System Dependability Lab Exercises on Safety Assessment of Static Systems

Hamza Mouddene, Ali Abdoulhamid Zakaria

November 19, 2021

1 Introduction

The computing platform designs support three applications (A_1, A_2 and A_3). Each application A_i is implemented by two tasks A_{iL} and A_{iR}. The application A_i fails if **both** tasks A_{iL} and A_{iR} fail. A task fails if all the computers that can host it fail.

FC_{A_i} loss of application A_i, with $i \in 1, 2, 3$.
FC_One_Appli loss of at least one application.
All the FC are classified CATASTROPHIC for an operation time of $T = 10^3 h$.

Question 1 What are the qualitative and quantitative safety requirements associated to the FCs?
We know that all the FC are Catastrophic, so the qualitative and quantitative safety requirements are :

- order ≥ 2 (Qualitative)
- $\overline{\Lambda} \leq 10^{-9}/flight\ hour$ (Quantitative)

2 Computing Platform Design – solution 1

Figure 1 presents the first solution for the computer platform design. In this solution the **application fails if its computer fails**. We assume that the loss of a computer is modelled by an exponential distribution of failure rate $\lambda = 10^{-5}.h^{-1}$.

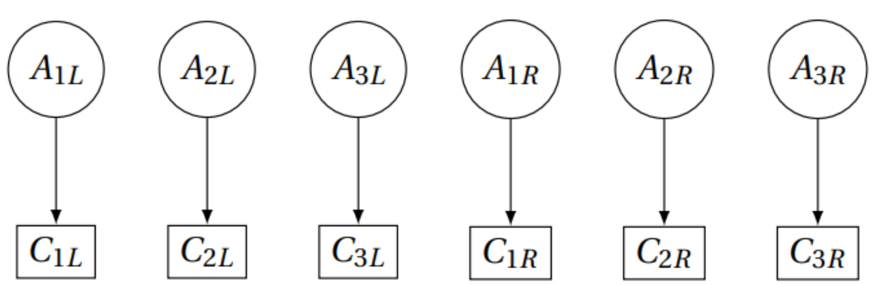


Figure 1: Solution 1 - one computer per task

Question 2

1. The fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.

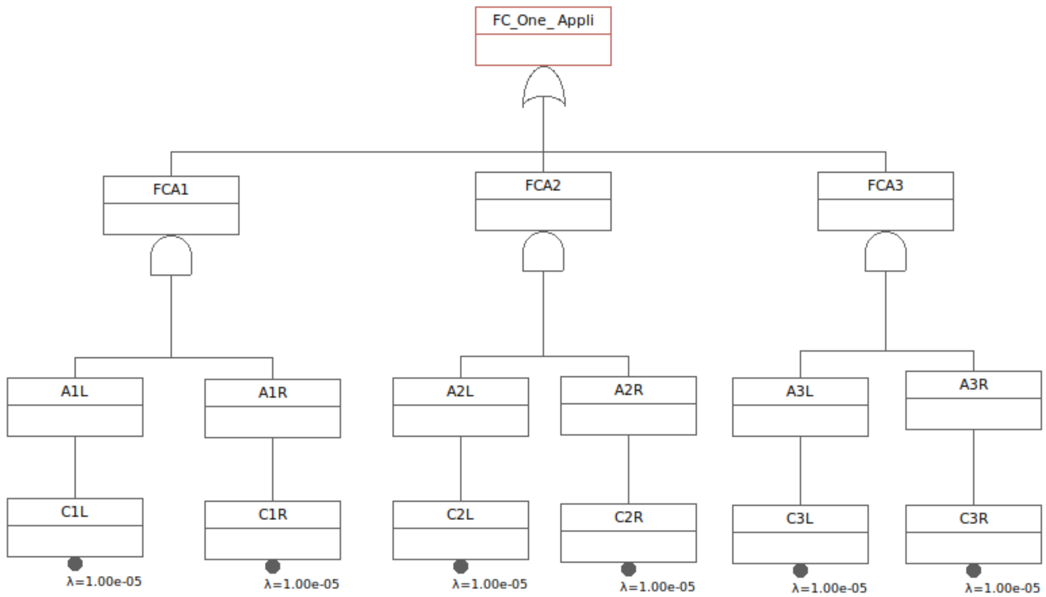
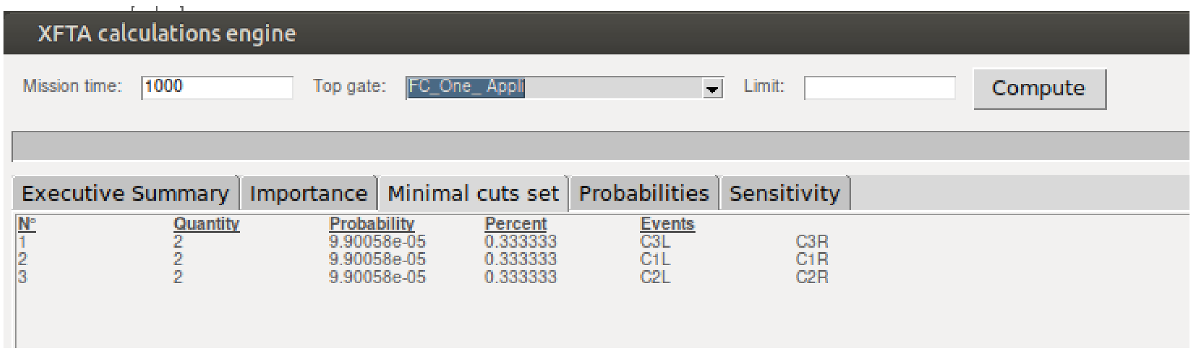


