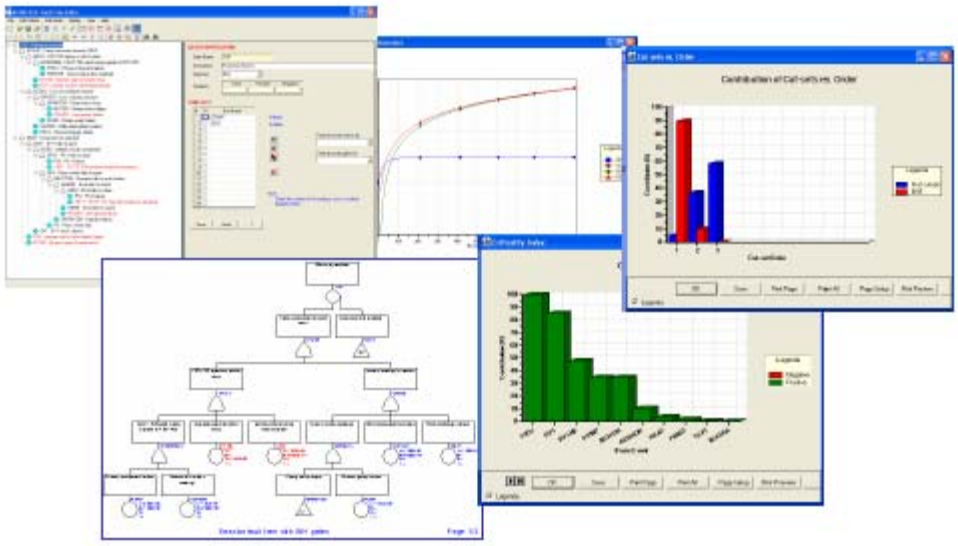
JRC Scientific and Technical Reports

ASTRA 3.0: Test Case Report

Results of a subset of test cases selected from those considered during the ASTRA testing activity

Sergio Contini, Vaidas Matuzas



EUR 24124 EN - 2009

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Sergio Contini
E-mail: Sergio.contini@jrc.ec.europa.eu
Tel.: +39 0332 789217
Fax: +39 0331 785145

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 55894

EUR 24124 EN
ISBN 978-92-79-14608-4
ISSN 1018-5593
DOI 10.2788/51332

Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

SUMMARY

In the context of activities related to the application of system analysis to safety and security of critical installations a new logical and probabilistic fault tree analysis procedure was developed and implemented in the software package ASTRA, version 3.0. This report contains the results of the logical and probabilistic analysis for a limited, but significant, subset of test cases considered during the test campaign performed at the JRC. Most of the described test cases come from the open literature, for which results are available to the reader. For more complex test cases ASTRA 3.0 was compared with other available tools, such as ASTRA 2.0 and XS-MKA, a Markovian analysis package. The experience gained with the testing activity also allowed the identification of a set of recommendations for future improvements.

TABLE OF CONTENTS

1. INTRODUCTION

This report describes the results of the application of ASTRA 3.0 to a set of test cases selected among those considered during the beta testing carried out at the JRC. ASTRA 3.0 is a Fault Tree Analyser (FTA) based on the state-of-the-art approach of Ordered Binary Decision Diagrams (OBDD). An OBDD is directed acyclic graph particularly suitable to efficiently analyse fault trees. A vast literature on the BDD approach applied to fault tree analysis is available, to which the interested reader is addressed, e.g. Bryant (1986); Rauzy (1996).

The main advantages of the OBDD approach, compared with the previous approach for fault tree analysis based on cut sets manipulation, rely on the possibility to:

- perform the probabilistic analysis directly on the OBDD, i.e. without the need of calculating the Minimal Cut Sets, (MCS);
- determine the exact values of the top event unavailability, expected number of failure and repair, as well as the importance measures of basic events, thus avoiding any problem of numerical approximation implied in the so-called bound-approaches;
- obtain a graph embedding all MCS, from which the Significant Minimal Cut Sets (SMCS) can easily be extracted using cut-off techniques.

The logical and probabilistic analysis implemented in ASTRA 3.0 allows the user to analyse both coherent and non coherent fault trees. Briefly speaking non coherent fault trees contain basic events in both positive and negated forms.

All these feature make ASTRA 3.0 suitable not only for safety applications, but also for security related ones…

ASTRA 3.0 was extensively verified on a large number of fault trees. The JRC internal test campaign was subdivided in different phases:

- Test of the logical analysis procedure, i.e. the construction of the BDD and the determination of the MCS;
- Tests of the probabilistic analysis procedure;
- Tests of the user interface;
- Test of the Fault tree Editor, Components' reliability database, Fault tree drawing, and Report Writer.

This report contains an extract of the test cases that were considered for checking the correctness of the implemented logical and probabilistic analysis algorithms. A good deal of the selected test cases comes from the open literature, for which results are available to the reader. For some other test cases ASTRA 3.0 was compared with other software for fault tree analysis such as ASTRA 2.0, ARALIA, RiskSpectrum and with the Markovian analysis tool XS-MKA. The experience gained with the test campaign was then summarised in a set of recommendations for future implementations.

The next section gives an overview of the main probabilistic analysis equations implemented in ASTRA 3.0. The test cases are provided is Section 3. Section 4 summarizes main findings and highlights areas for further development…

2. SUMMARY OF EQUATIONS FOR PROBABILISTIC ANALYSIS IMPLEMENTED IN ASTRA 3.0

The following parameters results from the probabilistic analysis performed on the Labelled Binary Decision Diagrams (LBDD):

- Unavailability;
- Unconditional failure and repair frequencies;
- Expected number of failure and repair;
- Unreliability;
- Characteristic times (MTTF, MTTR, MTBF);
- Importance measures of basic events;

This section contains the list of equations implemented in ASTRA.
Details can be found in Contini-Matuzas (2009).

2.1 Notation

λ	Failure rate (constant)
μ	Repair rate (constant)
τ	Repair time ($\tau = 1 / \mu$)
θ	Time between tests
θ_0	First time to test
$\omega(t)$	Unconditional failure frequency
$\upsilon(t)$	Unconditional repair frequency
$q(t)$	Basic event unavailability
$\Lambda_T(t)$	Top event conditional failure frequency
$Q_T(t)$	Top event Unavailability at time t
$Q_T(0)$	Top event Unavailability at t=0
$W_T(t)$	Top event Expected number of failures in 0-t
$V_S(t)$	Top event Expected number of repair in 0-t
$F_T(t)$	Top event Unreliability in 0- t
$Q_{Cj}(t)$	Top event Unavailability at time t for the j-th MCS
$Q_{Cj}(0)$	Unavailability at t=0 for the j-th MCS
$W_{Cj}(t)$	Expected number of failures in 0-t for the j-th MCS
$F_{Cj}(t)$	Unreliability in 0- t for the j-th MCS
MTBF	Mean Time Between failures
MTTR	Mean Time To Repair
MTTF	Mean Time To failure
MTTFF	Mean Time To First Failure
BE	Basic event
MCS	Minimal Cut Set
SMCS	Significant MCS
Ne	Number of basic events of the fault tree
n	Number of basic events in an MCS/SMCS
T	Mission time
$p^f_x(t)$	Probability of failure critical state for the generic event x
$p^r_x(t)$	Probability of repair critical state for generic event x
$IC_x(t)$	Criticality index of event x at time t
$RAW_x(t)$	Risk Achievement Worth of event x at time t
$RRW_x(t)$	Risk Reduction Worth of event x at time t
IS_x	Structural criticality of event x

2.2 Unavailability and failure frequency of basic events

ASTRA 3.0 allows the use of four different types of components:
- Un-repairable;
- On-line maintained;
- Periodically tested/inspected;
- Acting on demand.

The equations applied for determining the unavailability at basic event level are provided in Table 1.

Table 1. Equations for determining the basic events' unavailability

Event type	Unavailability	unconditional failure frequency	unconditional repair frequency
Not repairable	$q(t) = 1 - e^{-\lambda t} + q(0)\, e^{-\lambda t}$	$\omega(t) = [1 - q(t)]\,\lambda$	$\nu(t) = q(t)\,\mu$
On-line maintained	$q(t) = \frac{\lambda}{\lambda+\mu}(1 - e^{-\lambda t}) + q(0)\, e^{-(\lambda+\mu)t}$	$\omega(t) = [1 - q(t)]\,\lambda$	$\nu(t) = q(t)\,\mu$
Periodically tested inspected	$q(t) = 1 - e^{-\lambda t}$ for $0 \le t < \vartheta_0$ $q(t) = \frac{\tau}{\theta} q(\theta_k^*) + (1 - q(\theta_k^*))\,(1 - e^{-\lambda(t-\theta_k^*)})$ for $\vartheta_k^* \le t < \vartheta_k^* + \tau$ $q(t) = 1 - e^{-\lambda(t-(\theta_k^*+\tau))}$ for $\vartheta_k^* + \tau \le t < \vartheta_{k+1}^*$ and k = 0,1,2,… where $\vartheta_k^* = \vartheta_0 + k\vartheta$ and $\vartheta_{k+1}^* = \vartheta_0 + (k+1)\vartheta$	$\omega(t) = [1 - q(t)]\,\lambda$ applied to all time between test intervals	$\nu(t) = q(t)\,\mu$ applied to all time between test intervals
Acting on demand	q(t) = q(0) = const	$\omega(t) = 0$	$\omega(t) = 0$

2.3 Unavailability of a simple module

Let k be the k-th simple module of the modularized fault tree.

The unavailability of a simple module $Q_k(t)$ is calculated on the LBDD as:

$$Q_k(t) = q_x(t)\, Q_{1x}(t) + [1 - q_x(t)]\, Q_{0x}(t)$$

$Q_{1x}(t)$ and $Q_{0x}(t)$ are respectively the unavailability of the left (successful state) and right (failed state) branches of the node and $q_x(t)$ is the unavailability of the basic event x associated to the node.

If *x* represents a negated variable, say $\bar{x}$, then $q_{\bar{x}}(t) = 1 - q_x(t)$.

Probability of critical states for basic event x in a simple module

Let $\phi_k(\mathbf{x_k})$ be the logical function of the k-th simple module containing the vector of basic events $\mathbf{x_k}=\mid x_1,x_2,..,x_{nk}\mid$.
$p^f_{xk}(t) = Pr\{\phi_k\big|_{x=1} \wedge \overline{\phi_k\big|_{x=0}}\}$ is the probability that the generic event $x \in \mathbf{x_k}$ is critical, i.e. the module is verified if x = 1 and is not verified if x = 0;

$p^r_{xk}(t) = Pr\{\phi_k\big|_{x=0} \wedge \overline{\phi_k\big|_{x=1}}\}$ is the probability that the generic event $x \in \mathbf{x_k}$ in complemented form is critical, i.e. the module is verified if x = 0 and is not verified if x = 1;

If the event x appears in the positive form only, then $p^r_x(t) = 0$.
If the event x appears in the negated form only, then $p^f_x(t) = 0$.

These values are calculated for each event in each simple module.

2.4 Probabilistic quantification of the Top-module

Top event Unavailability

The variables in the LBDD of the Top-module can be simple modules and basic events.
The Top event unavailability is calculated on the Top-module as a function of the unavailability of its variables by applying the same algorithm used for simple modules.
Besides $Q_{Top}(t)$ for $0 \le t \le T$, if tested events are present, then ASTRA also calculates the mean value

$$Q^{mean}_{Top} = \int_0^t Q_T(\tau)\, d\tau$$

and the peak value Q^{peak}_{Top}.

Probability of critical states for basic events

Indicating with $p^f_k(t)$ and $p^r_k(t)$ the probability of critical states for the simple module k in the Top-module, the values $p^f_x(t)$ and $p^r_x(t)$ for event x in the input tree are obtained by means of the following equations:

$$p^f_x(t) = p^f_{xk}(t)\, p^f_k(t) + p^r_x(t)\, p^r_k(t)$$

$$p^r_x(t) = p^r_{xk}(t)\, p^f_k(t) + p^f_{xk}(t) p^r_k(t)$$

Unconditional failure and repair frequencies of the Top event

The probability of critical state determined for all basic events allow calculating the unconditional failure and repair frequencies of the Top event.

$$\omega_T(t) = \sum_{x=1}^{Ne} p^f_x(t)\, \omega_x(t) + \sum_{x=1}^{Ne} p^r_x(t)\, \upsilon_x(t) \qquad (1)$$

The unconditional repair frequency is given by:

$$\upsilon_T(t) = \sum_{x=1}^{Ne} p^r_x(t)\, \omega_x(t) + \sum_{x=1}^{Ne} p^f_x(t)\, \upsilon_x(t) \qquad (2)$$

Top event Expected number of failures

The Expected Number of Failures $W_T(t)$ is obtained as:

$$W_T(t) = \int_0^t \omega_T(\tau)\,d\tau + Q_T(0)$$

The ENF can also be interpreted as the upper bound for the unreliability $F_T(t)$.

If $\omega_T(t) \approx$ constant then $MTBF_T = \frac{1}{\omega_T(t)}$; if $Q_T(t) \approx$ constant then $MTTR_T = Q_T^{mean}$ $MTBF_T$

Top event Expected number of repairs

If there are neither INH gates nor tested events then also the Expected Number of Repair $V_T(t)$ is calculated as:

$$V_T(t) = \int_0^t \upsilon_T(\tau)\,d\tau$$

Top event Unreliability upper bound

For safety applications the Expected Number of Failure is generally a good upper bound for the top-event unreliability $F_T(t)$, provided that the unconditional failure frequency is constant or approximately constant.
A second bound for $F_T(t)$ is determined by ASTRA 3.0 when the unconditional failure frequency is not constant. In these cases the conditional failure frequency at Top level is determined on the basis of the unconditional failure frequency $\omega_T(t)$ and unavailability $Q_T(t)$, i.e.:

$$\Lambda_T(\tau) = \frac{\omega_T(\tau)}{1 - Q_T(\tau)}$$

Then,

$$F_T(t) = 1 - [1 - Q_T(0)]\, e^{-\int_0^t \Lambda_T(\tau)\,d\tau}$$

Mean time to first failure is given by: $MTTFF_T = \int_0^\infty (1 - F_T(t))\,dt$

2.5 Importance measures of basic events

The following importance measures are provided by ASTRA 3.0:

- Probability of critical state;
- Criticality;
- Risk Achievement Worth;
- Risk Reduction Worth.
- Structural importance;

For each importance measure two contributions are determined for events in double form, since such events are present in positive and negated forms.

Probability of critical states $p^f_x(t)$ and $p^r_x(t)$

The equations for determining the probability of critical state $p^f_x(t)$ for positive variables and $p^r_x(t)$ for negated variables (or negated part of double form variables) have been given above.

Criticality importance measure, IC_x

This index represents the probability that the event *x* is critical and its occurrence leads to system failure.

$$IC_x^+(t) = p_x^f(t)\frac{q_x(t)}{Q_T(t)}$$

For negated variables:

$$IC_x^-(t) = p_x^r(t)\frac{1-q_x(t)}{Q_T(t)}$$

Risk Achievement Worth, RAW_x

The RAW is defined as a measure of the increase of the system failure probability when *x* is supposed failed or removed e.g. for test/maintenance operations. In calculating the RAW it is important to consider all other components that are dependent by the failure / removal of *x*. According to the definition:

$$RAW_x^+(t) = 1 + p_x^f(t)\frac{1-q_x(t)}{Q_T(t)}$$

For negated variables:

$$RAW_x^-(t) = 1 + p_x^r(t)\frac{q_x(t)}{Q_T(t)}$$

Risk Reduction Worth RRW_x

The RRW is defined as a measure of the decrease of the system failure probability when *x* is supposed to be perfectly working:

$$RRW_x^+ = \frac{Q_T}{Q_T - p_x^f(t)\,q_x(t)}$$

For negated variables:

$$RRW_x^- = \frac{Q_T}{Q_T - p_x^r(t)[1-q_x(t)]}$$

Structural importance IS_x

The Structural importance is determined by applying the equation $p^f_x(t)$ and $p^r_x(t)$ in which all events have probability 0.5.

2.6 Probabilistic quantification of SMCS

The determination of the SMCS is followed by the probabilistic quantification of each of them for the determination of: Unavailability, unconditional failure frequency, Expected number of failures, and Unreliability.

Unavailability of a MCS

$$Q_{Cj}(t) = \prod_{i=1}^{nj} q_i(t)$$

Expected number of failures of a MCS

The ENF of a MCS is obtained by integrating, over the mission time interval, the unconditional failure frequency of the SMCS given by:

$$\omega_{Cj}(t)\,dt = \sum_{x=1}^{nj} \omega_x(t) \prod_{\substack{k=1 \\ k\neq x}}^{nx} q_k(t)\,dt \qquad (3)$$

The above equation expresses the concept that the SMCS occurs in a time interval t, t+dt if:

- *n-1* events have already been occurred at t, given by $\prod_{\substack{k=1 \\ k\neq i}}^{nj} q_k(t)$
- the last one occurs in *dt*, expressed as $\omega_i(t)\,dt$

The last event to occur may be the first, the second, and so on, that's why the use of the summation.

$$W_{Cj}(t) = \int_0^t \omega_{Cj}(\tau)\,d\tau + Q_{Cj}(0)$$

Unreliability upper bound of a MCS

As for the Top event, the unreliability of a MCS is calculated by means of the conditional failure frequency of the MCS.

$$\Lambda_{Cj}(\tau) = \frac{\omega_{Cj}(\tau)}{1 - Q_{Cj}(\tau)}$$

Then,

$$F_{Cj}(t) = 1 - [1 - Q_{Cj}(0)]\, e^{-\int_0^t \Lambda_{Cj}(\tau)\,d\tau}$$

2.7 Probabilistic quantification of initiating and enabling events

The two descendants of an INH gate represent the initiator of a perturbation of one or more process variables beyond a safety threshold that, if not interrupted by the intervention of the protection system (enabler event) a dangerous situation arises.

When the parameter of interest is the frequency of the catastrophic Top event then in equations (1), (2) and (3) enabler events are characterised by their on-demand unavailability $q_x(t)$ only, i.e. their unconditional the failure and repair frequencies are set to zero.

3. RESULTS OF TESTS ON SELECTED SAMPLE CASES

In this section the results of the performance of ASTRA 3.0 for a significant set of test cases, most of which taken from the scientific literature, are provided. The correctness of the results of ASTRA has been verified against the values reported in the various reference sources. Several test cases have been compared with the Markov modelling analysed by means of the software XS-MKA developed by De Cola, (2005).
Each test case taken from the literature is identified by means of the ASTRA filename and the bibliographical reference.
For testing purposes the probabilistic values are represented with more than two significant digits.

The considered examples range in complexity from a single component and simple fault trees up to complex fault trees.

In this report for each test case the following information is given:
- Name of the ASTRA input file;
- Source of the test case;
- ASTRA results and comparison with the results from the referenced source;
- Conclusion on the results given by ASTRA;
- Suggestions for further implementations (if any).

Input files for all the test cases can be obtained, under request, from the authors.

3.1. Simple systems with repairable, un-repairable and tested components

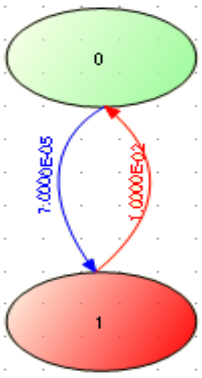
3.1.1 Single repairable component

Source: ASTRA Development team

Problem description

Determine the following parameters for a single repairable component, at three different mission times.

- Unreliability F
- Unavailability Q
- Expected number of failures W
- Expected number of repair V
- Mean Time Between failures MTBF
- Mean Time To Repair MTTR
- Mean Time To failure MTTF



The component is characterised by:
Failure rate λ = 1.0e-5
Repair rate μ = 1.0e-2

The following tables contain the results of the analysis performed by means of XS-MKA and ASTRA for different mission time intervals.

