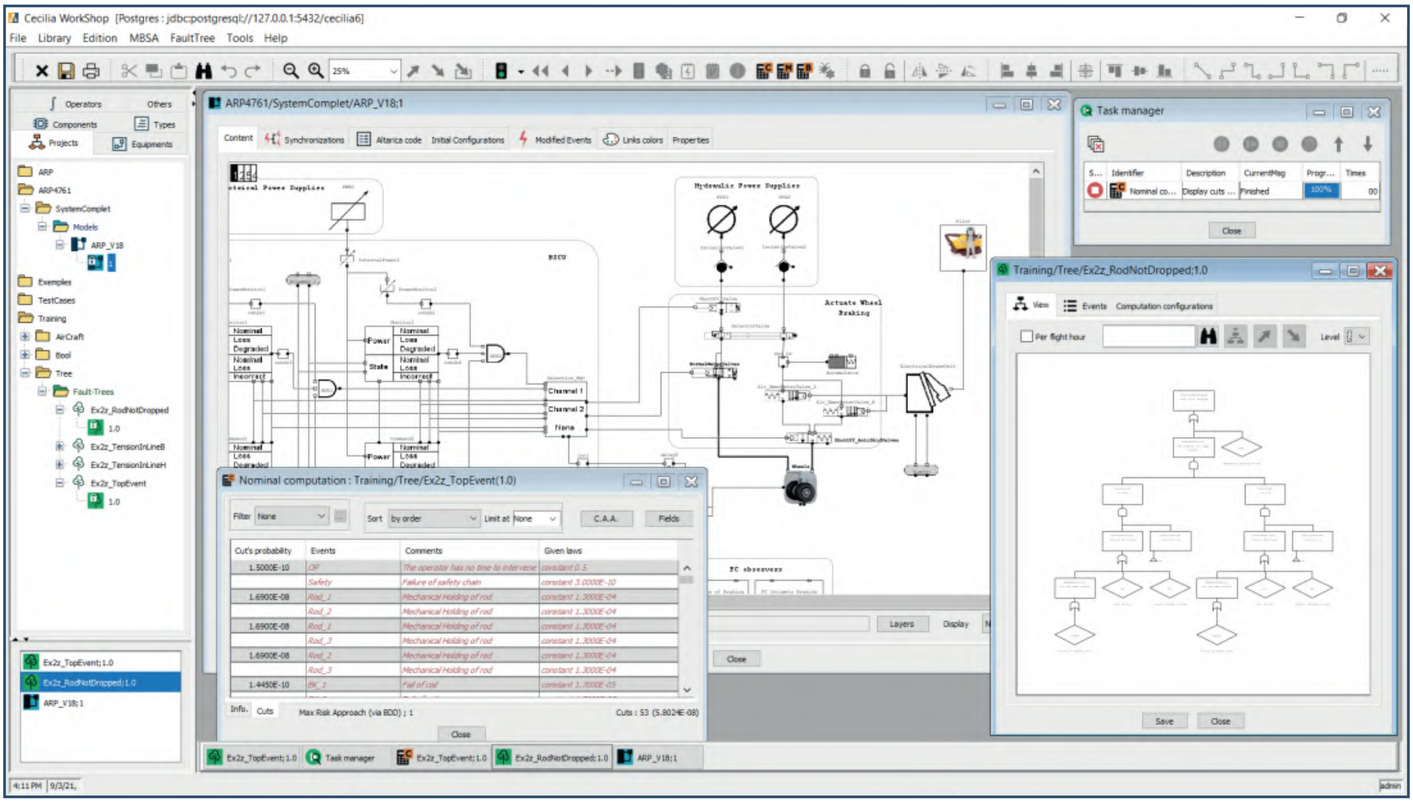
CECILIA-Workshop

MBSA and Fault-Tree software

DASSAULT AVIATION

CECILIA-Workshop

MBSA and Fault-Tree software



Nominal computation : Training/Tree/Ex2z_TopEvent(1.0)

