

ASTRA, a powerful software tool for Fault Tree Analysis

Description

Fault Tree Analysis (FTA) can be considered as the most popular methodology for dependability studies of complex systems, allowing to systematically describe the system's failure logics and to quantify the corresponding probabilities. FTA is applied for: design review, to prove that the system is reasonably safe and that it is well protected against both internal failures and external events; system diagnosis; and maintenance planning.

ASTRA is an efficient fault tree solver fully based on Binary Decision Diagrams, the state-of-the-art approach. The main advantage of the very efficient BDD approach is the possibility to exactly perform the quantitative analysis. The proprietary algorithms implemented are based on a labelling technique allowing the exact analysis of fault trees containing negated variables (NOT and XOR operators) and the handling of mutually exclusive events. These capabilities are particularly relevant for the new emerging applications in the domain of security, where the high events probability involved prevents the use of techniques based on classical Fault Tree approximated methods. Moreover, the use of NOT and XOR operators greatly facilitates the construction of fault trees of "complex top events" and "conditional events", whose definitions contain some working conditions. Many different design solutions may be identified, evaluated and compared from different viewpoints, e.g. safety level, costs, weight etc. The Sensitivity Analysis module of ASTRA performs the analysis of all fault trees concurrently: the effect of any design modification can be seen on all system critical states. The system can be improved through: Use of components of better quality or of higher maintainability; use of redundant configurations. A library of redundant configurations is available, comprising the K/N majority voting for active components or for tested components with different testing policy, the parallel configurations, and the stand-by configurations with single and multiple repairmen. A decision tree is used to manage and to rank all the identified design modifications.

Areas of application

- Safety and Security of Complex Systems
- Risk Analysis
- Test & Maintenance Optimisation

Innovative aspects and main advantages

- Exact Probabilistic Analysis
- Non Coherent Fault Trees
- Importance Analysis
- Boundary Conditions analysis
- Graphical Editor with Reliability Database
- Report Writer for Documentation.
- Export data and results in Excel format for further elaborations.
- Concurrent Sensitivity Analysis

Stage of development

Non exclusive license available



Scientific contact

Sergio Contini, Giacomo Cojazzi.
IPSC - European Commission
I-21020 Ispra – Italy
Tel: (+39) 0332/789217 or 785085
Email address:
sergio.contini@jrc.it, giacomo.cojazzi@jrc.it

Licensing contact

Intellectual Property and Scientific Collaboration Unit
JRC - European Commission
B-1049 Brussels, Belgium
Email: JRC-TechTransfer@ec.europa.eu

Reference: file n°2690