	XS-MKA $T = 10^3$	**ASTRA** $T = 10^3$
F	9.95017e-3	9.95016e-3
Q	9.98959e-4	9.98956e-4
W	9.99100e-3	9.99100e-3
V	8.99173e-3	8.99188e-3

XS-MKA $T=10^4$	**ASTRA** $T=10^4$		**XS-MKA** $T=10^5$	**ASTRA** $T=10^5$
9.51626e-2	9.51626e-2		0.632120	0.632120
9.99001e-4	9.99001e-4		9.99001e-4	9.99001e-4
9.99011e-2	9.99011e-2		0.999002	0.999002
9.89017e-2	9.89017e-2		0.998002	0.998002

	XS-MKA	**ASTRA**
MTBF	1.00100e+5	1.00100e+5
MTTR	100	100
MTTF	1.0e+5	1.0e+5

Conclusion. The comparison of the results given by ASTRA with those of XS-MKA proves that ASTRA works properly.

3.1.2 Filename: Series1

Source: Modarres book (1999), page 199.

Problem description:
Given the Series of three not repairable units, determine: system failure rate, unreliability at 1000 h and MTTF.

Data:
$\lambda_1 = 4.e-6$ $\lambda_2 = 3.2e-6$ $\lambda_3 = 9.8e-6$

Results:

Parameter	**Modarres**	**ASTRA**
λ_S	1.7 e-5	1.7 e-5
$F_S(1000)$	1.7 e-2	1.6856e-2
$MTTF_S$	58823 h	58855 h

The small disagreements between the unreliability values is due to the approximation introduced in the reference source (use was made of $R_S(1000) = 0.983$ instead of $R_S(1000) = 0.9831$).

The difference between the values of MTTF is due to the different method used. In ASTRA the MTTF is calculated as $MTTF_S = \int_0^{+\infty} (1 - F_S(t))\,dt$. In this particular case, being the component in series $\lambda_S = \sum_{i=1}^{3} \lambda_i$ and $MTTF_S = \frac{1}{\lambda_S} = \frac{1}{1.7\ x10^{-5}} = 58823.$

Conclusion: ASTRA performs correctly.

3.1.3 Filename: Series2

Source: Kumamoto-Henley (second edition), Example 17, page 397.

Problem description:
Determine the unavailability and the unconditional failure frequency for each component of a Series of three repairable components. Mission time (hours):1100 h

Data:

Comp.	Failure Rate	Repair Time
1	1.0 E-03	10
2	2.0 E-03	40
3	3.0 E-03	60

Results from K-H

Component1: q = 9.90e-3 ω = 9.90e-4
Component2: q = 7.41e-2 ω = 1.85e-3
Component3: q = 1.53e-1 ω = 2.54e-3

Results from ASTRA

Event Name	Unavailability q	Unconditinal failure freq. ω
1=A	9.900990E-03	9.900991E-04
2=B	7.407408E-02	1.851852E-03
3=C	1.525424E-01	2.542373E-03

Same case, but considering that the repair time is equal to zero. Mission time (hours):1100 h

Results from K-H

Component1: q = 0.632 ω = 3.33e-4
Component2: q = 0.889 ω = 2.22e-4
Component3: q = 0.963 ω = 1.11e-4

Results from ASTRA

Event Name	Unavailability q	Unc. Failure Frequency ω
1=A	0.6671289	3.328711E-04
2=B	0.8891969	2.216063E-04
3=C	0.9631168	1.106495E-04

Comment: good agreement, except for the unavailability of the first component, which is wrong in the K-H book (printing mistake).

Conclusion: ASTRA performs correctly.

3.1.4 Filename: Parallel1

Source: Modarres book, page 202.

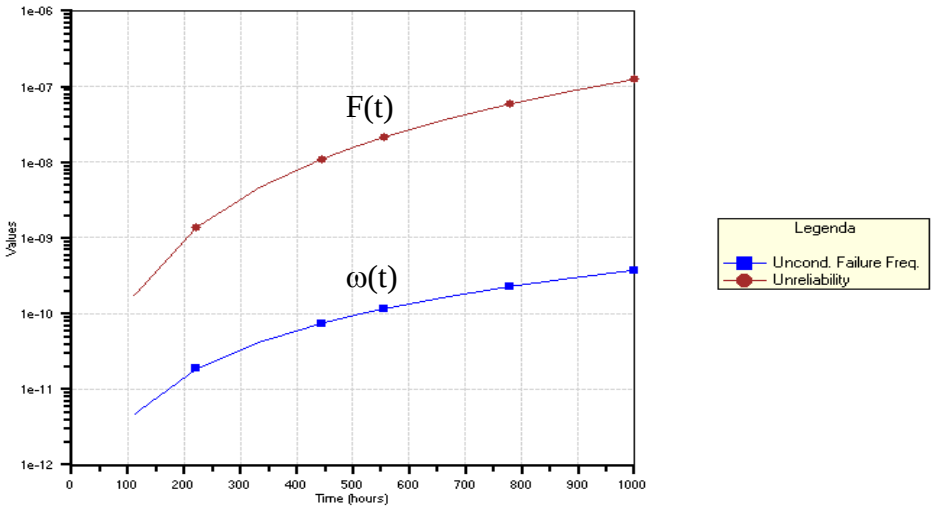
Problem Description:
Given a Parallel System of three not repairable units, determine: the system unreliability at 1000h and the MTTF.

Data:
$\lambda_1 = 4.e-6$ $\lambda_2 = 3.2e-6$ $\lambda_3 = 9.8e-6$

Results:

Parameter	Modarres	ASTRA
$F_S(1000)$	1.25 e-7	1.2439e-7
$MTTF_S$	4.35 e+5 h	4.35 e+5 h

The following picture shows the curves of the unreliability and of the increasing unconditional failure frequency (conservative approximation of the failure rate) for the parallel system.



In Modarres the MTTF is calculated analytically.

The small difference between the values of MTTF is due to the different method used. In ASTRA the MTTF is calculated as $MTTF_S = \int_0^{+\infty} (1 - F_S(t))\,dt$. The precision of the result depends on the integration parameter εr, representing the relative error.

For this test case the following table shows the variation of the calculated MTTF as a function of εr. The last column contains the running times

εr	MTTF(h)	Time (s)
10^{-3}	94842	< 0.1
10^{-4}	335230	< 0.1
10^{-5}	422600	0.29
10^{-6}	433785	0.5
10^{-7}	434950	0.68
10^{-8}	435070	1.1

The MTTF could also be calculated with a separate run in which the mission time is set very long. Considering for instance the mission time of 10^7 h for the parallel system, ASTRA gives the exact value, i.e. MTTF = 435080 in about 0.03 seconds.

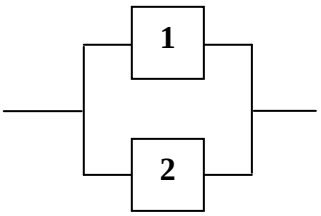
These results seem to suggest that it is preferable to perform a separate run for the determination of the MTTF for systems with non repairable components.
Moreover, since the numerical integration is time consuming it is suggested to adopt the approximated expression applicable when the system failure rate is constant.

3.1.5 Filename: And-Rip

Source: ASTRA Development team.

Problem Description:
Given a Parallel System of two repairable units, determine:

- The steady-state system unavailability, Q;
- The mean time between failures, MTBF;
- The mean time to repair, MTTR;
- The mean time to failure, MTTF;
- The conditional failure frequency Λ;
- The conditional repair frequency M.



Data:
λ_1 = 1 e-3, μ_1 = 0.1
λ_2 = 1 e-4, μ_2 = 0.01

The reference tool used is XS-MKA implementing the markovian analysis.

Parameter	XS-MKA	ASTRA
Q	9.8029 e-5	9.8029 e-5
MTBF	9.2736 e 4	9.2736 e 4
MTTR	9.0909	9.0909
MTTF	9.2727 e4	9.2727 e4
Λ	1.0784 e-5	1.0784 e-5
M	0.11	0.11

The analysis with ASTRA has been performed using a mission time of 100,000 h.

Conclusion: From the content of the above table it is possible to conclude that ASTRA performs correctly.

3.1.6 Majority voting system with not repairable components

Source: Rausand & Houland book, page 161.

Problem Description 1:
Given a system composed of N components. The system works if at least K out of N components work, indicated as K/N or KooN. Determine the system unreliability at 1000h and the MTTF.
Data: $\lambda = 1.0e-4$ for all components

The Reliability (survival probability) for KooN redundant configurations in the hypotheses of identical components is given by:

$$R(t) = \sum_{x=K}^{N} \binom{N}{K} e^{-\lambda x t} (1 - e^{-\lambda x t})^{N-x}$$

It can be shown that $MTTF = \frac{1}{\lambda} \sum_{x=K}^{N} \frac{1}{x}$

The following Table gives the expressions for the MTTF for different configurations of identical components.

K	**N**	**1**	**2**	**3**	**4**	**5**
1		1/λ	3/2λ	11/6λ	25/12λ	137/60λ
2		---	1/2λ	5/6λ	13/12λ	77/60λ
3		---	---	1/3λ	7/12λ	47/60λ
4		---	---	---	1/4λ	9/20λ
5		---	---	---	---	1/5λ

In this table 1ooN represents a parallel configuration since we are determining the reliability (the system works if at least one component out of N works), whereas KooN is a series configuration (the system works if all components work).

The results for equal components with $\lambda = 1.0e-4$ are as follows.

K	**N**	**1**	**2**	**3**	**4**	**5**
1		1e+4	1.5e+4	1.8333e+4	2.0833e+4	2.2833e+4
2		---	5e+3	8.333e+3	1.0833e+4	1.2833e+4
3		---	---	3.3333e+3	5.8333e+3	7.8333e+3
4		---	---	---	2.5e+3	4.5e+3
5		---	---	---	---	2.0e+3

Problem Description 2:
The objective is to determine the MTTF of different configurations using the fault tree technique. Since the FTA refers to the unreliability, the equations for determining the MTTF change since the working logic is different from the failure logic. Indeed, in the failure logic 1ooN represents a series configuration (the system fails if at least one component out of N fails), whereas NooN is a parallel configuration (the system fails if all components fail). Moreover if the system works with K components working, it will fail if N-K+1 component fail.

Therefore the KooN in the first Table become (N-K+1)/N in the following Table.

K	N	1	2	3	4	5
1		1/λ	1/2λ	1/3λ	1/4λ	1/5λ
2		---	3/2λ	5/6λ	7/12λ	9/20λ
3		---	---	11/6λ	13/12λ	47/60λ
4		---	---	---	25/12λ	77/60λ
5		---	---	---	---	137/60λ

The results for equal components with $\lambda = 1.0e-4$ determined using ASTRA 3.0 are as follows.

K	N	1	2	3	4	5
1		1e+4	5e+3	3.3333e+3	2.5e+3	2.0e+3
2		---	1.5e+4	8.333e+3	5.8333e+3	4.5e+3
3		---	---	1.8333e+4	1.0833e+4	1.2833e+4
4		---	---	---	2.0833e+4	7.8333e+3
5		---	---	---	---	2.2833e+4

These results have been obtained using the "Relative error parameter RE" = 1e-4 and a very long mission time T = 1.0e+6. Indeed, as already pointed out, the computation time for the determination of the unreliability is lower using a very long mission time.

The precision of the results depends also on the failure rate value. Consider some of the above configurations and suppose that λ = 1e-7. The following table gives the ASTRA results obtained using different values for the "Relative error parameter". The calculations have been performed using a mission time T = 1.0e+6.

Working logic	MTTF exact value	Failure logic	MTTF (h) RE = 1e-6	MTTF (h) RE = 1e-7	MTTF (h) RE = 1e-8
1oo2	1.5e+7	2oo2	1.361375e+7	1.485121e+7	1.498501e+7
2oo2	5.0e+6	1oo2	6.10701e+6	6.10701e+6	6.10701e+6
2oo3	8.33333e+6	2oo3	7.920150e+6	8.291366e+6	8.329153e+6
2oo4	1.083333e+7	3oo4	1.028207e+7	1.077836e+7	1.082789e+7
2oo5	1.283333e+7	4oo5	1.216790e+7	1.276786e+7	1.282687e+7
3oo4	5.833333e+6	2oo4	5.634183e+6	5.813490e+6	5.831369e+6
4oo4	2.5e+6	1oo4	2.439027e+6	2.493765e+6	2.499375e+6
4oo5	4.5e+6	2oo5	4.382567e+6	4.488402e+6	4.498856e+6

Therefore it is advisable to determine the MTTF using different values of RE, with a very long mission time, in order to judge the suitability of the chosen parameters' values.

Conclusion: From the content of the above table it is possible to conclude that ASTRA works correctly.

Suggestion: implement the exact formula for MTTF of not repairable configurations

3.1.7 Majority voting system with tested components and different testing policy

Source: JRC ASTRA development team

Problem description:
Determination of the point-wise and of the mean unavailability of a 2oo3 system considering the three different types of testing policy: simultaneous, sequential and staggered.

Top = a b + a c + b c

The system contains equal components characterised by the following data:

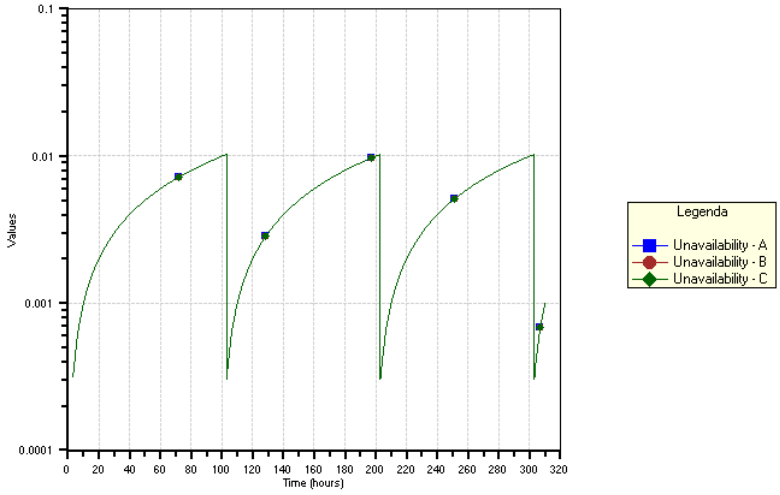
- failure rate = 1.e-4
- repair time = 1 h
- test interval = 100 h

1. Simultaneous testing policy. Filename: **Tested-Simultaneous-2oo3**

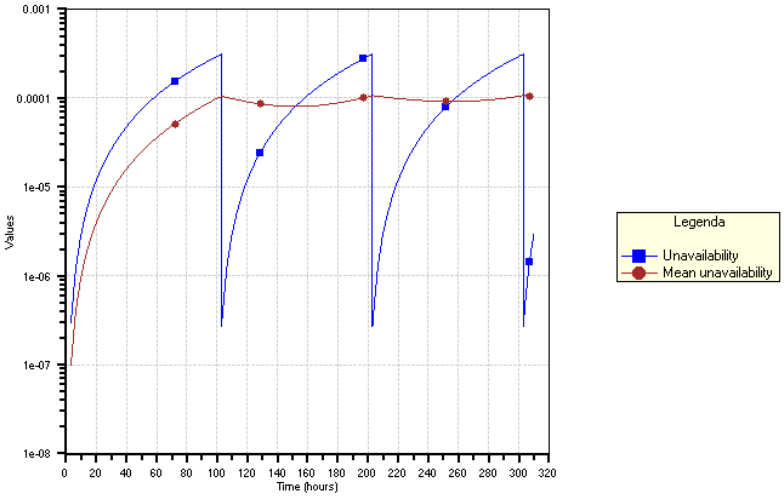
Components are all put off-line for testing and repair for a time interval given by the sum of the repair time of each component. In the hypothesis that the duration of the test is negligible, the data to be used are as follows:

x	λ h^{-1}	τ h	θ h	θo h
A	1.e-4	3	100	0.0
B	1.e-4	3	100	0.0
C	1.e-4	3	100	0.0

The unavailability of each component is shown in the following figure.



At both system and components level the unavailability has the classical saw-tooth behaviour.
The maximum value of the components' unavailability is about 10^{-2} just before the test.
The mean system unavailability is 9.8500 x 10^{-5}, which follows the behaviour displayed in the following figure.
The maximum value of the 2oo3 system unavailability is 3.00927 x 10^{-4}.

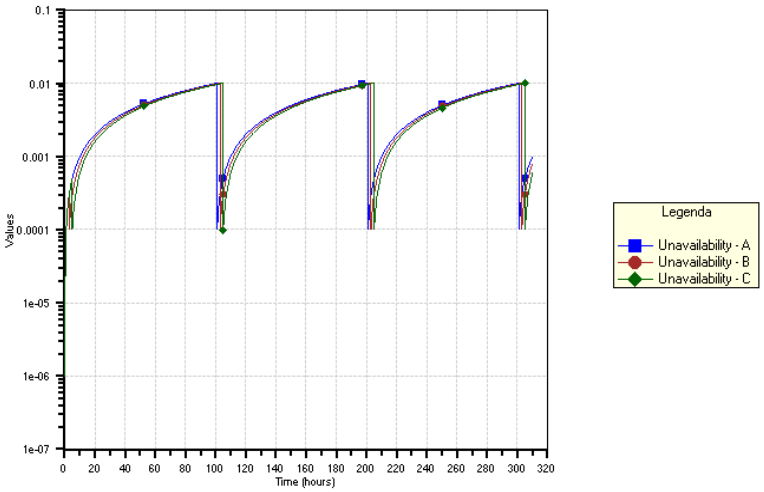


2. Sequential testing policy. Filename: **Tested-Sequential-2oo3**

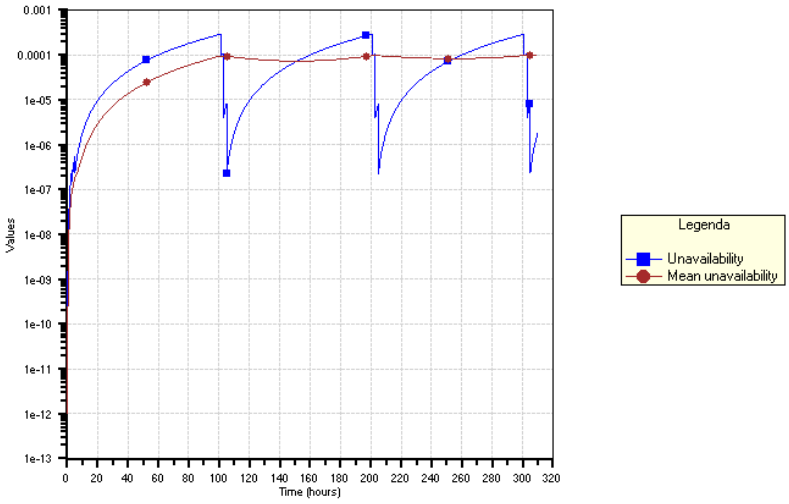
Components are tested one after the other. Only one component is put off line, tested and immediately put on-line before testing the next component. Suppose that each component is tested after 2 h from the initial testing of the previous one (θ_0 values). Under these hypotheses the data used are as follows:

x	**λ h^{-1}**	**τ h**	**θ h**	**θo h**
A	1.e-4	1	100	0.0
B	1.e-4	1	100	2
C	1.e-4	1	100	4

The plot of the unavailability of all components is shown in the following figure.



Concerning the system unavailability the mean value is equal to 9.481495 x 10^{-5}, which follows the behaviour displayed in the following figure. The maximum value of the unavailability is 2.89223 x 10^{-4}.

