Clarification of Design Philosophy for Railway Crossing System Based on FRAM

Keita Sakemi(1)#, Akimasa Okada(2)#
Satoru Kitamura(2), Takashi Kunifuji(2), Hideki Nomoto(1),
(1) Japan Manned Space Systems Corporation (JAMSS) - Japan
(2) East Japan Railway Company (JRE) - Japan

Accidents at railway crossings have big social impact. Therefore it's very important to prevent them. Existing railway crossing system safety is controlled by logic configured with traditional electrical relays and it has a history of high level of safety and reliability over several decades.
However, control by electrical relays are complex in terms of construction and maintenance. Hence, control by software which takes advantage of control logic based on electrical relays is required because control logic based on electrical relays is implemented at many railway crossings and it demonstrates a high level of safety.
In more detail, control logic implemented by means of such legacy mechanism includes deep tacit knowledge, some of which engineers have learned unconsciously through their work. Therefore, clarifying the implicit design philosophy is required. Replacement by software needs not simple imitation of logic based on electrical relays but reproduction of design philosophy extracted by the logic by latest technology. Analysis of success and risk factors is required.
By conducting FRAM analysis for railway crossing implementations, we have found out hidden design secrets and beautiful "pyramid" architecture in highly complex relay-based logic which have been allowing great diversity of the Japanese crossing sites for over 10,000 unique systems to achieve low accident rate. In this presentation, success and risk factors of this legacy system will be shown.

# Authors with this mark contributed equally to this research.