Software Architecture of a Safety-Related Actuator in Traffic Management Systems

Thomas Novak and Christoph Stoegerer
SWARCO FUTURIT, Muehlgasse 86, 2380 Perchtoldsdorf, Austria
{novak,stoegerer}@futurit@swarco.com

Abstract. Traffic Management Systems are used in traffic technology for propagating information from a Higher Order Control Unit to the traffic participant. In today’s systems the user interface to the traffic participant is provided by actuators like Variable Message Signs. Such information can be either non-safety-critical (e.g., traffic jams warning) or safety-critical (e.g., green arrow opening the emergency lane on the motorway). According to international and national standards, software of Variable Message Signs displaying safety-critical information has to meet distinct safety requirements.

This paper presents a general architecture of safety-related software in an actuator according to the product standard VDE 0832. It gives an introduction to the standard and the domain of traffic control. A hazard analysis is carried out and safety measures are derived. Afterwards, the corresponding software architecture is presented. Finally, a safety assessment is carried out to prove the concept.

Keywords: Safety-related embedded software, safety standard, traffic system.

1 Introduction

The increasing traffic density in urban and inter-urban areas as well as the desire to increase road safety has resulted in a magnitude of measures. A possibility is the use of traffic management systems. Such a system does not decrease traffic per se, but supports the distribution of traffic in a more efficient way. Furthermore, it informs and guides drivers about upcoming dangerous situations like traffic jams. Both, optimizing traffic distribution and supporting road safety are accomplished by displaying aspects or textual information to drivers. The aspects are mostly shown by means of actuators – so-called Variable Message Signs (VMS). A typical VMS includes a graphical part, where speed limits or warning signs are displayed supplemented by a text part showing “traffic jam” or “accident”.

According to European and national standards such as EN50556 [3] or the German standard VDE 0832 [2], actuators within traffic control systems have to fulfill a number of requirements relating to the hardware, the software, the application, the integration within an overall system and the engineering process. Requirements on the software and its process are very similar to the generic international standard IEC 61508 [5]. Objective of this paper is to present a software architecture of a VMS that meets the requirements of EN 50556 in general and of VDE 0832 in case traffic management systems in particular.
The remainder of the paper is therefore structured as follows: Section 2 gives an overview of the domain of traffic control and discusses relevant parts of the standards VDE 0832 and EN 50556, respectively. Section 3 presents a hazard analysis using HAZOP analysis. Section 4, in turn, introduces the safety-related software architecture derived from the safety and domain specific requirements. Moreover, Section 5 proves the software architecture by going through a typical use-case of a VMS. The main steps within the architecture are highlighted. Finally, Section 6 concludes by summarizing the key facts of the work done.

2 Related Work

This section is split into two subsections. The first subsection gives information on the domain of traffic management systems in general and on actuators used in the systems with focus on VMS. The second subsection highlights challenges and the key facts of national standard VDE 0832 and European standard EN 50556 on road traffic signals.

2.1 Traffic Management Systems

Today's traffic management systems are typically structured in a hierarchical way [1]. At the top there is the Traffic Management and Information Center. It collects data from underlying substations and provides it to the operator for global strategies regarding traffic monitoring and control. Substations, in turn, take care of intermediate data collection. They are linked to one or more Outstations where Actuators (e.g., VMS) and also Sensors (e.g., detector loops) are connected to. Outstations are responsible for data processing and autonomous control jobs. In the following, the aforementioned control entities are subsumed by the term Higher Order Control Unit (HOCU).

![Traffic Management System](Image)

Fig. 1. Traffic Management System