Solving geometric constraints to verify independence properties for safety-relevant systems

Andreas Baumgart

OFFIS - Institute for Information Technology,
Escherweg 2, 26121 Oldenburg, Germany,
andreas.baumgart@offis.de
WWW home page: http://www.offis.de/

Abstract

Safety-relevant systems like an automotive airbag controller or the wheel-braking system of an airplane may not fail due to a single fault. Typically redundancy is introduced into the system as a safety-means e.g. by adding another realization of the same sub-system. However, single faults can exists which are common causes for the failure of redundant sub-systems. Therefore, safety-standards like ISO26262 [1] or ARP4761 [2] require to verify these systems to be independent from such single faults as common causes. Independence includes spatial separation of redundant sub-systems to avoid effects of environmental factors or installation faults. In this presentation environmental factors are considered, each of which is a potential common cause. Typical environmental factors are radiation like electromagnetic fields and heat or objects on trajectories with high kinetic energy like accidentially occuring wheel fragments, turbine blades and birds. Subject of this investigation is the physical space claimed by a system-component and by a potential object due to an environmental factor. If such common space exists the system-component is affected by the environmental factor and its provided service potentially fails.

To be more specific in this presentation we will show how to apply interval-based constraint-solving methods to tackle this problem. In an independence analysis each system-component is considered to have a shape in a cartesian coordinate system. This shape defines the physical volume of the system-component and thus all positions belonging to it. If a system-component is installed to a system all of its positions are translated to coordinates relative to the system. Shapes are described in terms of primitive shapes like cylindroids, spheroids, cuboids, arbitrary polyhedrons or combinations thereof. Physical space claimed by an object of an environmental factor is also described as a shape which corresponds either to a fixed location in a system or to a trajectory. The mathmatical description of such installed shapes and trajectories is a system of non-linear equations and inequalities. They constrain the positions claimed by the installation of the system-components or by the environment factors. These equations and inequalities are used to formalize the question whether there are positions claimed by the environment factor which are also claimed by all installations of the redundant sub-systems. A candidate-solution provides a counter-example for the verification problem whether an installation of redundant sub-systems cannot fail due to single faults.

References

1. *Road Vehicles - Functional Safety.* International Standard Organization, November 2011.
2. Society of Automotive Engineers, *SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* Warrendale, USA, December 1996.