Filter: None — Sort: by order — Limit at: None — C.A.A. — Fields

Cut's probability	Events	Comments	Given laws
1.5000E-10	OP	The operator has no time to intervene	constant 0.5
	Safety	Failure of safety chain	constant 3.0000E-10
1.6900E-08	Rod_1	Mechanical Holding of rod	constant 1.3000E-04
	Rod_2	Mechanical Holding of rod	constant 1.3000E-04
1.6900E-08	Rod_1	Mechanical Holding of rod	constant 1.3000E-04
	Rod_3	Mechanical Holding of rod	constant 1.3000E-04
1.6900E-08	Rod_2	Mechanical Holding of rod	constant 1.3000E-04
	Rod_3	Mechanical Holding of rod	constant 1.3000E-04
1.4450E-10	BK_1	Fail of coil	constant 1.7000E-05

Info. Cuts — Max Risk Approach (via BDD) ; 1 — Cuts : 53 (5.8024E-08)

Close

CECILIA interface

PRESENTATION

Dassault Aviation has been developing the dependability software CECILIA-Workshop, for more than 30 years. Owing to its fault-tree and MBSA modeling modules (based on the AltaRica language), the software has been successfully used for developing and certifying civil and military aircraft. CECILIA has become a real reference tool in this domain, through the certification of civil aircraft and integration of the method into the Guidelines and Methods (ARP4761a).

CECILIA includes advanced computation and easy-modeling functionalities that make it an ideal solution for all companies and business sectors. This is why Dassault Aviation decided to market it again in 2021 after an interruption period. SATODEV (which has been developing and maintaining the software since 2012) is in charge of the marketing process and user support.

FUNCTIONALITIES

Library of reusable components

Whether for building AltaRica models or fault trees, the tool includes a library to capitalize on models of system sections for later use. This helps create a complete model of a complex industrial system much faster (plane, submarine, air flow control, car, etc.).

Collaborative work

Collaborative work is one of CECILIA's strong points and is also crucial for users. It's an essential asset for meeting the requirements of a large-scale industrial program. The main functionalities are:

- User and group administration
- Detailed specification of access rights on all objects (system, tree, attributes, etc.).
- A versioning mechanism for each model, model part or tree for any development steps or evolutions.
- The possibility of definitively freezing an entire system and all its dependencies for any milestones.
- A clear separation of the different activities to allow different services to work in parallel on the same system.
- Common modeling/verification rules to ensure the consistency of the work carried out by several different people.

Modeling and processing fault trees

CECILIA has a user-friendly graphical entry interface for creating fault trees. Trees are created as part of a guided process in order to respect the Top -> Down approach. Basic events can be configured according to several probability distributions, and their parameters are either entered directly or connected to different data sources ensuring the traceability and justification of the values used.