Figure 2: Solution 1 - The fault-tree

2. the Minimal Cut Sets for FC_{A_i} and FC_One_Appli is:



N°	Quantity	Probability	Percent	Events	
1	2	9.90058e-05	0.333333	C3L	C3R
2	2	9.90058e-05	0.333333	C1L	C1R
3	2	9.90058e-05	0.333333	C2L	C2R

Figure 3: Solution 1 - the Minimal Cut Sets for FC_One_Appli

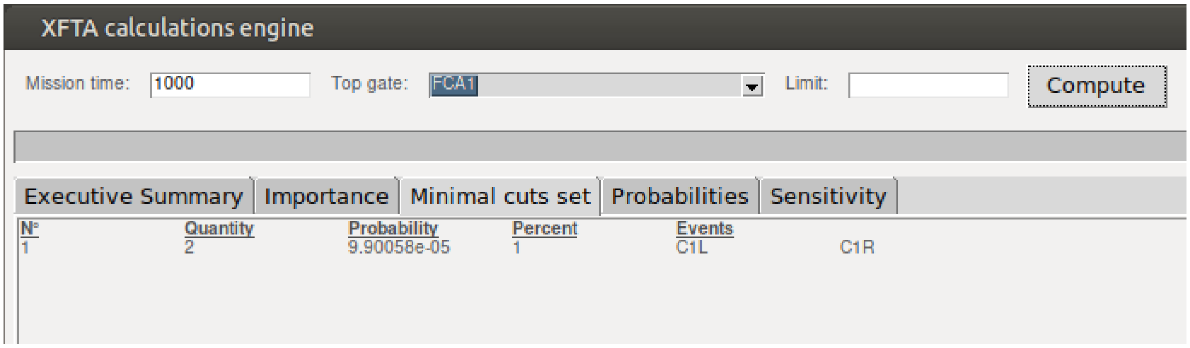


Figure 4: Solution 1 - the Minimal Cut Sets for FC_{A_1}

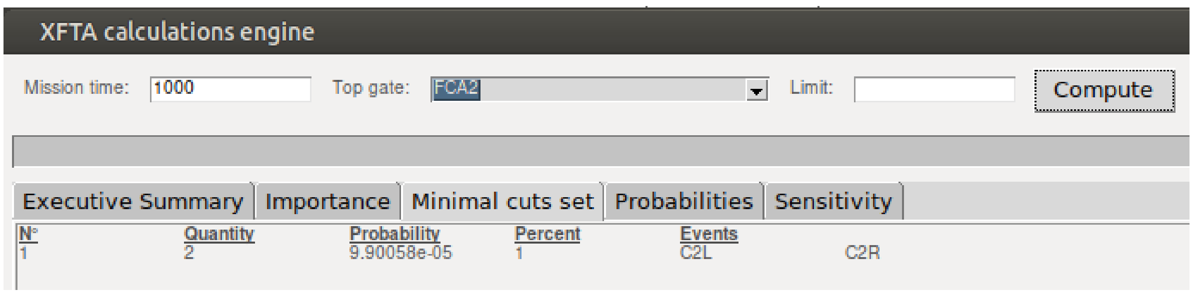


Figure 5: Solution 1 - the Minimal Cut Sets for FC_{A_2}

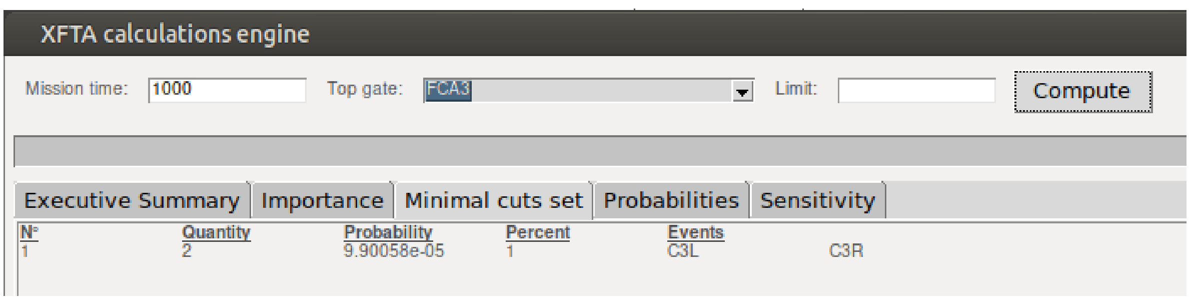


Figure 6: Solution 1 - the Minimal Cut Sets for FC_{A_3}

3. The mean failure rate of FC_{A_i} and FC_One_Appli is:

$$mean_{FC\_One\_Appli} = \frac{Q}{T} = \frac{3.10^{-4}}{1000} = 3.10^{-7}$$

