Compositional Verification of Multi-Station Interlocking Systems

Because interlocking systems are highly safety-critical complex systems, their automated safety verification is an active research topic investigated by several groups, employing verification techniques to produce important cost and time savings in their certification. However, such systems also pose a big challenge to current verification methodologies, due to the explosion of state space size as soon as large, if not medium sized, multi-station systems have to be controlled.

For these reasons, verification techniques that exploit locality principles related to the topological layout of the controlled system to split in different ways the state space have been investigated. In particular, compositional approaches divide the controlled track network in regions that can be verified separately, once proper assumptions are considered on the way the pieces are glued together.

Basing on a successful method to verify the size of rather large networks, we propose a compositional approach that is particularly suitable to address multi-station interlocking systems which control a whole line composed of stations linked by mainline tracks. Indeed, it turns out that for such networks, and for the adopted verification approach, the verification effort amounts just to the sum of the verification efforts for each intermediate station and for each connecting line.

General Information
- State: Published
- Organisations: Department of Applied Mathematics and Computer Science, Software and Process Engineering
- Pages: 279-293
- Publication date: 2016

Host Publication Information
- Title of host publication: Proceedings of the 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2016): Discussion, Dissemination, Applications - Part II
- Publisher: Springer
- ISBN (Print): 978-3-319-47168-6
- ISBN (Electronic): 978-3-319-47169-3
- (Lecture Notes in Computer Science, Vol. 9953).
- Electronic versions: comp.pdf. Embargo ended: 06/10/2017
- DOIs: 10.1007/978-3-319-47169-3_20
- Source: PublicationPreSubmission
- Source-ID: 127259495
- Research output: Research - peer-review: Article in proceedings – Annual report year: 2016