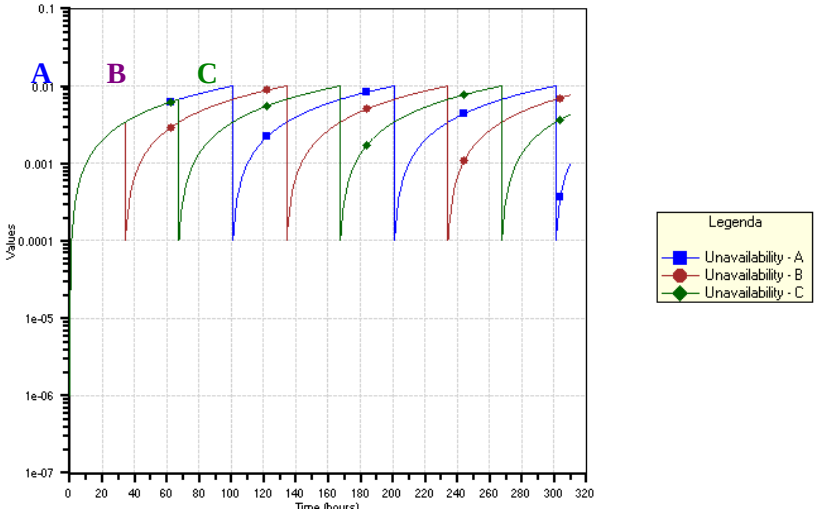


3. Staggered testing policy. Filename: **Tested-Staggered-2oo3**

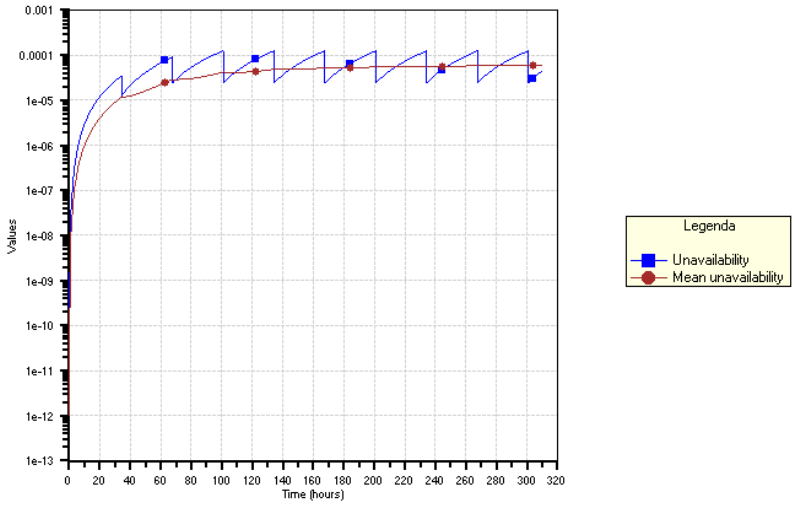
Components are tested one after the other at regular intervals of time. If θ is the test interval, then the first component is tested at t = 0 (first test at $\theta_0 = 0$), the second at t = θ / 3 (θ_0 = 33.33 h) and the third at t = 2θ /3 (θo = 66.66 h). In the hypothesis that the time to test duration is negligible, the data used are as follows:

x	λ	τ	θ	θ_0
A	1.e-4	1	100	0.0
B	1.e-4	1	100	33.33
C	1.e-4	1	100	66.66

The plot of the unavailability of the three components is as follows.



Concerning the system unavailability the mean value is equal to 5.9295 x 10^{-5}, which follows the behaviour displayed in the following figure, whereas the maximum value of the unavailability is equal to 1.25047 x 10^{-4}.



Comparing the three policies it can be noticed, as expected, that the best one is the symmetrical Staggered testing. Indeed the mean unavailability of a system under Staggered testing is about 2/3 of the unavailability under sequential testing.

The check of the correctness of results given by ASTRA has been performed by hand.

The following table summarises the results

Policy	Mean Unavailability	Max. unavailability
Simultaneous	9.85×10^{-5}	3.00×10^{-4}
Sequential	9.48×10^{-5}	2.89×10^{-4}
Staggered	5.93×10^{-5}	1.25×10^{-4}

Suggestions:

1) print the max value of Q instead of the value at the mission time if the fault tree contains at least a tested event;

2) add the test duration to the list of data of basic events and modify the equation for determining q(t).

3.2 IEC 61508 standard: Analysis of High Integrity Protection Systems (HIPS)

At the time the specifications of ASTRA were written, there was no idea to meet the requirements of the international standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems". However, during the ASTRA testing phase it was recognised the need to make ASTRA conform to the requirements of the standard by making some minor implementations. As a matter of fact the current version of the software is able to deal with such protection systems, but only in those particular cases in which the detection system is not present. In general, to correctly model the safety system failure the fault tree requires representing each basic event as the OR of two events. This is because the IEC standard considers the component failure rate λ_D (D stands for *dangerous*) as given by the Detected part (λ_{DD}) and the Undetected part (λ_{DU}). The first accounts for the failures that can be on-line detected and the second for those that can be detected only at test time intervals. In ASTRA the first type of failure is typical on the on-line maintained components and the second of tested / inspected components.

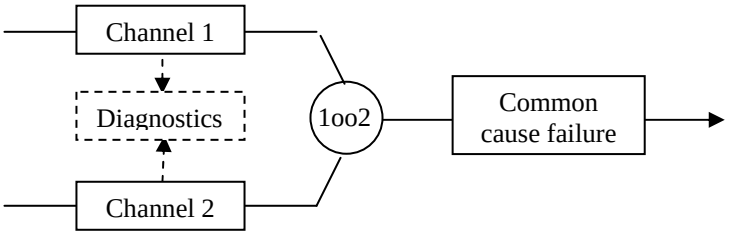
The examples given below intend to show on the one hand the practical possibility of the current ASTRA version to deal with the analysis of protective systems requiring the conformance to the standard, and on the other hand to show which new implementations should be performed to facilitate the system modelling.

3.2.1 Filename: IEC-1oo2

Source: IEC 61508-6, 2001 – Appendix B

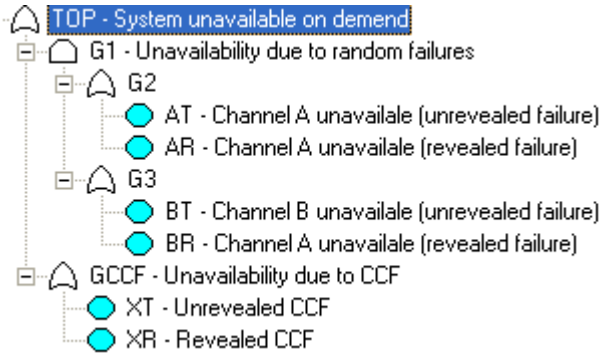
Problem Description:
Given a 1oo2 Protection System the aim is to determine the Probability of Failure on Demand (PFD) considering random failures and Common Cause Failures (CCF) as described in the IEC Standard.

In the considered example the Diagnostic System is able to detect a fraction DC (Diagnostic Coverage) of all failures of each channel. Channels are considered to be equal.
CCF analysis is performed considering the Beta factor model with β = 10% for the un-revealed faults and β_D = 5% for revealed faults.



In order to solve this simple problem, two extra data are to be added to the basic events' parameters and consequently the equation of tested events must be modified.

Taking into account the equations implemented in ASTRA 3.0, the problem can be modelled via fault tree as follows, where each component is represented by the OR of two events, one for modelling the un-revealed fault (tested event) and another for the revealed fault (on-line maintained event).



Data used.
$\lambda_{DD} = \lambda_{DU} = \lambda/2 = 2.5$ e-5
MTTR = 8 h
Time to test = 4380 h
DC = 0%; 60%; 90%; 99%
$\beta = 10\%$ and $\beta_D = 5\%$.
Time horizon: 23,000 h

The failure rate of events AT, BT, representing un-revealed faults, is respectively: $\lambda_T = \lambda_{DD}(1\text{-DC})$; whereas the failure rate for AR, BR, representing the revealed faults is $\lambda_R = \lambda_{DD}$ DC.

With the inclusion of the CCF analysis, the failure rates of events XT and XR are respectively:
– for un-revealed faults $\lambda_T = \lambda_{DD}(1\text{-DC})\ \beta$;
– for revealed faults $\lambda_R = \lambda_{DD}$ DC β.

For each basic event the data used are given in the following table.

AR	OM		2.475000E-05	8.000000E+00		
AT	T1		2.500000E-07	8.000000E+00		4.380000E+03
BR	OM		2.475000E-05	8.000000E+00		
BT	T1		2.500000E-07	8.000000E+00		4.380000E+03
XR	OM		1.123700E-06	8.000000E+00		
XT	T1		2.500000E-08	8.000000E+00		4.380000E+03

The results, for different DC values, are reported below in which the second column contains the values taken from the IEC standard.

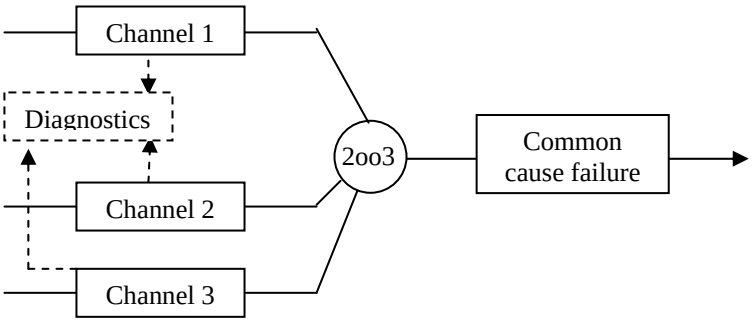
DC	**PFD according to IEC**	**ASTRA**
0%	8.8 e-3	8.79 e-3
60%	2.8 e-3	2.76 e-3
90%	6.0 e-4	5.79 e-4
99%	6.6 e -5	6.34 e-5

The differences between the Standard and ASTRA are due to the different degree of approximation of the equations used. The IEC Standard uses slightly approximated equations, whereas ASTRA uses exact equations. This explains the slightly lower values of the latter with respect to the former.

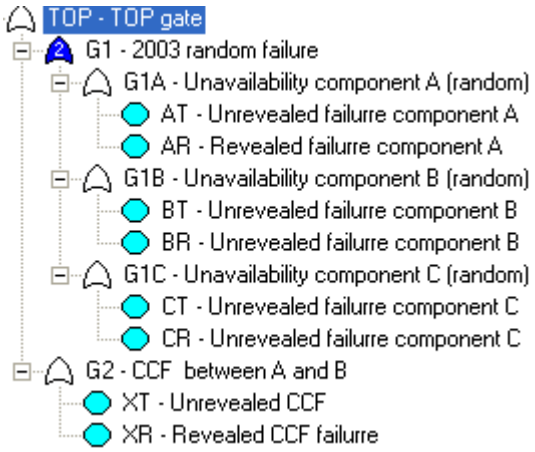
3.2.2 Filename: IEC+CCF

Source: IEC 61508-6, 2001 – Appendix B

Problem Description:
Given a Protection System configured as a 2oo3 systems (the signal from two channels are necessary for satisfying the working condition) the aim is to determine the Probability of Failure on Demand (PFD) considering both random failures and Common Cause Failures.



Taking into account the equations implemented in ASTRA 3.0, the problem can be modelled via fault tree as follows.



Data used.
$\lambda_{DD} = \lambda_{DU} = \lambda/2 = 2.5$ e-5
MTTR = 8 h
Time to test = 4380 h
DC = 0%; 60%; 90%; 99%
$\beta = 10\%$ and $\beta_D = 5\%$.
Time horizon: 23,000 h

The results are reported in the following table

DC	PFD according to IEC	ASTRA
0	1.5 e-2	1.49 e-2
60	3.9 e-3	3.87 e-3
90	6.8 e-4	6.57 e-4
99	6.7 e-5	6.38 e-5

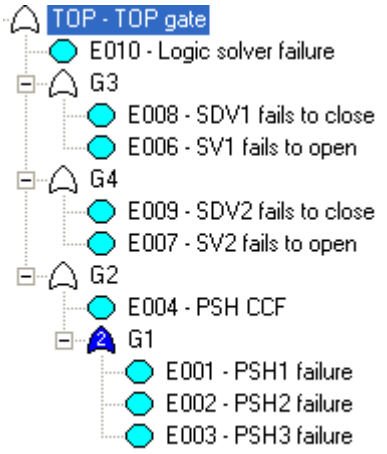
Also in this example each component is represented as the disjunction of two events, for dealing respectively with the unrevealed failures (tested event) and revealed failures (on-line monitored).

3.2.3 Filename: DRS

Source: Dutuit, Rauzy, Signoret, ESREL 2006, pag 1619

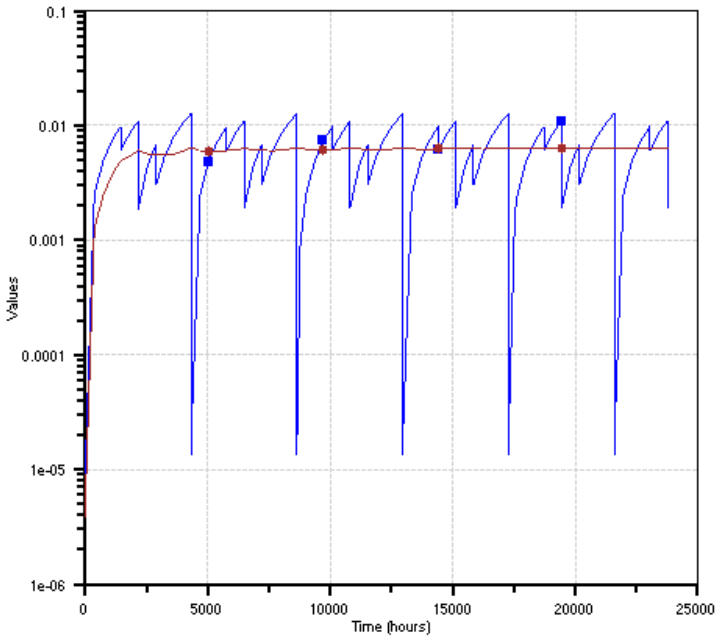
Problem Description:
Given a Protection System configured as a 2oo3 with a logic solver and two actuators the aim is to determine the Probability of Failure on Demand (PFD) considering both random failures and Common Cause Failures. In this case it is assumed that DC = 0%.

The fault tree and the basic events data are as follows:



Event Name	T	BC	Failure Rate	Repair Time	On-demand Unavailability	Test Interval	First Test Time
E001	T0		7.000000E-07			7.200000E+02	
E002	T0		7.000000E-07			7.200000E+02	1.000000E+00
E003	T0		7.000000E-07			7.200000E+02	2.000000E+00
E004	T0		3.500000E-08			7.200000E+02	7.200000E+02
E006	T0		1.300000E-06			1.440000E+03	
E007	T0		1.300000E-06			1.440000E+03	1.000000E+00
E008	T0		2.100000E-06			2.160000E+03	
E009	T0		2.100000E-06			2.160000E+03	1.000000E+00
E010	OM		1.000000E-06	1.000000E+01			

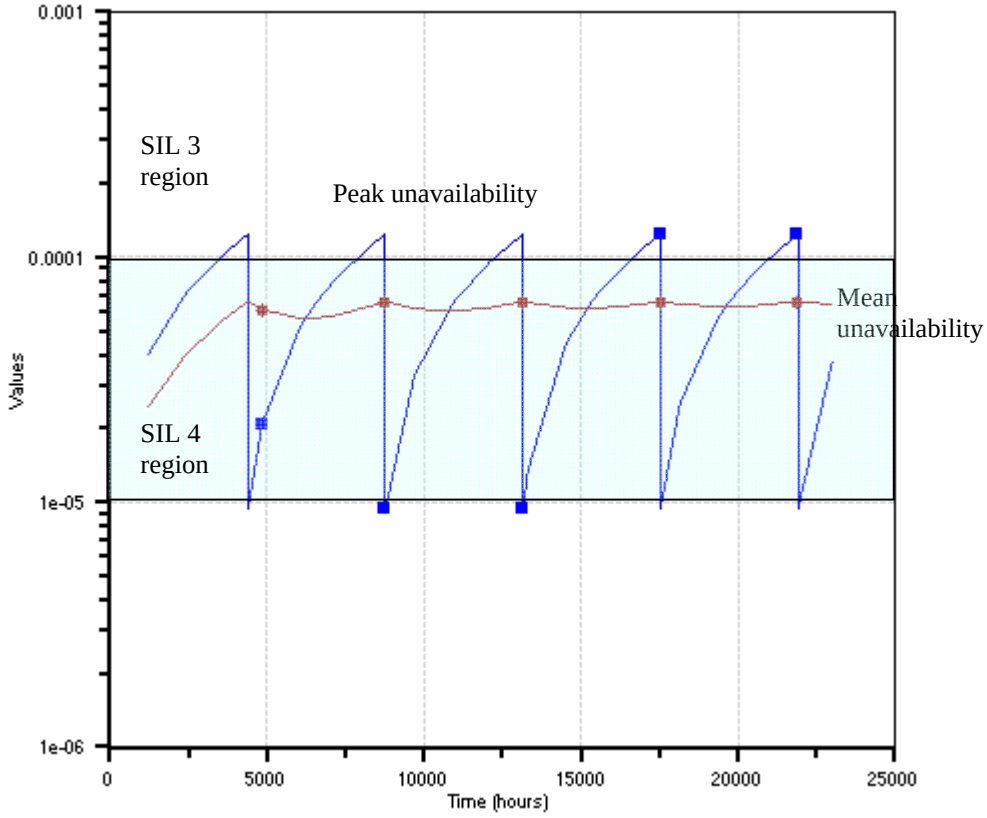
The authors of the paper determined the PFD using a mission time of 23,800 h. The PFD was calculated with different time intervals dt to show its the effect on the PFD value. With dt = 1 h they found, by means of Aralia, PFD = 6.374 x 10^{-3}, corresponding to a SIL 2 level.
The analysis of the fault tree with ASTRA gives the same result: PFD = 6.370 x 10^{-3}



As pointed out by Dutuit et al., the mean value of the PFD is not sufficient to state that the protective system presents a given SIL level. Indeed, the unavailability function has the classical saw-tooth behaviour with peaks that may enter in a lower SIL level region, as can be seen from the graph on the right.

Dutuit and al. calculated that for the present example the peak value of the unavailability on demand was greater that 10^{-2}, corresponding to SIL1, for about 12% of the mission time, corresponding to 2865 h, a figure that cannot be considered negligible.

Another example is shown in the following figure which is the plot given by ASTRA of the unavailability of the 2oo3 system with CCF and DC = 99%. In spite of the mean value Q = 6.38e-5 which positions the system at the SIL 4 level, the peak unavailability is greater than $10^{-4,}$ corresponding to a SIL 3 system. More precisely, the system will work as a SIL 3 for a certain period of time during which the plant safety is lower than expected.



From the above simple example it is evident that ASTRA can be correctly applied to analyse HIPS according to the standard IEC 61508. Even if it is possible to get the correct results by splitting events when DC > 0%, it is more convenient to implement what is needed to reduce the modelling effort.

Suggestion:

In order to represent each component failure mode with a single event it is necessary to:

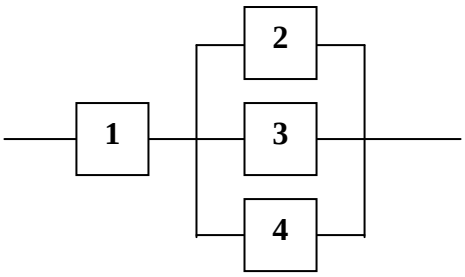
- *Add the field DC among the basic events' parameters;*
- *Determine the Maximum value of Q and possibly the time spent in each SIL level.*
- *Evaluate the need to associate the Beta factor to a set of selected events (CCF analysis).*

3.3. Importance analysis

3.3.1 Filename: Importance1

Source: Modarres book, page 361

Problem description:
Determine the Birnbaum importance of each component at 720 hours.