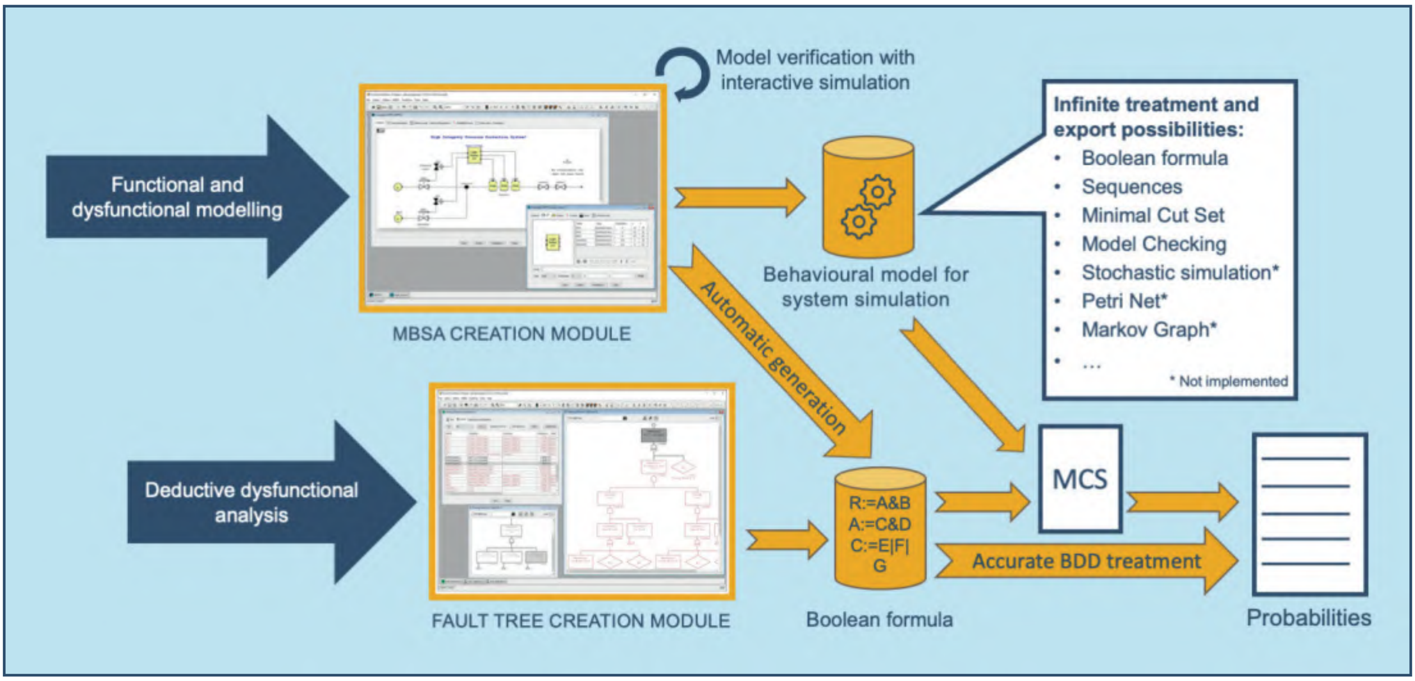
All processing is performed using a computation engine based on binary decision diagrams. All minimal cuts are provided without exception and probabilities are calculated without approximation. The specificities of the aeronautical domain are also covered by information concerning inspection periods and in-flight tests.

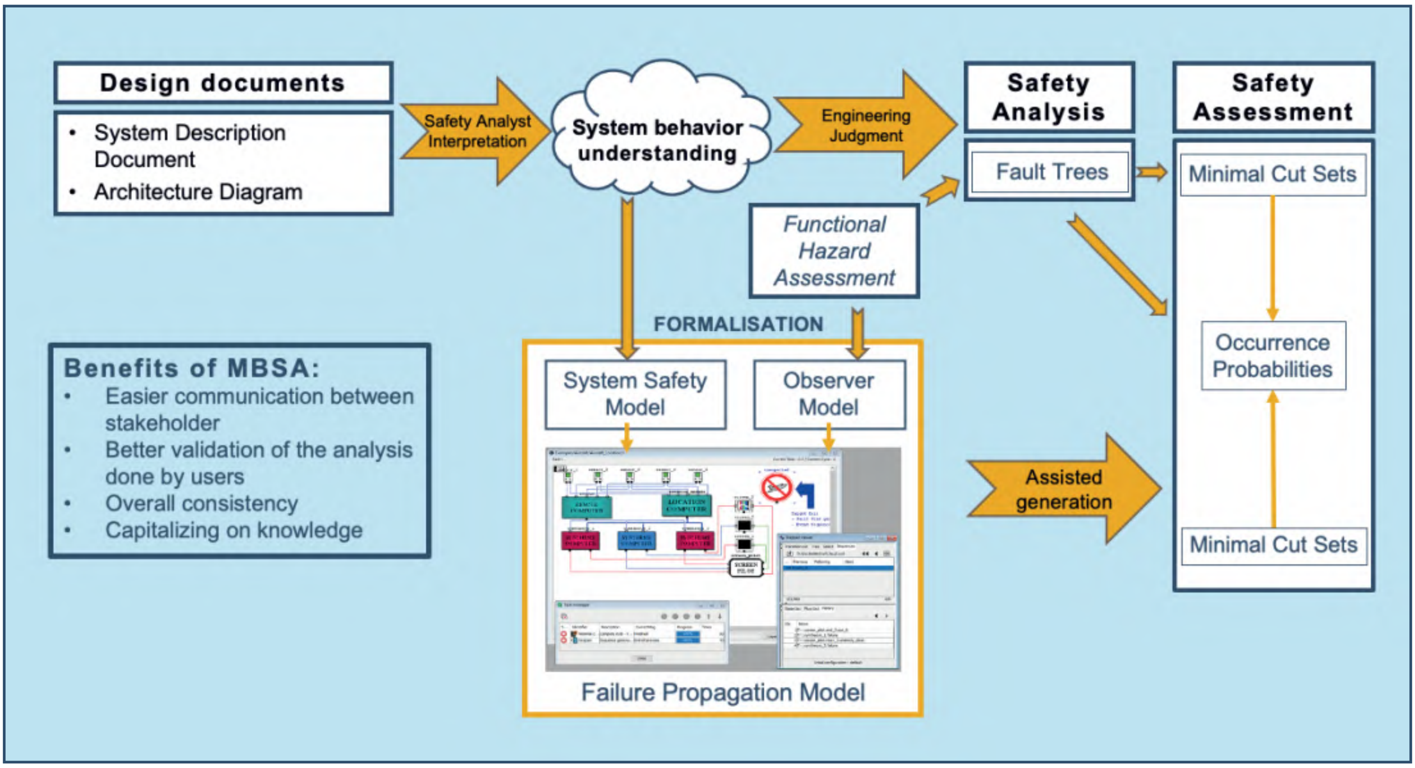
The notion of attributes enables a better description of events and makes it possible to run Common Attributed Analyses through post-processing of minimal cuts.

