PhD theme proposal

Property verification patterns for automated production systems

Supervisors

José Creissac Campos DI/CCTC, UMinho. jose.campos@di.uminho.pt

José Machado DEM/CT2M, UMinho. jmachado@dem.uminho.pt

Description

This proposal is part of a joint research agenda on the formal verification and simulation of automated production system by researchers from the departments of Mechanical Engineering, Informatics, Industrial Electronics, and Production and Systems, all from the University of Minho, with the close cooperation of researchers from the École Normale Supérieure (ENS) de Cachan (Paris). It is expected that the student will spend periods in Paris working at the ENS de Cachan.

The reliability, availability, and maintainability of automated systems (i.e. its safe operation) have a direct impact on people and goods safety. Guaranteeing the safe operation of a system requires an holistic approach to design, that takes safety considerations into account from the early design stages through to operational exploitation.

Formal verification of software is becoming established as a useful and powerful technique for guaranteeing the correctness of software artefacts in general. This is also the case for industrial controllers analysis [Moon, 1994]. In recent years, several approaches to applying formal verification techniques on automation systems dependability have been proposed. These range from formal verification by theorem proving [Roussel and Denis, 2002] to formal verification by model-checking [Smet and Rossi, 2002, Rossi, 2003, Gaid et al., 2005, Machado et al., 2006].

As verification tools gain popularity, the problem arises of making its use scale to more realistic settings. The scalability of such tools is affected by a number of factors, from the scalability of the algorithms being used as the size and complexity of the problems being faced increases, to their proneness to human errors during the modelling and interpretation of results phases as potential users become less proficient in the verification techniques being applied "under the hood".

Hence, in order to help the analysis of PLCs (Programmable Logic Controllers) programs, it is important to facilitate the use of automated reasoning tools. One specific aspect that deserves attention is the writing of properties to be verified. Meaningful properties can be hard to write and hard to get right. This is even more the case when we consider the behaviour of complex automated systems, whose requirements are difficult to describe.

Writing a property for verification is a two step process:

1. we must first identify what the relevant properties of a given system are,
2. and then we must decide how to correctly express them in the logic of the verification tool.

Step 1 is domain dependent, and largely relies on knowledge about the specific system being designed/verified and what its properties should be. Step 2 is a technical step. A correct understanding of the model, the requirement, and the logic in which properties are expressed is needed in order to guarantee that the property being tested correctly encodes the intent of the testing process. This is not a trivial step. In [Dwyer et al., 1999] and [Campos et al., 2008] examples are reported where properties have been incorrectly expressed/interpreted. The process is made more complex when the models are developed in such a way that verification must only be performed at certain specific points in the evolution of the system (for example, because not all states in the model represent *stable* system states).

A student accepting this PhD work proposal will look at how the process of expressing properties can be supported. The envisaged approach is to provide designers with patterns that can be instantiated to produce properties of interest. A tool will be developed to support the approach.

A paper exploring some initial ideas is available [Campos et al., 2008], as is as a first prototype of a patterns tool.

References

[Campos et al., 2008] Campos, J. C., Machado, J., and Seabra, E. (2008). Property patterns for the formal verification of automated production systems. In *IFAC 08*. accepted.

[Dwyer et al., 1999] Dwyer, M., Avrunin, G., and Corbett, J. (1999). Patterns in property specification for finite-state verification. In Boehm, B., Garlan, D., and Kramer, J., editors, *21st Intern. Conf. on Software Engineering (ICSE'99)*, pages 411–420. IEEE Computer Society Press.

[Gaid et al., 2005] Gaid, M., Bérard, B., and Smet, O. (2005). Verification of an evaporator system with uppaal. *European Journal of Automated Systems*, 39(9):1079–1098.

[Machado et al., 2006] Machado, J., Denis, B., and Lesage, J.-J. (2006). A generic approach to build plant models for des verification purposes. In *8th International Workshop On Discrete Event Systems (WODES'06)*, pages 407–412.

[Moon, 1994] Moon, I. (1994). Modeling programmable logic controllers for logic verification. *IEEE Control Systems*, 14(2):53–59.

[Rossi, 2003] Rossi, O. (2003). *Validation formelle de programmes ladder pour automates programmables industriels*. PhD thesis, École Normale Supérieure de Cachan, France.

[Roussel and Denis, 2002] Roussel, J.-M. and Denis, B. (2002). Safety properties verification of ladder diagram programs. *Journal Européen des Systèmes Automatisés*, 36:905–917.

[Smet and Rossi, 2002] Smet, O. D. and Rossi, O. (2002). Verification of a controller for a flexible manufacturing line written in ladder diagram via model-checking. In *21th American Control Conference, ACC'02*, pages 4147–4152, Anchorage, USA. CDROM paper n.734.