Components failure data

Event Name	Failure Rate
1	1.0E-05
2	1.0E-04
3	1.0E-04
4	1.0E-04

In Modarres the importance indexes are calculated with reference to the reliability. However, the book contains a typing mistake; it is easy to verify that the reliability values calculated for each of the three components correspond to a failure rate of 10^{-3} and not 10^{-4} as reported.
System Reliability at 720 h: 0.859, corresponding to F = 1 – R = 0.141.
Birnbaum importance values calculated at 720 h:

$$I_1^B(t = 720) = 0.865$$
$$I_2^B(t = 720) = 0.26$$
$$I_3^B(t = 720) = I_4^B(t = 720) = 0.26$$

Results from ASTRA
In order to compare the above figures with the results given by ASTRA, the correct failure rate (10^{-3}) is considered.
Unavailability: 0.1414 Number of MCS: 2

Birnbaum Importance values

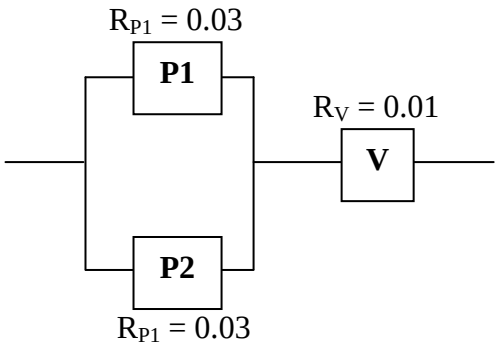
Event Name	Importance Contribution
1	0.86479
2	0.26153
3	0.26153
4	0.26153

Conclusion: The result obtained with ASTRA perfectly agrees with those from the referred source.

3.3.2 Filename: Importance2

Source: Modarres example 6.6, page 365 and 6.7 page 367

Problem description:
Determine the Birnbaum, Criticality, Risk Achievement Worth (RAW), Risk Reduction Worth (RRW) and Fussell-Vesely importance of the components in the following system.



Results from Modarres

System Reliability: 0.989 corresponding to the unreliability of F = 1.1 E-2

Importance of components.

Component	Birnbaum	Criticality	RAW	RRW	F-V
V	1	1	90.91	12.2	0.9
P1	0.03	0.029	3.64	1.1	0.08
P2	0.03	0.029	3.64	1.1	0.08

Results from ASTRA.

System Unreliability: F = 1.0891E-02

Importance of components.

Component	Birnbaum	Criticality	RAW	RRW	F-V
V	0.9991	0.917	91.81	12.10	--
P1	0.0297	0.0818	3.645	1.089	--
P2	0.0297	0.0818	3.645	1.089	--

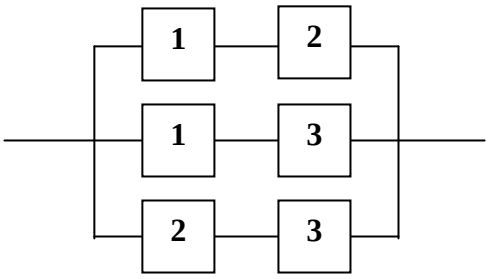
The current version of ASTRA does not calculate the F-V measure, since in practice the F-V measure is very close to the Criticality measure.

All results are slightly different. Apart from the Criticality values for both pumps, the reason for the difference relies on the different precision of the equations used. The exact equations, manually applied for the calculation of the Criticality of P1 and P2, gives the same results of ASTRA, i.e. the Criticality indexes in the reference source are approximated.

3.3.3 Filename: Importance3

Rausand book page 134

Problem description:
determine the structural importance for the 2/3 system.



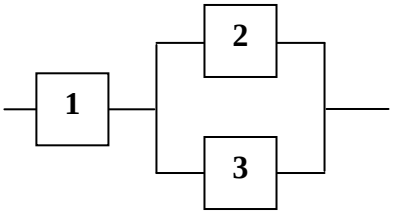
Results from Rausand: IS = 0.5 for all components.

Conclusion: ASTRA results: same values.

3.3.4 Filename: Importance4

Rausand book page 134

Problem description:
determine the structural importance for a series-parallel system.



Results from Rausand:
- Component 1: IS = 3/4
- Component 2: IS = 1/4
- Component 3: IS = 1/4

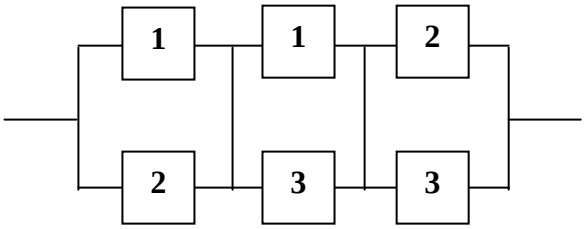
ASTRA results: same values.

Conclusion: The results obtained with ASTRA perfectly agree with those from the referenced source.

3.3.5 Filename: Importance5

Source: Henley-Kumamoto (first edition), page 434 + Table 10.3.

Problem description:
Determine Unavailability, Birnbaum and Criticality importance indexes for a majority voting system (2/3). Mission time: 20 h



Components Data

Comp. Name	Failure Rate	Repair Time
1	1.0E-03	10
2	2.0E-03	40
3	3.0E-03	60

Results from H-K:

Component1: IB = 7.89e-2 IC = 0.305
Component2: IB = 5.77e-2 IC = 0.803
Component3: IB = 3.92e-2 IC = 0.875

Results from ASTRA

Event Name	Birnbaum	Criticality
1	7.744733E-02	3.025462E-01
2	5.734178E-02	8.062145E-01
3	3.896427E-02	8.792604E-01

The calculation with Matlab of the Birnbaum index gave results that agreed with those of ASTRA, i.e.:
Component1: IB = 7.74e-2
Component2: IB = 5.73e-2
Component3: IB = 3.90e-2

Conclusion: The results supplied by ASTRA are correct.

3.3.6 Filename: Importance6

Source: Kumamoto-Henley (first edition), page 422 + Table 10.2.

Problem description:
Determine Unavailability, Birnbaum and Criticality importance indexes for a majority voting system (2oo3) made up of not repairable components. Mission time: 20 h

Test: Unavailability, Birnbaum and Criticality importance indexes.

Components Data

Comp. Name	**Failure Rate**
1	1.000000E-03
2	2.000000E-03
3	3.000000E-03

Results from H-K

Unavailability: Q_S = 4.12258e-3

Component1: IB = 9.2879e-2 IC = 0.811666
Component2: IB = 7.5730e-2 IC = 0.72028
Component3: IB = 5.7459e-2 IC = 0.446111

Results from ASTRA

Unavailability: Q_S = 4.122576e-3

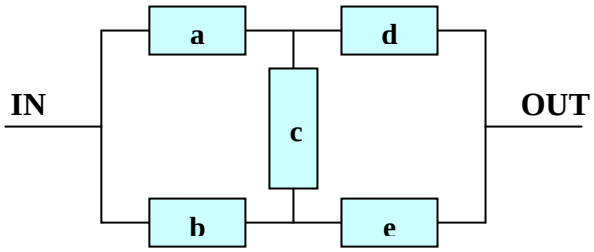
Event Name	**Birnbaum**	**Criticality**
1	9.287914E-02	8.116660E-01
2	7.573052E-02	7.202866E-01
3	5.745905E-02	4.461119E-01

Conclusion. The result obtained with ASTRA perfectly agrees with those from the referred source.

3.3.7 Filename: Importance7

Source: Dutuit - Rauzy, (2001).

Problem description:
Determine Unavailability, Birnbaum, Criticality, RAW and RRW for the reliability Block Diagram (RBD) reported below (bridge system).



P(a) = 0.1
P(b) = 0.2
P(c) = 0.3
P(d) = 0.4
P(d) = 0.5

Results from the source are as follows.

Comp.	MIF	Criticality	RAW	RRW
a	0.22	0.0940171	1.84615	1.10377
b	0.125	0.106838	1.42735	1.11962
c	0.06	0.0769231	1.17949	1.08333
d	0.505	0.863248	2.29487	7.3125
e	0.3848	0.822222	1.82222	5.625

Since the system is coherent, MIF is the Birnbaum importance index.

The analysis with ASTRA required the transformation of the RBD into a fault tree and then the analysis of the resulting fault tree. Results are as follows: Unavailability Qs = 0.234. Number MCS = 4.
Importance analysis:

Comp.	MIF	Criticality	RAW	RRW
a	0.22	0.0940171	1.846154	1.103774
b	0.125	0.1068376	1.427350	1.119617
c	0.06	0.0769231	1.179487	1.083333
d	0.505	0.8632479	2.294872	7.31250
e	0.3848	0.8222222	1.822222	5.6250

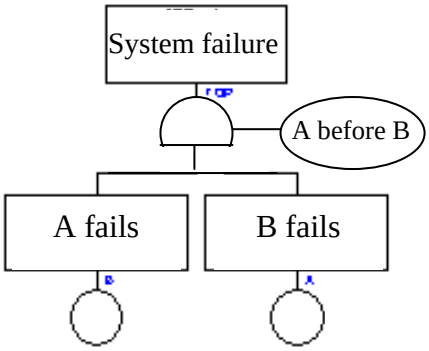
Conclusion. The result obtained with ASTRA perfectly agrees with those from the referred source.

3.4. Modelling catastrophic Top-events using the extended INH gate

3.4.1 Filename: INH1

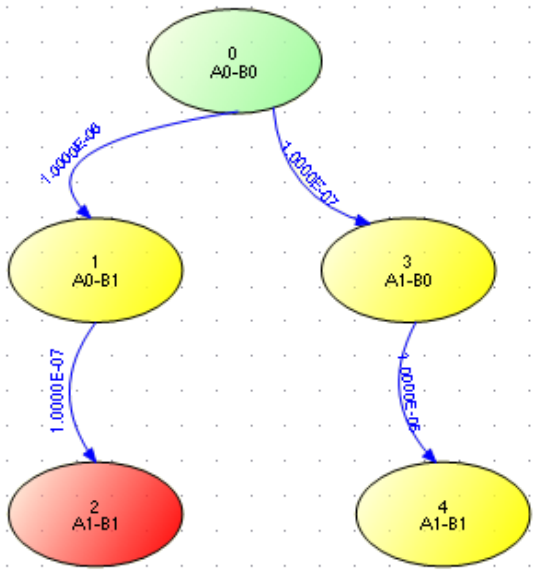
Source: Ericson, page 330.

Problem description:
A system is comprised of two components: A monitors the operation of the component B. System failure occurs if both fail, but only if A fails before B.



Component A: λ_A = 1.e-6 μ_A = 0
Component B: λ_B = 1.e-7 μ_B = 0

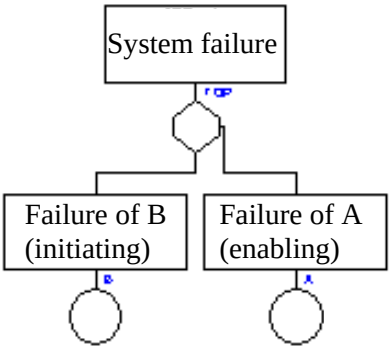
This problem can be solved using the Markov approach.. The state diagram is as follows.



Markov state diagram (from the XS-MKA Software)

ASTRA allows solving this problem by modelling it by means of an extended implementation of the INH gate.
In ASTRA the initiating and enabling events can also be complex events (sub-trees) not necessarily independent. Common event are treated as initiators.
Initiator events cause perturbations of process variables; enabling events are associated with the failure on demand of protective systems. An accident occurs if at the time of occurrence of the initiating event (plant perturbation) the enabling event (protective system) has already occurred (failed) or it occurs at the time it is called to intervene.

The modelling of the above system by means of the fault tree technique is as follows.



ASTRA representation

The following table shows the comparison of the unavailability values Qs(t) (which is equal to the unreliability F(t) since components are not repairable) obtained using the Markovian approach with those calculated by ASTRA, in which the problem is modelled using the (extended) INH gate.

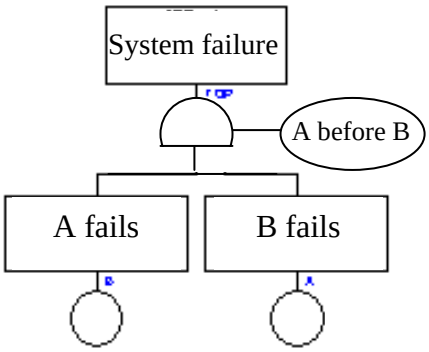
Mission time (h)	**Markov Q(t)**	**ASTRA Q(t)**
100	4.99980E-10	4.99979E-10
1,000	4.99800E-8	4.99794E-8
10,000	4.98006E-6	4.97943E-6
100,000	4.80542E-4	4.79950E-4
1,000,000	3.45145E-2	3.41377E-2
10,000,000	5.41213E-1	4.93338E-1

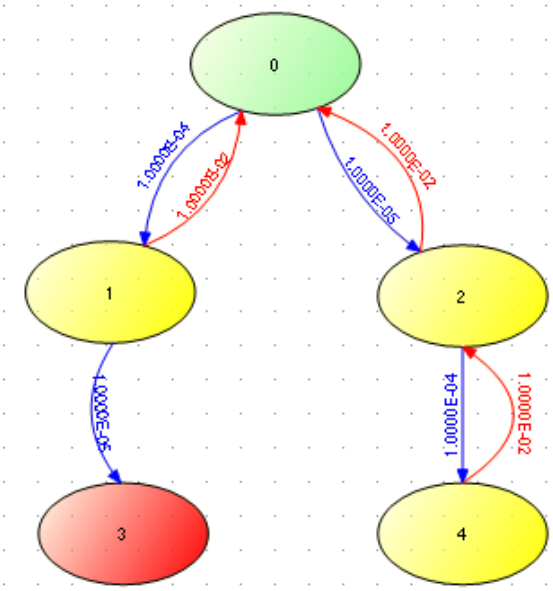
Conclusion: The agreement is very good for all values of practical interest.

3.4.2 Filename: INH2

Source: Ericson, page 330.

Problem description:
A system is comprised of two components: A monitors the operation of the component B. System failure occurs if both fail, but only if A fails before B. The aim is to determine the probability of system failure F(t) for different mission times.



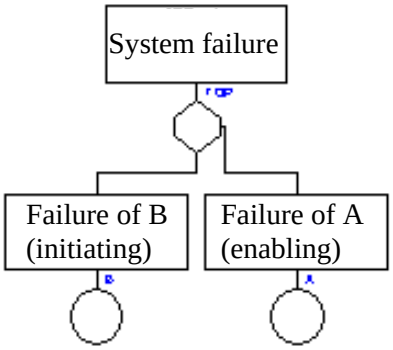


Markov state diagram for the system with sequential failures

Component A: λ_A = 1.e-4 μ_A = 0.01
Component B: λ_B = 1.e-5 μ_B = 0.01

The following table shows the comparison of the unreliability values Fs(t) obtained using the markovian approach (software XS-MKA) and the fault tree technique (ASTRA).

Mission time (h)	**Markov** F(t)	**ASTRA** F(t)
1,000	8.90125 e-5	8.91150 e-5
10,000	9.77870 e-4	9.78822 e-4
100,000	9.82286 e-3	9.83254 e-3
1,000,000	9.40554 e-2	9.41647 e-2
10,000,000	0.62693	0.62805



System model using the extended INH gate of ASTRA.

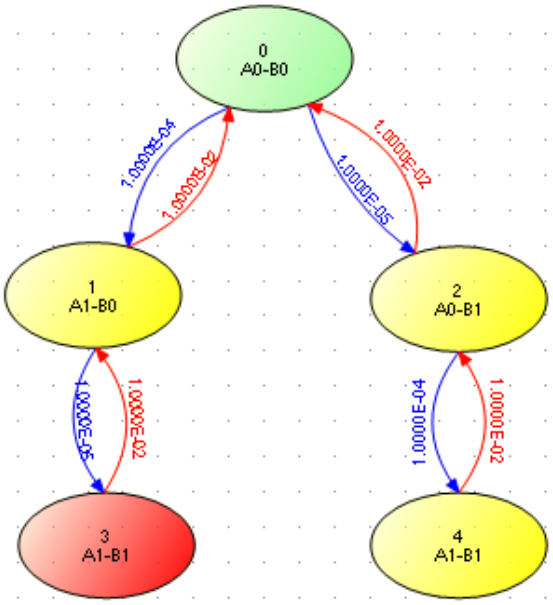
Conclusion: The agreement between Markov and ASTRA is very good for all values.

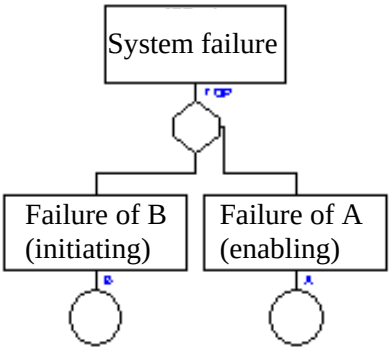
3.4.3 Filename: INH2-rep

Source: ASTRA Development team.

Problem description:
A system is comprised of two components: A monitors the operation of the component B. System failure occurs if both fail, but only if A fails before B. The aim is to determine all parameters for three different mission times.

The Markov state diagram is as follows.





	MKA T = 10^3	ASTRA T = 10^3
F	8.90125 e-5	8.91150 e-5
Q	9.8855 e-6	9.89024 e-6
W	8.91148 e-5	8.91220 e-5

MKA =10^5	ASTRA T=10^5
9.82286 e-3	9.83254 e-3
9.89100 e-6	9.89101 e-6
9.88120 e-3	9.88130 e-3

MKA T=10^7	ASTRA T=10^7
0.62693	0.62805
9.89100 e-6	9.89101 e-6
0.9890903	0.9890987

	MKA	ASTRA
MTBF	1.011020 e+7	1.011010 e+7
MTTR	100	100
MTTF	1.010010 e+7	1.011000 e+7

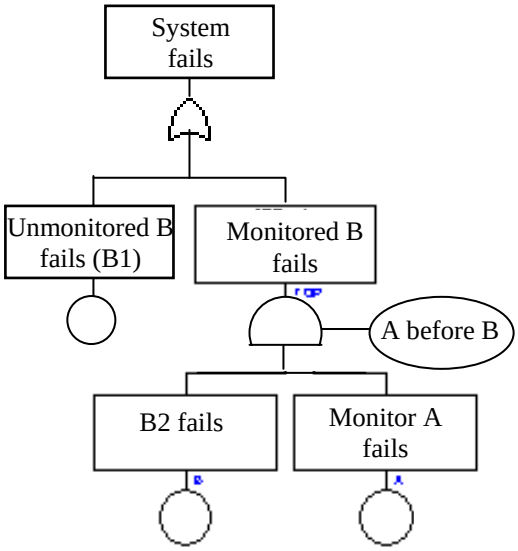
Conclusion: The comparison of the results given by ASTRA with those obtained from XS-MKA show a very good agreement.

Suggestion: *Remove the calculation of V(t) due to the low relevance.*

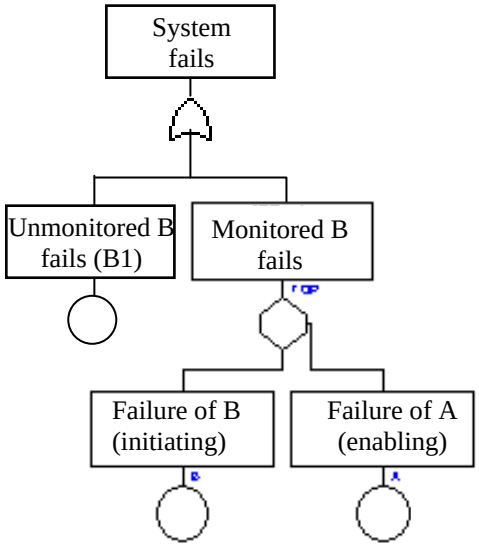
3.4.4 Filename: INH3

Source: Ericson, page 331

Problem description:
A system is comprised of two components: A monitors the operation of the component B. However, A can monitor only 80% of B. If it detects any failure in B, it takes corrective action. System success requires that B must operate successfully. System failure occurs if B fails, which can only happen if A fails to detect a problem with the monitored portion of B, or if the unmonitored portion of B fails.



Fault tree of the reference source



ASTRA representation

Component A: λ_A = 1.e-4 μ_A = 0
Component B1: λ_B = 1.e-5 μ_B = 0
Component B2: λ_B = 1.e-5 μ_B = 0

The following table shows the comparison of the unreliability values Fs(t) obtained using the markovian approach with those calculated by ASTRA, in which the problem is modelled using the (extended) INH gate.

