

The ACCESS Safety Case Toolset

The use of safety cases to document the rationale for a safety claim about a system has become increasingly popular. Safety cases are now mandated by several European government agencies including the British Ministry of Defense.

Arguments in safety cases are often documented graphically using the Goal Structuring Notation (GSN). In this paper, we introduce a new toolset called ACCESS for supporting the creation and maintenance of safety cases that include arguments documented in GSN. ACCESS provides a comprehensive environment in which engineers can develop and analyze safety cases. Particular emphasis in ACCESS is placed on the safety cases in modern safety-critical systems that include large arguments involving hundreds of GSN nodes.

ACCESS is a Microsoft Windows application. It uses Visio to display and manipulate arguments, Word for other documents, and the Windows file system for collecting and cataloging complete safety cases. ACCESS provides a set of basic features combined with a set of plug-in tools. The basic features include: (a) a node labeling system that allows GSN nodes to be labeled or relabeled as arguments are built. Labels can include combinations of user-set strings and sequence numbers; (b) a node coloring system so that groups of GSN nodes can be highlighted; and (c) a simple encapsulation mechanism for collections of documents in a safety case. Users can also edit GSN arguments directly from Visio.

ACCESS maintains an internal representation of GSN arguments that can be accessed by plug-in tools. Tools currently in ACCESS include a pattern library tool, an argument inspection tool, and an argument annotation tool. The pattern tool allows users to browse a library of patterns and insert selected patterns into an evolving GSN argument. The inspection tool provides support for rigorous human inspection of GSN arguments including display of check lists and monitoring of the progress of inspections. The annotation tool allows nodes in GSN arguments to be annotated with any number of notes that supplement the text typically displayed by GSN nodes. Notes are collected and can be processed by report generators to provide collected or summary information.

The various features of ACCESS can be configured for use in specific circumstances from XML configuration files. Thus, the meanings of node colors, the text of inspection checklists, and so on can be tailored to different project needs.

In this paper, we present details of the toolset and its application.