Prevention of human control errors by robust filter for manufacturing system
Marangé P., Benlorhfar R., Gellot F., Riera B.

CReSTIC, UFR des Sciences Exactes et Naturelles, Université de Reims Champagne-Ardenne
Moulin de la Housse - BP 1039, 51687 REIMS Cedex 2 – France
{pascale.marange, rachid.benlorhfar, francois.gellot, bernard.riera}@univ-reims.fr

Abstract: In this paper, we are interested at the errors that can commit by a human operator in the control program. When a command error is made, the presence of a product in the system can cause damage. In this paper, we design a robust filter placed inside the PLC which authorizes or forbids outputs from the PLC. The filter is composed of several logical constraints which have to be respected at each PLC cycle. In order to guarantee the filter quality, it is necessary to check that all constraints have been well defined. For that, in order to validate the filter, an original formal method has been proposed. This one is based on a modular modelling approach of the manufacturing system by using different timed automata models (actuators, sensors, items, and PLC), and by considering the most permissive PLC program. UPPAAL checker is used to verify that the filter is sufficient to avoid the manufacturing system to reach dangerous forbidden states. If it is the case, the filter guarantees the safety whatever the PLC program. Hence, the filter still remains active even if there are changes in the PLC program during the lifecycle of the production system.