Mission time (h)	**Markov**	**ASTRA**
100	0.0001	0.0001
1,000	0.010314	0.0103010
10,000	0.103269	0.103186
100,000	0.666795	0.666151
1,000,000	0.999982	0.999983

Conclusion: The agreement between Markov and ASTRA is very good for all values.

3.4.5 Filename: OR-two-INH

Source: ASTRA development team

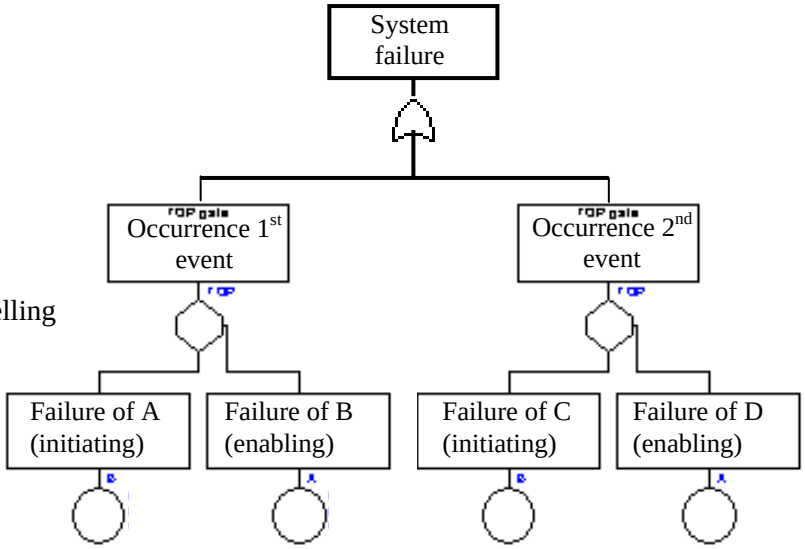
Problem Description:

Two process variables A and C are monitored respectively by two other components B and D. The two INH gates are connected through a logical OR gate, meaning that the output catastrophic event occurs if at least one event occurs.

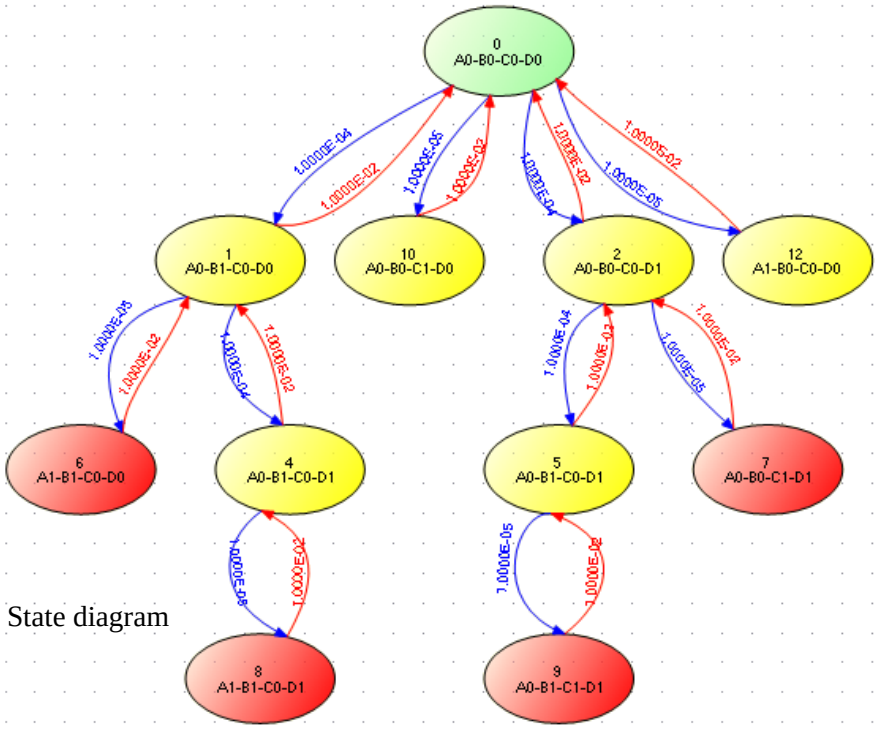
The following figures show respectively the fault tree modelling by means of two INH gates and the Markov state diagram representation.

The aim is to determine the system failure probability (unreliability) for different mission times.

ASTRA modelling



XS-MKA Markovian State diagram



The comparison between the results obtained with XS-MKA and ASTRA are given in the following table. The very high mission times are considered for comparison purposes.

Mission time (h)	**XS-MKA F(t)**	**ASTRA F(t)**
1000	1.77652 e-4	1.78229 e-4
10,000	1.95254 e-3	1.95674 e-3
100,000	1.95271 e-2	1.95687 e-2
1,000,000	0.17896	0.17946
10,000,000	0.85929	0.86168

From the table it is possible to see that the agreement is very good for all mission times.

Problem description

Same as before, but considering the restoration of the initiating event with μ=0.01 (for each failure state the transition is to the closest state, e.g. from state 6 to state 1, from 8 to 4).
Results are shown for three mission times.

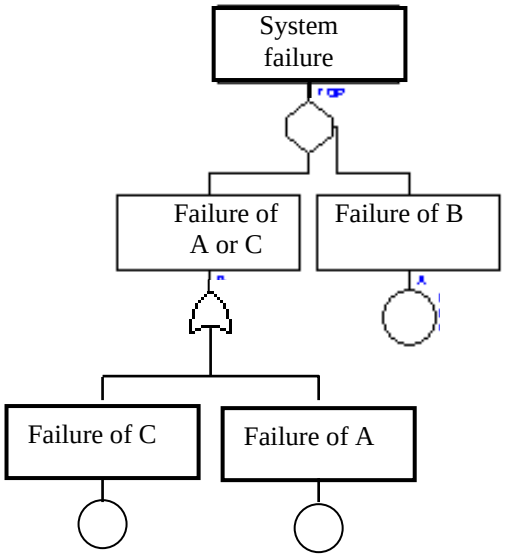
	XS-MKA $T = 10^3$	**ASTRA** $T = 10^3$
F	1.77652 e-4	1.78230 e-4
Q	1.97480 e-5	1.97821 e-5
W	1.77869 e-4	1.78242 e-4

XS-MKA $T=10^5$	**ASTRA** $T=10^5$		**XS-MKA** $T=10^7$	**ASTRA** $T=10^7$
1.95271 e-2	1.95688 e-2		0.859295	0.861684
1.97609 e-5	1.97821 e-5		1.97609 e-5	1.97821 e-5
1.97411 e-2	1.97624 e-2		1.97607	1.97817

	XS-MKA	**ASTRA**
MTBF	5.060496 e+6	5.055100 e+6
MTTR	100	100
MTTF	5.065355 e+6	5.055000 e+6

Conclusion: The comparison of the results given by ASTRA with those obtained from XS-MKA show very good agreement.

Note that if the enabling branch of the two INH gates is the same event / sub-tree, i.e. B = D, then the above fault tree is equivalent to the following one:


System failure
Failure of A or C
Failure of B
Failure of C
Failure of A

3.4.6 Filename: AND-two-INH

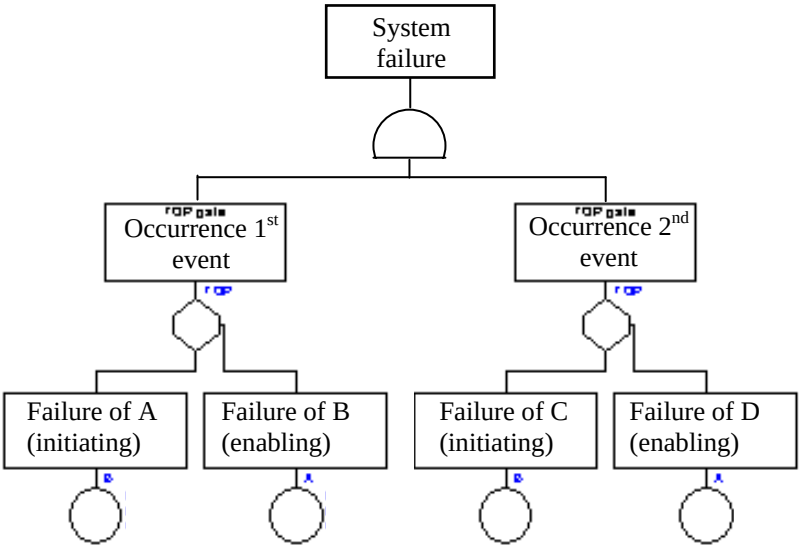
Source: ASTRA development team

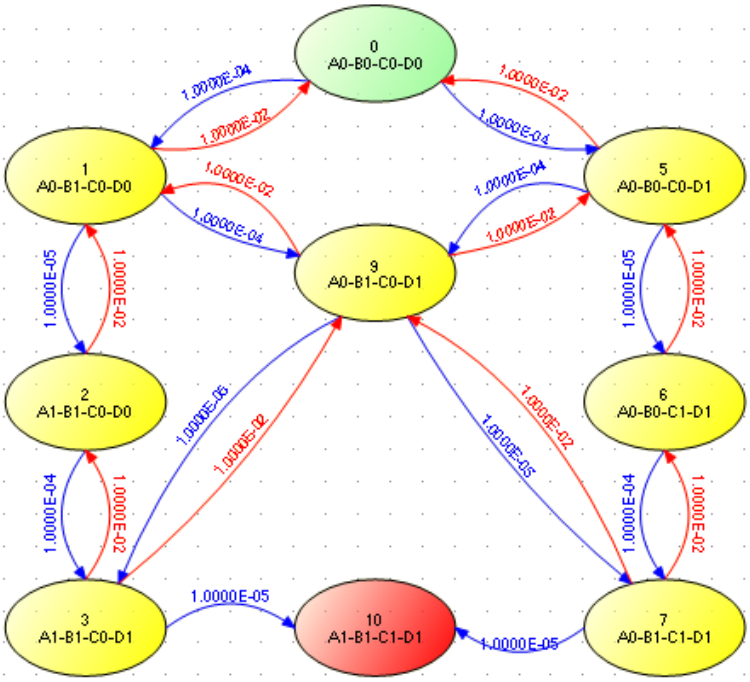
Problem Description:

Two process variables A and C are monitored respectively by two other components B and D. The two INH gates are connected with a logical AND, meaning that the output event occurs if both events occur.

The following figures show respectively the fault tree modelling by means of two INH gates and the Markov state diagram representation.

ASTRA modelling





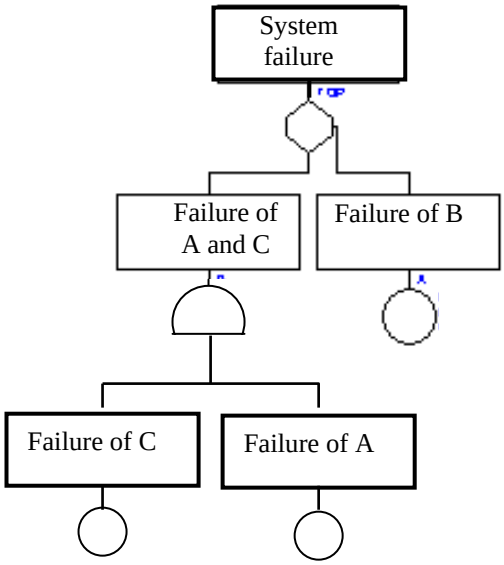
XS-MKA
Markovian State diagram

The comparison between the results obtained with XS-MKA and ASTRA are given in the following table. The very high mission times are considered to compare the two different modelling.

Mission time (h)	Markov F(t)	ASTRA F(t)
1000	1.51583 e-9	1.60048 e-9
10,000	1.91516 e-8	1.92105 e-8
100,000	1.95512 e-7	1.95311 e-7
1,000,000	1.95912 e-6	1.95632 e-6
10,000,000	1.95950 e-5	1.95662 e-5
100,000,000	1.95937 e-4	1.95647 e-4

Conclusion: From the table it is possible to see that the agreement is very good for all mission times.

Note that if the enabling branch of the two INH gates is the same event / sub-tree, i.e. B = D, then the above fault tree is equivalent to the following one:



3.5 Test on Exclusive OR (XOR)

The use of the XOR logical operator is allowed in ASTRA, but no referenced examples have been found in literatures for testing purposes. Hence XS-MKA has been considered as a reference code.

3.5.1 Filename: XOR1

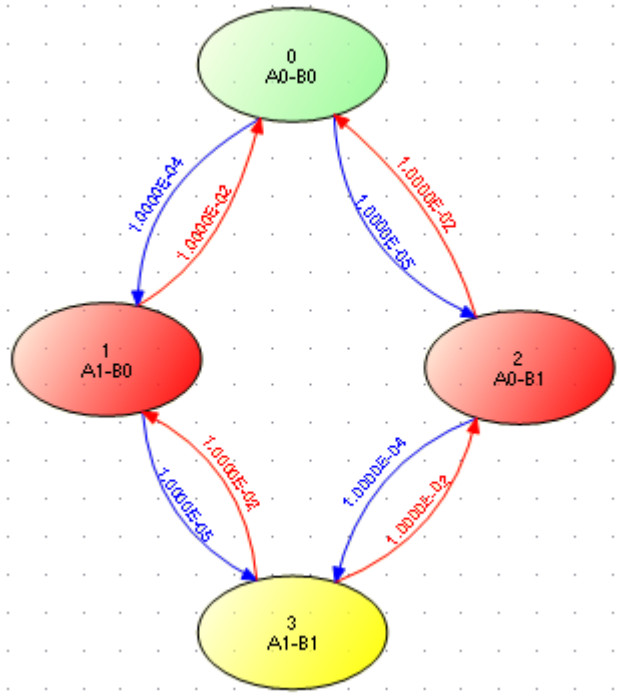
Source: JRC ASTRA development team.

Problem description:
Determine the Unavailability of Top = A ⊕ B. Components are assumed to be characterised by the following values:
λ_A = 1.0e-4; μ_A =1.0e-2
λ_B = 1.0e-5; μ_B =1.0e-2
The determination of all parameters at system level is requested.

The exclusive OR of two variables is defined as

$XOR(A,B) = A \oplus B = A\ \bar{B} + \bar{A}\ B,$

i.e. if one variable is true the other is false and vice versa. Since XOR(A,B) is a Boolean expression, variables A and B are independent.
The Markov graph is hereinafter represented.



Results from XS-MKA and ASTRA are shown for three mission times.

	XS-MKA $T = 10^2$	ASTRA $T = 10^2$
F	1.09341e-2	1.09430e-2
Q	6.95487e-3	6.91876e-3
W	1.09583e-2	1.09589e-2
V	4.10301e-3	4.04012e-3

XS-MKA $T = 10^3$	ASTRA $T=10^3$		XS-MKA $T=10^4$	ASTRA $T=10^4$
0.104076	0.104310		0.66052	0.66778
1.08798e-2	1.08798e-2		1.08802e-2	1.08802e-2
0.109088	0.109091		1.090087	1.09008
9.83056e-2	9.82074e-2		1.07930	1.07920

The characteristic times have been obtained with MKA by running the code with the Steady State (SS) analysis option, whereas with ASTRA the mission time of 10,000 h has been used.

	XS-MKA (SS)	**ASTRA** ($T=10^4$)
MTBF	9.1743e+3	9.1743e+3
MTTR	99.819	99.818
MTTF	9.0900e+3	9.07450e+3
Λ	1.10198e-4	1.10198e-4
M	1.00181e-2	1.00181e-2

Conclusion: The agreement is quite good.

3.5.2 Filename: XOR3

Source: JRC ASTRA development team.

Problem description:
Determine the Unavailability of Top = A ⊕ B ⊕ C. Components are assumed to be characterised by the following values:
λ_A = 1.0e-4; μ_A =1.0e-2
λ_B = 2.0e-4; μ_B =1.0e-2
λ_C = 3.0e-4; μ_C =1.0e-2

The determination of all parameters at system level is requested.

As described before the calculation is performed by ASTRA on the reduced XOR function.

Results from XS-MKA and ASTRA are shown for three mission times.

	XS-MKA $T = 10^2$	**ASTRA** $T = 10^2$
F	5.76318e-2	5.85759e-2
Q	3.67007e-2	3.67013e-2
W	5.90577e-2	5.90575e-2
V	2.23552e-2	2.23487e-2

XS-MKA $T =10^3$	**ASTRA** $T=10^3$		**XS-MKA** $T=10^4$	**ASTRA** $T=10^4$
0.443373	0.461060		0.979564	0.99799
5.65430e-2	5.65428e-2		5.65450e-2	5.65447e-2
0.586502	0.586495		5.862160	5.862167
0.529948	0.529876		5.805604	5.804789

The characteristic times have been obtained with MKA by running the code with the Steady State (SS) analysis option, whereas with ASTRA the mission time of 10,000 h has been used.

	XS-MKA (SS)	**ASTRA** ($T=10^4$)
MTBF	1.70594e+3	1.70595e+3
MTTR	96.46799	96.46302
MTTF	1.66666e+3	1.60949e+3
Λ	6.21316e-4	6.21328e-4
M	1.03666e-2	1.03667e-2

Conclusion: The agreement is quite good.

3.6 Coherent Fault Tree analysis

3.6.1 Filename: AFS

Source: Modarres book, page 320.

Problem description:
Determine the Unavailability and the Minimal Cut Sets (MCS) of a Simplified Auxiliary Feed water System of a PWR. Assume that the system is in stand-by mode and all of the components are periodically tested. The following data characterise the components:

Block name	Failure Rate	Average Repair Time	Average test duration	Test Interval	First Time to Test
A	1.000000E-07	5.000000E+00	0	7.200000E+02	
B	1.000000E-07	5.000000E+00	0	7.200000E+02	
C	1.000000E-06	1.000000E+01	0	7.200000E+02	
D	1.000000E-06	1.000000E+01	0	7.200000E+02	
E	1.000000E-06	1.000000E+01	0	7.200000E+02	
F	1.000000E-06	1.000000E+01	0	7.200000E+02	
H	1.000000E-07	2.400000E+01	0	7.200000E+02	
I	1.000000E-04	3.800000E+01	0	7.200000E+02	
J	1.000000E-04	3.800000E+01	2	7.200000E+02	
K	1.000000E-05	2.600000E+01	2	7.200000E+02	
L	1.000000E-07	1.000000E+01	2	7.200000E+02	
M	1.000000E-04	1.000000E+01	0	7.200000E+02	
MG1	1.000000E-07	1.500000E+01	0	7.200000E+02	
N	1.000000E-07	5.000000E+00	0	7.200000E+02	

Since the Test interval is the same for all components the test policy is “simultaneous testing”.
In the reference source the system is described by means of a Reliability Block Diagram.

Results from Modarres.
Mean unavailability (rare event approximation): $Q_S = 7.49\,x10^{-5}$; $Number\,of\ MCS : 26$

Analysis with ASTRA

The RBD has been transformed into the equivalent fault tree (Filename: AFS)

Basic events are all tested at 720 h. This produces discontinuities on the system unavailability function at 720 h and its multiple values.

Looking at the different data on components, it can be realised that the model used by ASTRA for determining the unavailability of tested component is different from the one used in the reference case. Indeed, ASTRA considers the time to perform the test as negligible, whereas in the reference case there are three components i.e. J, K, L with a test time of 2 h. The corresponding unavailability is $q_{test} = \frac{2}{720} = 2.7x10^{-3}$, which is about 1/10 of the of unavailability between tests.