“Calculation after first failure” is a mechanism that simulates a component failure at t=0 in order to analyze the reliability of the system with a pre-existing failure. When all the pre-existing failure calculations have been performed, the software generates a summary table to help the user draw up a Minimum Equipment List.

All the data entered, and the results can then be printed in PDF format. The automatic page layout and vector printing guarantee perfect readability of the reports whatever the size of the medium (A4, A3, A2, etc.).

CECILIA workflow





Safety analysis methods with MBSA

Modeling and MBSA processing

What sets CECILIA-Workshop apart from other dependability tools, is its management of the MBSA (Model Based Safety Assessment). When systems become dynamic and complex, the fault tree approach is no longer sufficient, either because of the mathematical limitations of Boolean approaches, or because it cannot take into account changes in hypotheses within an acceptable amount of time.

An MBSA model describes both the functioning and dysfunctioning of the system, allowing better communication between the system engineering and the people running the Safety analyses. The model of each component or equipment item can be simulated step by step to check how closely it reflects reality. This interactive simulation enables a better identification of failure leading to the top event, and shows possible side effects that would be difficult to predict with complex systems.

Hierarchical by nature, MBSA modeling is perfectly adapted to large industrial systems comprising interconnected sub-systems/equipment/components.

Even though it is just one of the many MBSA possibilities offered by CECILIA-Workshop, the automatic generation of Boolean formulas is undeniably a key functionality. It produces exactly the same results as a fault tree created manually, while making it much easier to check/validate results when the systems are made up of thousands of components. A minor change in the functioning of the system causes only a minor change in the MBSA model, and it is no longer necessary to totally recreate the fault tree. Only one modeling is necessary for the study of all the top events. This generation of Boolean formula from MBSA enables every post-treatment of the fault tree part (CAA, MAL, etc.)

Advanced processing options

To help users save time, the software features a batch calculation system that automatically starts calculations and exports results.

A distributed calculation plugin enables users to run calculations at a distance on one or several servers in parallel in order to drastically reduce calculation times compared to those of a laptop.

USES

Safety

At Dassault Aviation, CECILIA Workshop was successfully used to certify civil aircraft (Falcon), the multi-role fighter aircraft Rafale, and the nEUROn combat drone. These programs involved up to 80 users on several sites and contributed to proving that the software meets the expectations of users and the certification authorities alike.

