be reliable.

Proper formulation of requirements for the future railway system is essential. It has been proved that most errors (above 50%) arise already at the stage of specifying requirements of the design and at the engineering stage (above 25%). Errors at the coding stage make less than 10% of all errors arising in the production cycle [3].

Engineering, implementation and exploitation of the software for railway traffic control systems are subject to European PN-EN 50128 standard developed by CENELEC. In control systems which should meet high security requirements, the rule of fail-safe assurance is applied. In railway technology this rule has been used for quite a long time in order to ensure reliability and safety in railway traffic control systems functioning. The rule of fail-safe assurance can be expressed in the following way: "failures of the equipment or software errors in the data processing system can lead to unserviceability that may cause damage to the system's condition, however, the system should always be safe, i.e. such damage should not threaten the controlled process or the environment". This means that a single damage does not cause a dangerous situation and should be detected in the properly short time. The above mentioned rule of

J. Mikulski (Ed.): TST 2010, CCIS 104, pp. 202–209, 2010.

safety assurance in the case of damages might be applied in two forms, different as regards safety assurance, i.e. in the form of direct or indirect safety assurance.

The direct safety assurance method implies that all equipment failures causing functional disturbances directly bring the system to a safe condition. The indirect fail-safe safety assurance method is a modification of the method described above which allows to assure reliability by introducing additional supervisory and control functions to the system. This method is implemented by means of a multichannel control logic in which channels are fully reliable and therefore are supervised by a special comparator system, by first failure detector and by a system disabling the damaged channel, which control compatibility of output conditions.

2 Software Engineering Methods and Status of Works Related to Safety Related Software for Railways Systems

The software life cycle represents the recurrent totality of actions undertaken from the disclosure of the need for system construction to the end of its utilization [6]. Among cycles of the software engineering the classical models such as the cascade model, the spiral model, the evolutionary model and the V model are the most common. Unfortunately, as it turned out in practice, classical models are not error-free. Additionally, the situation becomes more complicated due to the users' growing requirements, the greater specialization and the complexity of systems. That is why contemporary models, often connected with object-oriented methodology, have gained importance lately. They include: the model of the object-oriented production cycle or the Checkland's model.

Research that has been done on similar issues concerned mainly determining reliability characteristics in systems of signalling devices used in traffic and modelling of fail-safe systems using e.g. Petri's networks or Markov's chains. Also, several dissertations on software engineering methods for fail-safe systems have been published. [7]. They mainly concerned application and role of methods such as: Petri's networks, Z, SDL, or UML in safe software engineering.

Software engineering methods may be classified in respect of their degree of formalization, i.e. the description's conciseness and accuracy and the way the system's different aspects are presented. When applying the first criterion, the following methods may be discerned: informal, semi-formal and formal.

3 Safety Related Software for Level Crossing Signaling Systems

As far as the role of control is concerned, railway traffic control system is a set of: material objects (e.g. executive devices), abstract objects (e.g. the set of control software), attributes (e.g. conditions or properties of objects) and relations between attributes, describing control functions which ensure safe execution of the assigned tasks[11].