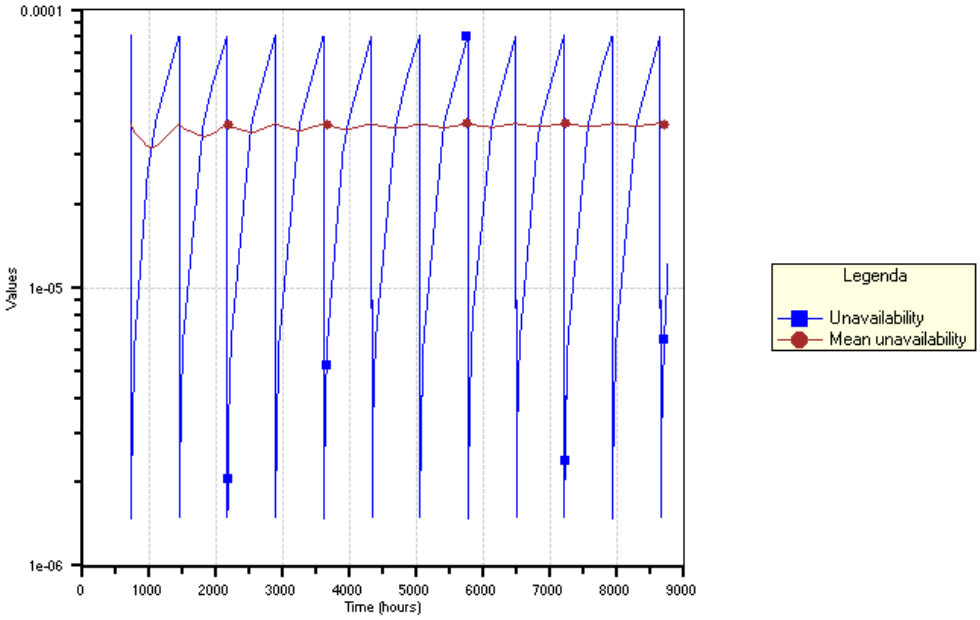
The input fault tree and the parameters of basic events are shown below.

Gate Name	Op.	Sons	
TOP	OR	N	G1
G1	AND	G11	G12
G11	OR	L	G2
G12	OR	M	G3
G2	AND	G21	G22
G3	OR	H	G7
G21	OR	MG1	G4
G22	OR	K	G3
G7	AND	G71	G72
G4	AND	G41	G42
G71	OR	A	D
G72	OR	F	B
G41	OR	I	G5
G42	OR	J	G5
G5	OR	MG1	G6
G6	AND	G61	G62
G61	OR	C	A
G62	OR	E	B

Primary Events Input Data

Event Name	Failure Rate	Repair Time	On-demand Unavailability	Test Interval	First Test Time
A	1.000000E-07	5.000000E+00		7.200000E+02	
B	1.000000E-07	5.000000E+00		7.200000E+02	
C	1.000000E-06	1.000000E+01		7.200000E+02	
D	1.000000E-06	1.000000E+01		7.200000E+02	
E	1.000000E-06	1.000000E+01		7.200000E+02	
F	1.000000E-06	1.000000E+01		7.200000E+02	
H	1.000000E-07	2.400000E+01		7.200000E+02	
I	1.000000E-04	3.800000E+01		7.200000E+02	
J	1.000000E-04	6.400000E+01		7.200000E+02	
K	1.000000E-05	5.200000E+01		7.200000E+02	
L	1.000000E-07	3.800000E+01		7.200000E+02	
M	1.000000E-04	1.000000E+01		7.200000E+02	
MG1	1.000000E-07	1.500000E+01		7.200000E+02	
N	1.000000E-07	5.000000E+00		7.200000E+02	

The plot of the point wise unavailability and the mean unavailability determined by ASTRA is represented in the following figure.



The mean value of the unavailability is Qs = 3.87 x 10^{-5}. The number of MCS is 26.

The reason why the mean unavailability calculated with ASTRA is different from that of the reference case cannot be due to the different model used for determining the unavailability of the tested components; rather the Modarres value is the maximum Top-event unavailability valuew, not the mean one!

Below is the list of the 26 MCS obtained by ASTRA.

The list of MCS sorted by importance is represented in the following table.

#	Value	Importance	Order	Minimal Cut Set		
1	1.199993E-05	9.878587E-01	1	N		
2	1.431386E-07	1.178346E-02	2	L	M	
3	2.035424E-09	1.675603E-04	4	I M	J	K
4	1.707398E-09	1.405565E-04	3	H	I	J
5	1.716633E-10	1.413167E-05	3	K	M	MG1
6	1.439983E-10	1.185423E-05	2	H	MG1	
7	1.439983E-10	1.185423E-05	2	H	L	
8	1.439983E-10	1.185423E-05	2	A	B	
9	2.048644E-12	1.686486E-07	4	D J	F	I
10	2.059724E-13	1.695607E-08	4	C M	E	K
11	2.048755E-13	1.686577E-08	4	A J	F	I
12	2.048755E-13	1.686577E-08	4	B J	D	I
13	1.727782E-13	1.422346E-08	3	B	C	D
14	1.727782E-13	1.422346E-08	3	C	E	H
15	1.727782E-13	1.422346E-08	3	D	F	L
16	1.727782E-13	1.422346E-08	3	A	E	F
17	1.727782E-13	1.422346E-08	3	D	F	MG1

#	Value	Importance	Order	Minimal Cut Set		
18	2.059836E-14	1.695699E-09	4	B M	C	K
19	2.059836E-14	1.695699E-09	4	A M	E	K
20	1.727876E-14	1.422423E-09	3	A	E	H
21	1.727876E-14	1.422423E-09	3	B	C	H
22	1.727876E-14	1.422423E-09	3	B	D	MG1
23	1.727876E-14	1.422423E-09	3	B	D	L
24	1.727876E-14	1.422423E-09	3	A	F	MG1
25	1.727876E-14	1.422423E-09	3	A	F	L
26	2.073102E-16	1.706620E-11	4	C F	D	E

The results given by ASTRA are equal to those of the reference source.

***Suggestion**: In future implementations the test duration should be introduced.*

3.6.2 Filename: Chemical-Reactor

Source: Kumamoto-Henley (first edition), page 524 + Table 10.3. Fault tree in Fig.13.6

Problem description:
Analysis of a simplified chemical reactor for the top event: runaway reaction. Mission time = 100h

Fault tree description

Gate Name	Op.	Sons			Description
TOP	AND	GTEMP	GEXC		Runaway
GTEMP	OR	GFICV	GCOOL		Temp. Excursion towards 300
GEXC	OR	GSV1	FICV	BY1HE	Excursion not arrested
GFICV	OR	GWRONGS	BY1HE	FICV	FICV-702 opens or sticks open
GCOOL	OR	GPRESS	WATER	HEAT	Loss of cooling to reactor
GSV1	OR	GCIRC	SV1		SV-1 fails to open
GWRONGS	OR	PINST	SENSOR		FE/FT-702 send wrong signals to FICV-702
GPRESS	OR	GPMOTOR	PUMP		Loss of pump pressure
GCIRC	AND	GPS1	GPS		Interlock circuit not opened
GPMOTOR	OR	MOTOR	POWER		Pump motor stops
GPS1	OR	PS1	TETT		PS-1 fails to open
GPS	OR	GBUTTON	PS		Panic switch fails to open
GBUTTON	OR	GHORN	OPERATOR		Operator fails to push button
GHORN	OR	GPS2	HORN	POWER	Horn fails to sound
GPS2	OR	PS2	TETT		PS-2 fails to close

Primary Events Input Data

Event Name	T	Failure Rate	Repair Time	On-demand Unavailability	Description
BY1HE	OM	1.000000E-06	1.000000E+02		By-pass opens (human error)
FICV	OM	7.000000E-05	3.000000E+01		primary control valve failure (open)
HEAT	OM	5.000000E-05	5.000000E+01		Heat exchanger failure
HORN	UN			3.000000E-04	Horn fails to sound
MOTOR	OM	1.000000E-06	2.000000E+01		Primary motor failure
OPERATOR	UN			1.000000E-03	Operator failure
PINST	OM	5.000000E-05	1.000000E+01		Primary instrument failure
POWER	OM	3.000000E-07	1.000000E+02		Area power failure
PS	UN			3.000000E-04	Panic switch fails
PS1	OM	4.000000E-05	2.000000E+01		PS-1 failure
PS2	OM	4.000000E-05	2.000000E+01		PS-2 failure
PUMP	OM	3.000000E-06	2.000000E+01		Primary pump failure
SENSOR	OM	1.300000E-04	2.000000E+01		Sensor failure (low reading)
SV1	OM	5.000000E-05	2.000000E+01		SV-1 stuck closed

Event Name	T	Failure Rate	Repair Time	On-demand Unavailability	Description
TETT	OM	4.000000E-05	2.000000E+01		TE/TT-714 transmits/reads low temp.
WATER	OM	1.000000E-06	3.000000E+02		Utility interruptions (water)

Results from Kumamoto-Henley

Q-Unavailability: 2.20582E-03

ω-Unconditional failure frequency: 7.17993E-05

ν-Unconditional repair frequency: 7.19580E-05

W-Expected number of failures: 7.16904E-03

V-Expected number of repairs: 7.15654E-03

Number of MCS: 41 distributed as 2 of order 1; 15 of order 2; 24 of order 3;

Check: Q = W – V = 1.2503E-2 **WRONG** because of the use of approximated equations.

Results from ASTRA

Q-Unavailability: 2.094106E-03

ω-Unconditional failure frequency: 7.175528E-05

ν-Unconditional repair frequency: 6.889023E-05

W-Expected number of failures: 7.159382E-03

V-Expected number of repairs: 5.065273E-03

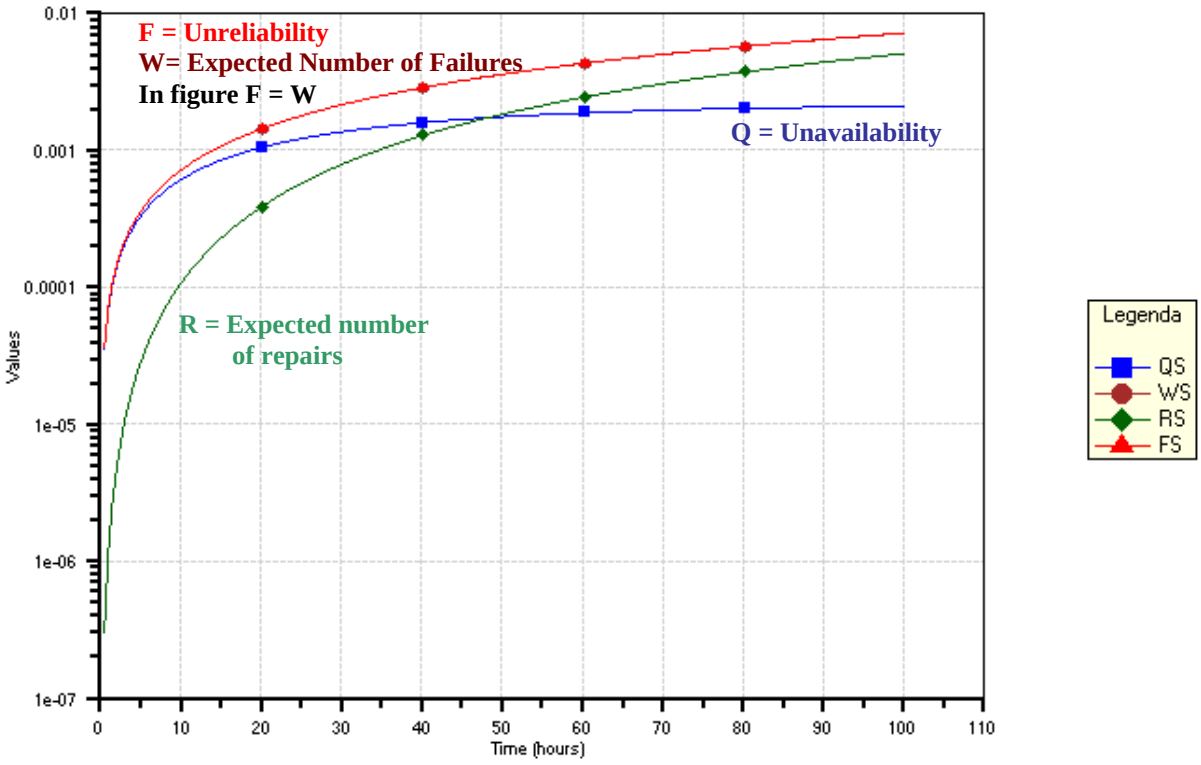
Number of MCS: 41 distributed as 2 of order 1; 15 of order 2; 24 of order 3;

Check: Q = W – V = 2.094109E-03 **CORRECT**

Analysis Results: Cut-sets vs. Unavailability

#	Value	Importance	Order	Minimal Cut Set		
1	2.021362E-03	9.652629E-01	1	FICV		
2	6.320941E-05	3.018444E-02	1	BY1HE		
3	2.556183E-06	1.220656E-03	2	SENSOR	SV1	
4	2.141345E-06	1.022558E-03	2	HEAT	SV1	
5	2.045341E-06	9.767136E-04	2	SENSOR	TETT	
6	1.713407E-06	8.182046E-04	2	HEAT	TETT	
7	4.958813E-07	2.367986E-04	2	PINST	SV1	
8	3.967816E-07	1.894755E-04	2	PINST	TETT	
9	8.438209E-08	4.029505E-05	2	SV1	WATER	
10	6.751871E-08	3.224226E-05	2	TETT	WATER	
11	5.913361E-08	2.823812E-05	2	PUMP	SV1	
12	4.731602E-08	2.259486E-05	2	PUMP	TETT	
13	1.971196E-08	9.413070E-06	2	MOTOR	SV1	
14	1.881742E-08	8.985900E-06	2	POWER	SV1	
15	1.577262E-08	7.531910E-06	2	MOTOR	TETT	
16	1.505685E-08	7.190108E-06	2	POWER	TETT	
17	1.505685E-08	7.190108E-06	2	POWER	PS1	
18	2.045342E-09	9.767136E-07	3	OPERATOR	PS1	SENSOR
19	1.713407E-09	8.182047E-07	3	HEAT	OPERATOR	PS1
20	1.623993E-09	7.755066E-07	3	PS1	PS2	SENSOR
21	1.360438E-09	6.496511E-07	3	HEAT	PS1	PS2
22	6.136025E-10	2.930141E-07	3	PS	PS1	SENSOR
23	6.136025E-10	2.930141E-07	3	HORN	PS1	SENSOR
24	5.140221E-10	2.454614E-07	3	HEAT	HORN	PS1
25	5.140221E-10	2.454614E-07	3	HEAT	PS	PS1
26	3.967816E-10	1.894755E-07	3	OPERATOR	PINST	PS1
27	3.150430E-10	1.504427E-07	3	PINST	PS1	PS2
28	1.190345E-10	5.684264E-08	3	PINST	PS	PS1
29	1.190345E-10	5.684264E-08	3	HORN	PINST	PS1
30	6.751871E-11	3.224227E-08	3	OPERATOR	PS1	WATER
31	5.360958E-11	2.560023E-08	3	PS1	PS2	WATER
32	4.731602E-11	2.259486E-08	3	OPERATOR	PS1	PUMP
33	3.756873E-11	1.794022E-08	3	PS1	PS2	PUMP
34	2.025561E-11	9.672680E-09	3	PS	PS1	WATER
35	2.025561E-11	9.672680E-09	3	HORN	PS1	WATER
36	1.577262E-11	7.531910E-09	3	MOTOR	OPERATOR	PS1
37	1.419481E-11	6.778458E-09	3	HORN	PS1	PUMP
38	1.419481E-11	6.778458E-09	3	PS	PS1	PUMP
39	1.252339E-11	5.980306E-09	3	MOTOR	PS1	PS2
40	4.731785E-12	2.259573E-09	3	MOTOR	PS	PS1
41	4.731785E-12	2.259573E-09	3	HORN	MOTOR	PS1

ASTRA plot of results at the system level.



Henley Kumamoto, Example 3, Page 524

3.7 Non-Coherent Fault Tree analysis

3.7.1. Filename: Zhang-Mei0.

Source: Zhang-Mei, IEEE Trans. Reliab. Vol R-34, N,. 4, 1985, 308-313

Problem description:
Determine Unavailability, Failure frequency, Birnbaum and Criticality importance indexes of the following non-coherent function:
TOP = $x_1 x_2 + x_1 x_3 + x_2 \bar{x}_3$

Primary Events Input Data

Event Name	Failure Rate	Repair Time
1	1.000000E-03	10
2	2.000000E-03	20
3	3.000000E-03	60

Mission time (hours): 500 h

Zhang-Mei	ASTRA 3
Q_{UB} = 3.4 e-4	Q_{TOP} = 3.4105 e-2
ω = 1.9e-3	ω = 1.9017e-3

Importance analysis Zhang-Mei

Event	IB	IB+	IB-	IC	IC+	IC-
x_1	1.525e-1			4.42847e-2		
x_2	8.475e-1			9.95571e-1		
x_3		9.5e-3	3.8e-2		4.25813e-2	9.46254e-1

Importance analysis ASTRA 3

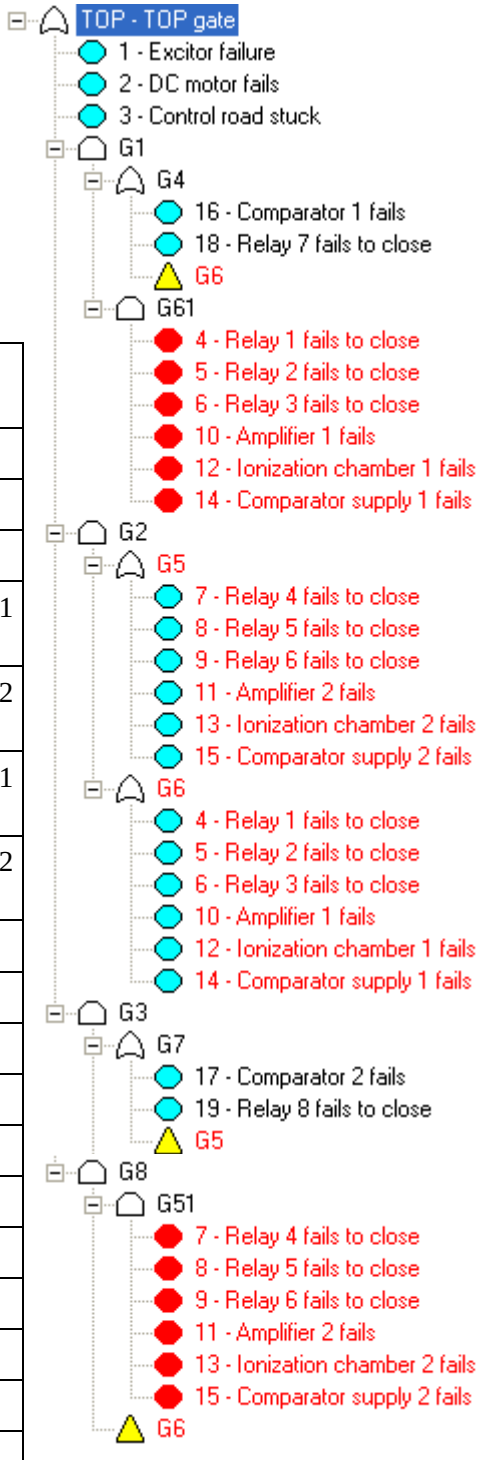
Event	IB	IB+	IB-	IC	IC+	IC-
x_1	1.525e-1			4.42819e-2		
x_2	8.4746e-1			9.955718e-1		
x_3		9.520e-3	3.808e-2		4.25788e-2	9.46255e-1

Conclusion: The results from ASTRA are in perfect agreement with those of the reference source.