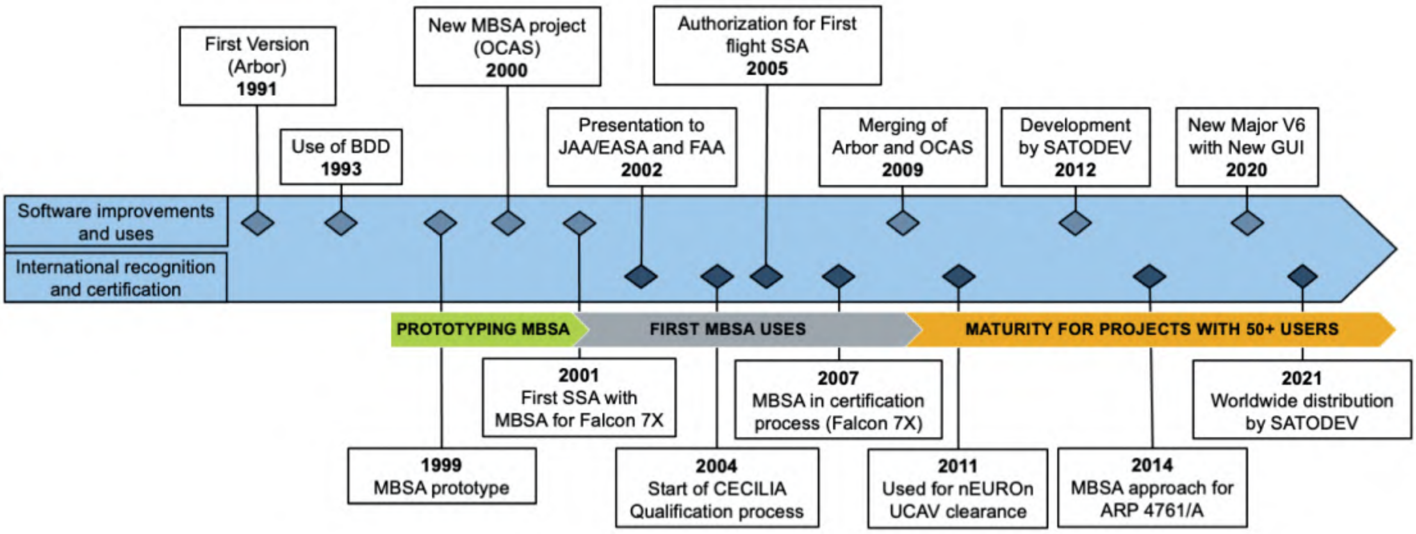
Other applications

Outside safety applications in aeronautics, MBSA has already been used to perform operational efficiency calculations, testability/diagnosis studies and accident investigations in different areas. Step by step simulation can also be used as an educational tool to explain the functioning of a system in a training course. MBSA can adapt to any business sectors.

CONCLUSION

CECILIA-Workshop benefits from several decades of research and development and has already proved its worth on the sites of several industrial players. It has become a reference tool for MBSA in the aeronautical sector and can adapt to your company's requirements.

The software is constantly evolving and also features a plugin system to extend its functionalities and meet specific needs.


First Version (Arbor) 1991
Use of BDD 1993
New MBSA project (OCAS) 2000
Presentation to JAA/EASA and FAA 2002
Authorization for First flight SSA 2005
Merging of Arbor and OCAS 2009
Development by SATODEV 2012
New Major V6 with New GUI 2020
Software improvements and uses
International recognition and certification
PROTOTYPING MBSA
FIRST MBSA USES
MATURITY FOR PROJECTS WITH 50+ USERS
1999 MBSA prototype
2001 First SSA with MBSA for Falcon 7X
2004 Start of CECILIA Qualification process
2007 MBSA in certification process (Falcon 7X)
2011 Used for nEUROn UCAV clearance
2014 MBSA approach for ARP 4761/A
2021 Worldwide distribution by SATODEV

PRACTICAL INFORMATION

Required configuration: Windows 10, OpenJDK8, PostgreSQL 11,12,13, Core I3 or later version, 4 GB available RAM, 400 MB disk space for installation.

The distributor of CECILIA-Workshop is SATODEV 58 avenue Marcel Dassault 33700 MERIGNAC (FRANCE). For more detailed information, please write to: contact@satodev.fr.

Trainings are available off-site at SATODEV office or on-site at your office.

You can also find more information on the website https://satodev.com/.
Please contact cecilia@satodev.fr to obtain a demo version.