3.7.2 Filename: Zhang-Mei1

Source: Zhang-Mei, IEEE Trans. Rel., Vol. R326, N. 4, 1987, 436-439

Problem description:
Determine Unavailability, Failure frequency, Birnbaum and Criticality importance indexes of the non-coherent fault tree shown on the right (red events are negated events)



The following table contains the data characterising the basic events

vent Name	Failure Rate h^{-1}	Repair Time h	Description
1	1.0 E-05	200	Excitor failure
10	1.0 E-04	100	Amplifier 1 fails
11	1.0 E-04	100	Amplifier 2 fails
12	1.0 E-04	200	Ionization chamber 1 fails
13	1.0 E-04	200	Ionization chamber 2 fails
14	1.0 E-05	100	Comparator supply 1 fails
15	1.0 E-05	100	Comparator supply 2 fails
16	4.0 E-06	100	Comparator 1 fails
17	4.0 E-06	100	Comparator 2 fails
18	1.0 E-05	100	Relay 7 fails to close
19	1.0 E-05	100	Relay 8 fails to close
2	5.0 E-06	200	DC motor fails
3	5.0 E-06	200	Control road stuck
4	1.0 E-05	100	Relay 1 fails to close
5	1.0 E-05	100	Relay 2 fails to close
6	1.0 E-05	100	Relay 3 fails to close
7	1.0 E-05	100	Relay 4 fails to close
8	1.0 E-05	100	Relay 5 fails to close
9	1.0 E-05	100	Relay 6 fails to close

Results:

Zhang-Mei	ASTRA 3
Q_{TOP} = 6.5 E-3	Q_{TOP} = 6.477 E-3
ω_{TOP} = 5.0 E-5	ω_{TOP} = 4.97 E-5

MTBF= 20000 h MTBF= 20111 h

The small differences are due to the fact that Zhang-Mei use the rare event approximation.

Birnbaum importance

Zhang-Mei		**ASTRA 3**		
Ranking	**IB = IB+ - IB-**	**IB+**	**IB-**	**Compar.**
1	0.995510	0.9955097	0	**OK**
2	0.994516	0.994516	0	**OK**
3	“	“	0	**OK**
18	0.962571	0.962706	0	**OK**
16	0.961994	0.9619936	0	**OK**
12	3.25519e-2	3.387804e-2	1.326127e-3	**OK**
13	“	3.25519e-2	0	**OK**
10	3.22328e-2	3.35545e-2	1.326127e-3	**OK**
11	“	3.223277e-2	0	**OK**
4	3.19456e-2	3.32469e-2	1.301425e-3	**OK**
5	“	“	“	**OK**
6	“	3.19455e-2	0	**OK**
7	“	“	“	**OK**
8	“	“	“	**OK**
9	“	“	“	**OK**
14	“	3.32469e-2	1.301425e-3	**OK**
15	“	3.19455e-2	0	**OK**
19	“	“	“	**OK**
17	0.319264e-2	0.319264e-2	0	**OK**

Criticality importance

Zhang-Mei			**ASTRA 3**		
Ranking	**IC+**	**IC-**	**IC+**	**IC-**	**Compar.**
1	0.306766	0	0.300766	0	**OK**
4	0.512765e-2	0.200717	0.5127647e-2	0.2007174	**OK**
5	“	“	“	“	**OK**
6	“	“	“	“	**OK**
14	“	“	“	“	**OK**
10	5.127665e-2	0.200717	5.1276647e-2	0.2007174	**OK**
12	0.102533	0.200717	0.1025529	0.2007174	**OK**
2	0.153383	0	0.1533832	0	**OK**
3	“	0	“	0	**OK**
18	0.148456	0	0.1484563	0	**OK**
13	9.85386e-2	0	9.85386e-2	0	**OK**
16	5.93825e-2	0	5.93825e-2	0	**OK**
11	4.92693e-2	0	4.92693e-2	0	**OK**
7	4.92693e-3	0	4.92693e-3	0	**OK**
8	“	0	“	0	**OK**
9	“	0	“	0	**OK**
19	“	0	“	0	**OK**
17	1.97077e-3	0	1.97077e-3	0	**OK**

Conclusion: The results from ASTRA are in perfect agreement with those of the reference source.

3.8 Test on the use of Cut off thresholds

The following test cases are reported to prove the correct implementation of the cut-off technique.

3.8.1 Filename: Salp3

N. events: 34; N. gates: 45; Mission time T= 8760 h.

ASTRA 3

$Q_m(T)$ = 7.789e-4 due to the presence of tested events.

Total number of MCS = 205

Distribution of MCS vs. order and vs probability

Order	Number of MCS
1	0
2	5
3	13
4	38
5	102
6	43
7	4

Decade	Number of MCS
1.e-4	6
1.e-5	2
1.e-6	6
1.e-7	5
1.e-8	25
1.e-9	11
1.e-10	39
1.e-11	23
1.e-12	29
1.e-13	21
1.e-14	2
1.e-15	21
1.e-16	10
1.e-17	12
1.e-18	2

Check on the percentage value

Nlim = 4	Plim = 0	N.MCS = 56	% Q_{TOP} = 99.98	OK
Nlim = 2	Plim = 0	N.MCS = 5	% Q_{TOP} = 33.22	OK
Nlim = 99	Plim = 1.e-6	N.MCS = 56	% Q_{TOP} = 99.98	OK
Nlim = 99	Plim = 1.e-5	N.MCS = 8	% Q_{TOP} = 99.85	OK
Nlim = 99	Plim = 1.e-4	N.MCS = 6	% Q_{TOP} = 98.30	OK
Nlim = 2	Plim = 1.e-7	N.MCS = 5	% Q_{TOP} = 33.22	OK

3.8.2 Filename: Baobab1

Source: Dutuit - Rauzy (2001)

N. events: 61; N. gates: 84; Mission time: 8760 h.

ASTRA 3

Q_{TOP} = 1.282305e-6. Total number of MCS = 46,188

Distribution of MCS vs. order and probability

Order	Number of MCS (ASTRA)	Number of MCS (source)
1	0	0
2	1	1
3	1	1
4	70	70
5	400	400
6	2212	2212
7	14748	14748
8	8460	8460
9	10624	10624
10	6600	6600
11	3072	3072

The agreement between ASTRA and the source is perfect.

Decade	Number of MCS
1.e-8	12
1.e-9	244
1.e-10	1357
1.e-11	6664
1.e-12	5777
1.e-13	5202
1.e-14	4176
1.e-15	3496
1.e-16	4872
1.e-17	3852
1.e-18	3196
1.e-19	4840
1.e-20	2252
1.e-21	248

Check on the percentage value

Nlim = 5	Plim = 0	N.MCS = 472	% Q_{TOP} = 5.00	OK
Nlim = 8	Plim = 0	N.MCS = 25892	% Q_{TOP} = 99.99	OK
Nlim = 99	Plim = 1.e-10	N.MCS = 1613	% Q_{TOP} = 84.29	OK
Nlim = 99	Plim = 1.e-11	N.MCS = 8277	% Q_{TOP} = 98.52	OK
Nlim = 6	Plim = 1.e-12	N.MCS = 2142	% Q_{TOP} = 73.14	OK
Nlim = 6	Plim = 0	N.MCS = 2684	% Q_{TOP} = 73.15	OK
Nlim = 7	Plim = 0	N.MCS = 17432	% Q_{TOP} = 99.89	OK

3.9 Comparison of ASTRA with other FTA tools

3.9.1 Comparison on the number of MCS

Source: Rauzy (1993), Caldarola (1980), JRC ASTRA development team.

Comparison of the total number of MCS for a set of fault trees of different complexity. ASTRA results were compared with the results obtained using ARALIA and RISKSPECTRUM PSA (Relcon Scandpower, http://www.riskspectrum.com) tools.

Table below presents number of MCS obtained using ASTRA and ARALIA.

Tree	N. gates	N. events	N. MCS Aralia	N. MCS ASTRA
Chinese	36	25	392	392
European1	84	61	46,188	46,188
European2	40	32	4,805	4,805
European3	107	80	24,386	24,386
1-das-008	145	103	8,060	8,060
2-das-1	82	122	14,217	14,217
3-das-3	30	51	16,200	16,200
4-das-4	30	53	16,704	16,704
5-das-5	20	51	17,280	17,280
6-das-6	112	121	19,518	19,518
7-das-7	275	276	25,988	25,988
9-das-2	36	49	27,788	27,778

In the Caldarola report two simplified scram systems are described and solved. The results are given in the following table:

Tree	N. gates	N. events	N. MCS Caldarola	N. MCS ASTRA
Cal2	40	32	5,630	5,630
Cal3	68	58	11,220,036	12,378,546

The agreement is perfect, except for the Cal3 fault tree.

***Comment**: The manual verification of the calculation made by Caldarola (Cal3) has confirmed the ASTRA result not the Caldarola's result. Difference in the results is due to the incorrect number of MCS in the Caldarola report for the supercomponent SCO1.*

The Table below contains the number of MCS obtained using ASTRA and RISKSPECTRUM PSA (RS) for a set of fault trees of real systems.

Tree	N. gates	N. events	N. MCS RS	N. MCS ASTRA
Abtrw014	88	118	10302	10302
ASEA1and	178	149	347936	347936
Iveco_01	165	392	67762	67762
Reactinh	15	16	41	41
TOP 4	252	264	53378	53378
UTOP 2	49	67	12096	12096

Conclusion: The agreement between ASTRA and the tools ARALIA and RISKSPECTRUM PSA is perfect.

3.9.2 Comparison of ASTRA 3 with ASTRA2

This set of tests concerns the comparison between ASTRA2 and ASTRA3 on a set of coherent fault trees of real systems.
For each fault tree, analysed by means of ASTRA 2 and ASTRA 3, all results are considered. ASTRA 2 performs the probabilistic analysis on the basis of the set of significant MCS, i.e. using the rare event approximation. For this reason the rare event approximation has also been implemented, for testing purposes only, in ASTRA 3.

3.9.2.1. Filename: gen-008

N. events: 73; N. gates: 85; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 2.23340e-1 (UB = upper bound)	Q_{TOP} = 2.0990e-1	Q_{UB} = 2.23340e-1
	ω_{TOP} = 2.40449e-5	
W_{UB} = 2.23340	W_{TOP} = 2.09843e-1	

Distribution of MCS in ASTRA 2

Total Number of MCS = 551

Order	Number
1	6
2	60
3	299
4	170
5	16

Distribution of MCS in ASTRA 3

Total Number of MCS = 551

Order	Number
1	6
2	60
3	299
4	170
5	16

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.2. Filename: hur-001

N. events: 108; N. gates: 101; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 2.0046e-2	Q_{TOP} = 1.99442e-2	Q_{UB} = 2.0046e-2

Distribution of MCS in ASTRA 2

Total Number of MCS = 7958

Order	Number
1	2
2	1
3	39
4	23
5	34
6	698
7	2448
8	4156
9	560

Distribution of MCS in ASTRA 3

Total Number of MCS = 7958

Order	Number
1	2
2	1
3	39
4	23
5	34
6	698
7	2448
8	4156
9	560

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.3 Filename: isp-001

N. events: 143; N. gates: 104; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 6.8811e-2	Q_{TOP} = 5.17 e-2	Q_{UB} = 6.8811e-2

Note the difference between the Q_{UB} and the exact value Q_{TOP}.

Distribution of MCS in ASTRA 2 Automatic probabilistic cut-off = 1.0e-10

Total Number of MCS = 276.785

Order	Number
1	1
2	587
3	100
4	85
5	106,920

Distribution of MCS in ASTRA 3 With probabilistic cut-off = 1.0e-10

Total Number of MCS =276.785

Order	Number
1	1
2	587
3	100
4	85
5	106,920

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.4 Filename: isp-002

N. events: 116; N. gates: 122; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 1.79519e-2	Q_{TOP} = 1.72447e-2	Q_{UB} = 1.79519e-2

Distribution of MCS in ASTRA 2 Automatic probabilistic cut-off P_{lim} = 1.0e-10; n_{Lim} = 99

Total Number of MCS = 5.197.647

Order	Number
1	1
2	77
3	210
4	3973

Distribution of MCS in ASTRA 3 With probabilistic cut-off P_{lim} = 1.0e-10; n_{Lim} = 99

Total Number of MCS = 5.197.647

Order	Number
1	1
2	77
3	210
4	3973

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.5 Filename: isp-003

N. events: 91; N. gates: 95; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 3.5308e-3	Q_{TOP} = 3.23326e-3	Q_{UB} = 3.5308e-3

Distribution of MCS in ASTRA 2

Total Number of MCS = 3434

Order	Number
1	0
2	22
3	1320
4	1070
5	720
6	200
7	82
8	16

Distribution of MCS in ASTRA 3

Total Number of MCS = 3434

Order	Number
1	0
2	22
3	1320
4	1070
5	720
6	200
7	82
8	16

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.6 Filename: ixi-003

N. events: 74; N. gates: 73; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 1.009014e-5	Q_{TOP} = 1.007926e-5	Q_{UB} = 1.009014e-5

Distribution of MCS in ASTRA 2

Total Number of MCS = 1446

Order	Number
1	1
2	525
3	820
4	100

Distribution of MCS in ASTRA 3

Total Number of MCS = 1446

Order	Number
1	1
2	525
3	820
4	100

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.7 Filename: psa-002

N. events: 174; N. gates: 191; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 2.378224e-4	Q_{TOP} = 2.347892e-4	Q_{UB} = 2.378224e-4

Distribution of MCS in ASTRA 2

Total Number of MCS = 470

Order	Number
1	0
2	2
3	173
4	167
5	102
6	26

Distribution of MCS in ASTRA 3

Total Number of MCS = = 470

Order	Number
1	0
2	2
3	173
4	167
5	102
6	26

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.2.8 Filename: iveco-01

N. events: 392; N. gates: 165; Mission time: 8760 h.

ASTRA 2	ASTRA 3	
Q_{UB} = 0.6163417	Q_{TOP} = 0.466617	Q_{UB} = 0.616341
ω_{UB} = 3.84779e-5	ω_{TOP} = 6.65147e-5	
W_{UB} = 4.67521e-1	W_{TOP} = 6.89016e-2	

Distribution of MCS in ASTRA 2

Total Number of MCS = 67,762 Plim automatically determined. Plim = 7.66 e-7

Order	Number
1	235
2	1969
3	
4	
5	

Distribution of MCS in ASTRA 3

Total Number of MCS = 67,762

Order	Number
1	235
2	1969
3	22
4	0
5	65,536

Conclusion: For this test case the agreement between ASTRA 2 and ASTRA 3 is perfect.

3.9.3. Comparison of ASTRA with SAPHIRE

Source: SAPHIRE in NUREG/CR-6116, EGG-2717, Vol. 1.

Comparison between ASTRA3 and SAPHIRE on a simple system.

Filename: **Saphire1** N. events: 5; N. gates: 5;

P(B1) = 0.01; P(B2) = 0.02; P(B3) = 0.03; P(B4) = 0.04; P(B5) = 0.05.

ASTRA 3	SAPHIRE
Q_{UB} = 7.05e-4	Q_{UB} = 7.05e-4
Q_{EXACT} = 6.94024e-4	Q_{EXACT} = 6.93148e-4

Total number of MCS = 5

Distribution of MCS in ASTRA 3

Order	Number
1	0
2	2
3	3

Importance analysis SAPHIRE

Event	**RAW**	**RRW**	**Birnbaum**
B1	86.1	7.832	6.060E-2
B2	16.96	1.484	1.148E-2
B3	5.809	1.175	3.494E-3
B4	16.64	2.877	1.148E-2
B5	3.827	1.175	2.097E-3

Importance analysis ASTRA 3

Event	**RAW**	**RRW**	**Birnbaum**
B1	87.33	7.8155	6.0522E-2
B2	16.54	1.4618	1.1011E-2
B3	5.75	1.1723	3.4008E-3
B4	16.54	2.8397	1.1240E-2
B5	3.79	1.1723	2.0405E-3

From hand calculations the results obtained are equal to those given by ASTRA. The unavailability value reported in the Saphire manual is not correct. This explains also the differences in the importance analysis tables.

3.10 Test on the application of Boundary Conditions

3.10.1 Application of boundary conditions to the SAPHIRE fault tree. See 3.9.3

Source: SAPHIRE in NUREG/CR-6116, EGG-2717, Vol. 1.

Filename: **Saphire1** N. events: 5; N. gates: 5;

P(B1) = 0.01; P(B2) = 0.02; P(B3) = 0.03; P(B4) = 0.04; P(B5) = 0.05.

In ASTRA basic events may be associated with boundary conditions, i.e. their state can be set and remain fixed for the whole mission interval. Boundary conditions are applied to the fault tree prior to the modularisation. Hence the fault tree is reduced by properly deleting the events with an associated BC value.

Boundary Condition set: B4=good; B5 = failed.

In ASTRA good = 0; failed = 1.

Minimal Cut Sets without boundary condition analysis:

B1	B4	
B1	B2	
B3	B4	B5
B2	B3	B5
B1	B3	B5

Q_{EXACT} = 6.94024e-4

Minimal Cut Sets with boundary condition analysis:

B1	B2
B2	B3
B1	B3

Q_{EXACT} = 1.08800e-3

Conclusion: Boundary conditions correctly applied.

3.10.2 Application of boundary conditions to the Chemical reactor fault tree. See 3.6.2

Source: Kumamoto-Henley (first edition), page 524 + Table 10.3. Fault tree in Fig.13.6
This Fault tree has already been considered in 3.6.2.

Cut-sets list

#	Order	Minimal Cut Set		
1	1	FICV		
2	1	BY1HE		
3	2	SENSOR	SV1	
4	2	HEAT	SV1	
5	2	SENSOR	TETT	
6	2	HEAT	TETT	
7	2	PINST	SV1	
8	2	PINST	TETT	
9	2	SV1	WATER	
10	2	TETT	WATER	
11	2	PUMP	SV1	
12	2	PUMP	TETT	
13	2	MOTOR	SV1	
14	2	POWER	SV1	
15	2	MOTOR	TETT	
16	2	POWER	TETT	
17	2	POWER	PS1	
18	3	OPERATOR	PS1	SENSOR
19	3	HEAT	OPERATOR	PS1
20	3	PS1	PS2	SENSOR
21	3	HEAT	PS1	PS2
22	3	PS	PS1	SENSOR
23	3	HORN	PS1	SENSOR
24	3	HEAT	HORN	PS1
25	3	HEAT	PS	PS1
26	3	OPERATOR	PINST	PS1
27	3	PINST	PS1	PS2
28	3	PINST	PS	PS1
29	3	HORN	PINST	PS1
30	3	OPERATOR	PS1	WATER
31	3	PS1	PS2	WATER
32	3	OPERATOR	PS1	PUMP
33	3	PS1	PS2	PUMP
34	3	PS	PS1	WATER
35	3	HORN	PS1	WATER
36	3	MOTOR	OPERATOR	PS1
37	3	HORN	PS1	PUMP
38	3	PS	PS1	PUMP
39	3	MOTOR	PS1	PS2
40	3	MOTOR	PS	PS1
41	3	HORN	MOTOR	PS1

1) Boundary condition Set1: SENSOR = failed; SV1 = failed

Result from ASTRA: The Top-event is verified.

2) Boundary condition Set2: TETT = good; SV1 = good

Test: MCS containing TETT or SV1 are removed from the full list, giving the flowing reduces list.

#	Order	Minimal Cut Set		
1	1	FICV		
2	1	BY1HE		
3	2	POWER	PS1	
4	3	OPERATOR	PS1	SENSOR
5	3	HEAT	OPERATOR	PS1
6	3	PS1	PS2	SENSOR
7	3	HEAT	PS1	PS2
8	3	HORN	PS1	SENSOR
9	3	PS	PS1	SENSOR
10	3	HEAT	PS	PS1
11	3	HEAT	HORN	PS1
12	3	OPERATOR	PINST	PS1
13	3	PINST	PS1	PS2
14	3	OPERATOR	PS1	WATER
15	3	PS1	PS2	WATER
16	3	HORN	PINST	PS1
17	3	PINST	PS	PS1
18	3	HORN	PS1	WATER
19	3	PS	PS1	WATER
20	3	OPERATOR	PS1	PUMP
21	3	PS1	PS2	PUMP
22	3	MOTOR	OPERATOR	PS1
23	3	PS	PS1	PUMP
24	3	HORN	PS1	PUMP
25	3	MOTOR	PS1	PS2
26	3	MOTOR	PS	PS1
27	3	HORN	MOTOR	PS1

3) Boundary condition Set3: TETT = good; SV1 = failed

Test: MCS containing TETT are removed; SV1 is removed from all MCS in which appears and finally all remaining combinations must be minimised. This activity has been performed manually.

#	Order	Minimal Cut Set
1	1	SENSOR
2	1	HEAT
3	1	FICV
4	1	PINST
5	1	WATER
6	1	BY1HE
7	1	PUMP
8	1	POWER
9	1	MOTOR

Conclusion: Boundary conditions correctly applied.

3.10.3 Application of boundary conditions to a non-coherent fault tree. See 3.7.2

Source: Zhang-Mei, IEEE Trans. Rel., Vol. R326, N. 4, 1987, 436-439

List of MCS calculated without any boundary condition.

#	Order	Minimal Cut Set	
1	1	1	
2	1	18	
3	1	2	
4	1	3	
5	1	16	
6	2	12	13
7	2	10	13
8	2	11	12
9	2	10	11
10	2	13	6
11	2	12	8
12	2	13	5
13	2	12	9
14	2	13	4
15	2	13	14
16	2	12	19
17	2	12	15
18	2	12	7
19	2	11	5
20	2	11	14
21	2	11	6
22	2	10	15
23	2	10	8
24	2	10	7
25	2	10	19
26	2	11	4
27	2	10	9
28	2	12	17
29	2	10	17
30	2	4	9
31	2	4	7
32	2	6	7
33	2	5	7

#	Order	Minimal Cut Set	
34	2	6	9
35	2	5	9
36	2	15	6
37	2	6	8
38	2	5	8
39	2	4	8
40	2	15	5
41	2	15	4
42	2	19	4
43	2	19	5
44	2	19	6
45	2	14	19
46	2	14	15
47	2	14	9
48	2	14	7
49	2	14	8
50	2	17	6
51	2	17	5
52	2	14	17
53	2	17	4

1) Boundary condition Set3: 5 = 12 = good; 11 = failed

Test: manual removal of MCS containing events 5 or 12; event 11 is also removed from all MCS in which it appears and finally all remaining combinations have been minimised. Results reported in the following Table are the same as determine by ASTRA.

#	Order	Minimal Cut Set		
1	1	1		
2	1	18		
3	1	2		
4	1	3		
5	1	16		

#	Order	Minimal Cut Set		
6	2	10		
7	2	14		
8	2	6		
9	2	4		

3.11 Analysis of large fault trees: truncated ZBDD

For very large fault trees the working memory can be not sufficient to generate and store the LBDD representation. In order to analyse large fault trees the direct ZBDD construction module was developed. By using this module it is possible to apply the cut-off technique during the ZBDD construction, thus by-passing the LBDD construction. The advantage is the decreased memory usage; the high level of quantification accuracy is still achievable even without any information on the truncation error. The current implementation is limited to coherent fault trees; the extension to non coherent fault trees is part of future developments.
The set of tests described in this section concerns the comparison of MCS obtained by the ZBDD module using different probabilistic cut-off levels with the MCS calculated by the ASTRA3 LBDD module.

3.11.1 Filename: 7-das-7

Source: Rauzy (1993)

N. events: 276; N. gates: 275.

Problem description:
Determine the Minimal Cut Sets (MCS) and the Upper-bound unavailability of a large fault tree by applying different cut-off levels. All components are assumed to be characterised by the same probability:
q = 1.0e-2.

MCS obtained using ASTRA 3 LBDD module

Total Number of MCS = 25988
Q_{UB} = 4.554e-1

Cut-off level	Number of MCS*
1e-02	32
1e-04	1277
1e-06	12082
1e-08	25988

* Number of MCSs was obtained using the ASTRA 3 Cut-sets analysis module

MCS obtained using ASTRA 3 ZBDD module with different cut-off levels

Cut-off level	Number of MCS	Q_{UB}
1e-02	32	3.20000e-01
1e-04	1277	4.44500e-01
1e-06	12082	4.55305e-01
1e-08	25988	4.55444e-01

The peek size of the ITE records table during execution of the LBDD module was 20452. The memory usage by the ZBDD algorithm changes with the probabilistic cut off value and is provided in the table below.

Cut-off level	ITE peek
1e-02	1435
1e-04	2833
1e-06	6725
1e-08	7563

It can be seen that the maximum memory usage by ZBDD module was significantly lower than that used by the LBDD module.

Conclusion: For this test case the agreement on MCS number between ASTRA 3 LBDD and ZBDD modules is perfect.

3.11.2 Filename: Baobab1

Source: Dutuit - Rauzy (2001)

N. events: 61; N. gates: 84.

Problem description:
Determine the MCS and the Upper-bound unavailability for a large fault tree by applying different cut-off levels. All components are assumed to be characterised by the same probability: q = 1.0e-2.

MCS obtained using ASTRA 3 LBDD module

Total Number of MCS = 46188
Q_{UB} = 1.681464E-06

Cut-off level	Number of MCS*
1e-08	12
1e-09	256
1e-10	1613
1e-11	8277
1e-12	14054
1e-13	19256
1e-14	23432
1e-15	26928
1e-16	31800
1e-17	35652
1e-18	38848
1e-19	43688
1e-20	45940
1e-21	46188

* Number of MCSs was obtained from the chapter 3.7.2

MCS obtained using ASTRA 3 ZBDD module with different cut-off levels

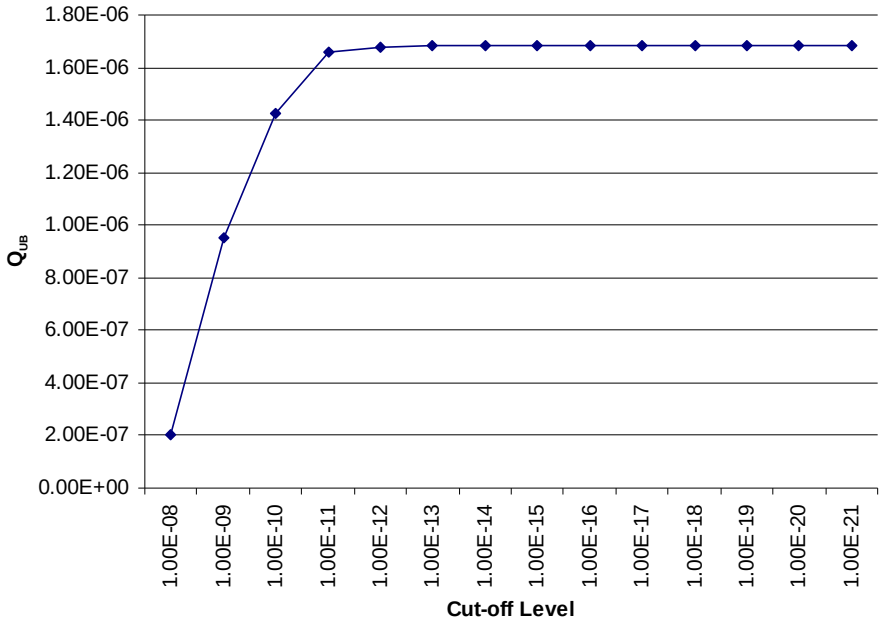
Cut-off level	Number of MCS	Q_{UB}
1e-08	12	1.996769e-07
1e-09	256	9.525085e-07
1e-10	1613	1.423015e-06
1e-11	8277	1.656581e-06
1e-12	14054	1.679147e-06
1e-13	19256	1.681284e-06
1e-14	23432	1.681450e-06
1e-15	26928	1.681462e-06
1e-16	31800	1.681463e-06
1e-17	35652	1.681464e-06
1e-18	38848	1.681464e-06
1e-19	43688	1.681464e-06
1e-20	45940	1.681464e-06
1e-21	46188	1.681464e-06

The ITE peek size during execution of LBDD module was 34476. The memory usage by the ZBDD algorithm is provided in the table below.

Cut-off level	ITE peek
1e-08	2260
1e-09	4877
1e-10	8447
1e-11	15673
1e-12	28997
1e-13	52800
1e-14	98845
1e-15	174733
1e-16	318732
1e-17	549817
1e-18	938637
1e-19	1397785
1e-20	2022743
1e-21	2593887

It can be seen that the peek size of the ITE record table used by the ZBDD module is lower for higher cut-off levels. Lowering of the cut-off level leads to rapid increase of the peek ITE record table size. This is mainly due to the caching of the ITE records and frequent rewriting of the ZBDD during the elimination of non-minimal cut-sets.
However in many cases the top-event probability converges very fast to the exact value and there is no need of using very low cut-off values.

The plot of the Q_{UB} vs. cut-off level showing the convergence is represented in the following figure, in which it can be seen that a good approximation of the Top event unavailability can be obtained using a probabilistic cut-off value equal to $10^{-12} – 10^{-13}$.



Conclusion: For this test case the agreement on MCS number between ASTRA 3 LBDD and ZBDD modules is perfect.

3.11.3 Filename: EDF9203

Source: Rauzy webpage (http://iml.univ-mrs.fr/~arauzy/aralia/benchmark.html).

N. events: 362; N. gates: 707.

Problem description:
Determine the Minimal Cut Sets (MCS) and the Upper-bound unavailability of a fault tree by applying different cut-off levels. All components are assumed to be characterised by the same probabilities:
q = 1.0e-03.

MCS obtained using ASTRA 3 LBDD module

Total Number of MCS =20807446
Q_{UB} = 4.565136e-02

Cut-off level	Number of MCS*
1e-03	37
1e-06	8368
1e-09	327178
1e-12	1873598
1e-15	3580162
1e-18	N/A
1e-21	N/A
1e-24	N/A
1e-27	N/A
1e-30	N/A
1e-33	N/A
1e-36	N/A

* Number of MCSs was obtained using ASTRA 3.0. Cut-sets analysis module
N/A – result not available due to the insufficient working memory

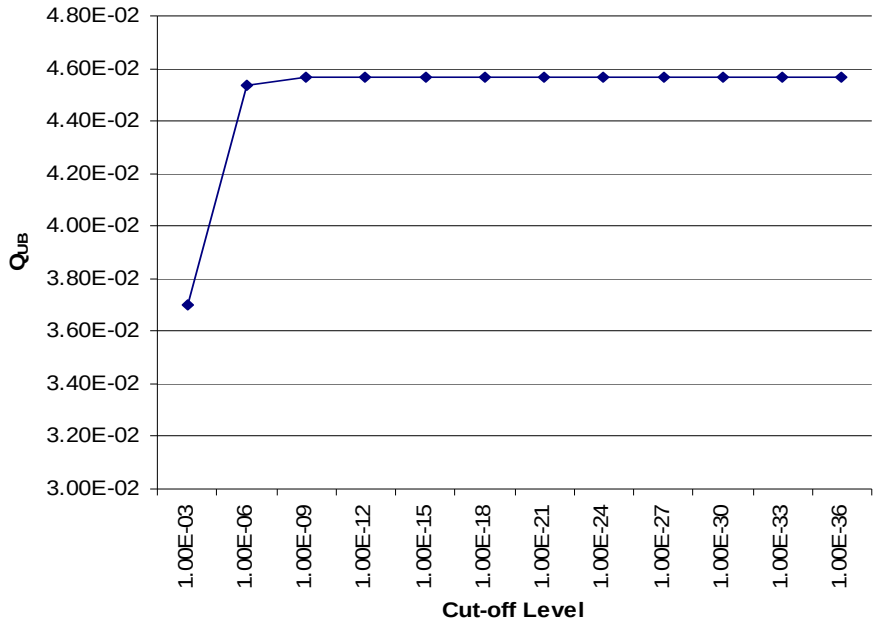
MCS obtained using ASTRA 3 ZBDD module with different cut-off levels

Cut-off level	Number of MCS	Q_{UB}
1e-03	37	3.700000e-02
1e-06	8368	4.533100e-02
1e-09	327178	4.564981e-02
1e-12	1873598	4.565136e-02
1e-15	3580162	4.565136e-02
1e-18	5413130	4.565136e-02
1e-21	8809758	4.565136e-02
1e-24	13381950	4.565136e-02
1e-27	20500566	4.565136e-02
1e-30	20500566	4.565136e-02
1e-33	20798206	4.565136E-02
1e-36	20807446	4.565136E-02

The ITE peek size during the execution of the LBDD module was 1634239. The memory usage by the ZBDD module vs. the probabilistic cut off value is provided in the table below.

Cut-off level	ITE peek
1e-03	4041
1e-06	20848
1e-09	83793
1e-12	221018
1e-15	444296
1e-18	663475
1e-21	1254806
1e-24	1922312
1e-27	2191710
1e-30	3363473
1e-33	3669406
1e-36	3673573

Top-event upper bound probability converges to the exact value very fast. The exact value is obtained by using 1e-12 cut-off value. With this cut-off level the peek size of the ITE record table was 221018 in comparison to the 1634239 used by LBDD module. The plot of the Q_{UB} vs. Cut-off level showing the convergence is represented in the following figure.



Conclusion: For this test case the agreement on available MCS data between ASTRA 3 LBDD and ZBDD modules is perfect.

4. CONCLUSIONS

In this report the results of the application of ASTRA 3.0 to a selected number of fault trees extracted from those considered during the test activity have been described. This activity allowed to prove the correctness of the implemented algorithms and to identify further improvements.

ASTRA is based on the state-of-the-art approach of Binary Decision Diagrams. Two analysis procedures have been developed. The main procedure is based on the dynamic labelling of nodes with the type of the associated variables in order to apply to each node the appropriate logical and probabilistic algorithms; the probabilistic quantification is exactly performed on the LBDD, i.e. without calculating the MCS. Unfortunately, for very complex fault trees, the number of nodes of the LBDD grows exponentially: it may happen that the working memory is not enough to store all nodes; in these cases the analysis cannot be completed. To overcome this difficulty a second analysis method has been implemented which, however, gives approximated results.

The two analysis methods have been successfully tested on a wide range of fault trees as described in this report.

Suggestions for further improvements have also been identified, namely:

- There is room to improve the efficiency of some algorithms, e.g. integration of unreliability function, construction of the LBDD, determination of the SMCS;
- Implementation of the importance measures of basic events in case of failure frequency analysis;
- Extension of the algorithm based on direct construction of truncated ZBDD for non coherent fault trees;
- Make ASTRA conform with the standard IEC 61508 *"Functional safety of electrical / electronic / programmable electronic safety-related systems"*.
- Insert the new basic event parameter *duty time* to model components with mission time less than the system mission time;
- Development of a module for uncertainty analysis applied to the LBDD

ACKNOWLEDGEMENTS

The present work has been executed in 2009 in the framework of the Project "Systems Analysis Applied to Nuclear Safeguards and Non Proliferation", carried out in the NUSIM (Nuclear Fuel Cycle Simulations) action of the Nuclear Security unit of JRC-IPSC. The work was performed as part of the AMENUS (Assessment Methodologies for Nuclear Security) action activities until the end of 2008.

The authors wish to thanks W. Janssens, P. Peerani, and M. Sironi for the support to the activity. A particular thank is due to G.G.M. Cojazzi for the helpful discussions and advice during the whole period in which the ASTRA project was under his responsibility.

REFERENCES

Bryant R.E, 1986, “Graph Based Algorithms for Boolean Functions Manipulation”, *IEEE Transactions on Computers*, Vol. C-35.

Caldarola L., Wickenhauser A., 1981, The Booolean Algebra with Restricted Variables as a Tool for Fault Tree Modularisation, KfK 3190/EUR 7056e, Karlsruhe.

Clarotti C. A., 1981 Limitation of Minimal Cut Set Approach in Evaluating Reliability of Systems with Repairable Components, IEEE Trans. Reliability, Vol. R-30, pp335-338.

Cojazzi, G.G.M., Contini, S., Renda, G., 2005, Fault Tree Analysis in Security related Applications: Challenges and Needs, ESReDA 29th Seminar, Systems Analysis for a More Secure World. Application of System Analysis and RAMS to Security of Complex Systems, JRC, Ispra, Italy

Contini S., Cojazzi G.G.M., De Cola G., 2006, On the exact analysis of non coherent fault trees: the ASTRA package, PSAM 8, New Orleans, USA.

Contini, S., Cojazzi, G.G.M., Renda G., 2008, On the use of non-coherent fault trees in safety and security studies, *Reliability Engineering and System safety, V.93, N.12.*

Contini S., Matuzas V. 2009, “ASTRA 3.0. Theoretical manual”, EUR Technical Report, under publication.

De Cola G., 2005, XS Toolset – MKA Module for Markovian Analysis, User Guide.

Dutuit Y., Rauzy A., Signoret J.P., 2006, Probabilistic assessment in relationship with Safety Integrity Levels by using Fault Trees, ESREL 2006 Conference, Guedes Soares & Zio ed.

Dutuit Y., Rauzy A., 2001, Efficient algorithms to assess component and gate importance in fault tree analysis, *Reliability Engineering and System Safety*, 72,

Ericson, 2005 C.A., Hazard Analysis Techniques for System Safety, Wiley Interscience, ISBN: 0.471-72019-4

Kumamoto H., Henley E.J., 1981, Probabilistic Risk assessment and Management for Engineers and Scientists, Prentice Hall, Englewood Cliffs, NY.

Kumamoto H., Henley E.J., 1996, Probabilistic Risk assessment and Management for Engineers and Scientists, Second Edition, IEEE Press.

IEC 61508-6, 2000 Functional safety of electric/electronic/programmable electronic safety-related systems, Parts 1-7.

IAEA 1991, Case study on the use of PSA methods: determining safety importance of systems and components at nuclear power plants, IAEA TECDOC 590, ISSN 1011-4289, Vienna

Modarres M., Kaminskiy M., Krivstov V., 1999, Reliability Engineering and Risk Analysis, Quality and Reliability / 55, Marcel Dekker Inc. NY, ISBN: 0-8247-2000-8

NUREG/CR-6116, EGG-2717, Vol.1, 1994.

Rausand M., and Hoeland, A., 2004, System Reliability Theory, Models, Statistical Methods, and Applications, Wiley Series in Probability and Statistics, Second edition, ISBN: 0-471-47133-X.

Rauzy A., 1993, New algorithms for fault tree analysis, *Reliability Engineering & System Safety*, Vol 40. N. 3.

Rauzy A., 1996, A Brief Introduction to Binary Decision Diagrams. *RAIRO-APII-JESA*, 30(8).

Rauzy A. Webpage (http://iml.univ-mrs.fr/~arauzy/aralia/benchmark.html).

Twigg D.W., Ramesh A.V. & Sharma, T.C. 2000, Modelling events dependencies using disjoint sets in fault trees, Proceeding 18th International System Safety Conference.

Vaurio J.K. 2001, Making systems with mutually exclusive events analysable by standard fault tree analysis tools, *Reliability Engineering and System Safety*, Vol. 74.

Woo Sik Jung, Sang Hoon Han, Jaejoo Ha, 2004, A fast BDD algorithm for large coherent fault tree analysis, *Reliability Engineering & System Safety*, Vol. 83.

Woo Sik Jung, Sang Hoon Han, Joon-Eon Yang, 2008, Fast BDD truncation method for efficient top event probability calculation, *Nuclear Engineering and Technology*, Vol. 40.

Zhang Q., Mei Q., 1985, Element Importance and System Failure Frequency of a 2-State System, *IEEE Transaction on Reliability*, Vol. R-24, N. 4.

Zhang Q., Mei Q., 1987, Reliability analysis of a real non-coherent system, *IEEE Transaction on Reliability*, Vol. R326, N. 4.

European Commission

EUR 24124 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: ASTRA 3.0: Test Case Report
Author(s): Sergio Contini, Vaidas Matuzas
Luxembourg: Office for Official Publications of the European Communities
2009 – 89 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-14608-4
DOI 10.2788/51332

Abstract
In the context of activities related to the application of system analysis to safety and security of critical installations a new logical and probabilistic fault tree analysis procedure was developed and implemented in the software package ASTRA, version 3.0. This report contains the results of the logical and probabilistic analysis for a limited, but significant, subset of test cases considered during the test campaign performed at the JRC. Most of the described test cases come from the open literature, for which results are available to the reader. For more complex test cases ASTRA 3.0 was compared with other available tools, such as ASTRA 2.0 and XS-MKA, a Markovian analysis package. The experience gained with the testing activity also allowed the identification of a set of recommendations for future improvements.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LB-NA-24124-EN-C

Publications Office
Publications.europa.eu

ISBN 978-92-79-14608-4
9 789279 146084