$$\forall i \in \{1,2,3\}, \quad mean_{FC_{A_i}} = \frac{Q}{T} = \frac{9,9.10^{-5}}{1000} = 9,9.10^{-8}$$

4. The qualitative and quantitative requirements are not enforced for failure conditions FC_{A_i} and FC_One_Appli, because the order is equal to 2 (Qualitative) and the mean failure rate is greater than 10^{-9}.

3 Computing Platform Design – solution 2

Figure 2 describes the solution 2 for the computing platform design. In this solution the application fails if its computer fails except for task A_{1L} (resp. A_{3R}) that fails if both the computers C_{1L} and C_{1Lb} (resp. C_{3R}

and C_{3Rb}) fail.

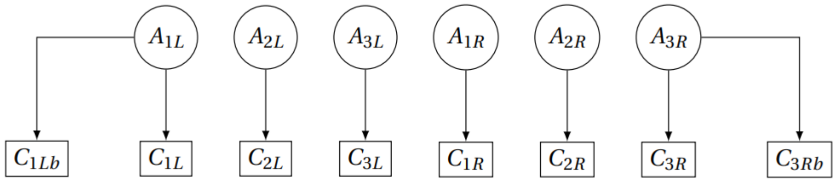


Figure 7: Solution 2 - backup computers for tasks A_{1L} and A_{3R}

Question 3

1. The fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.

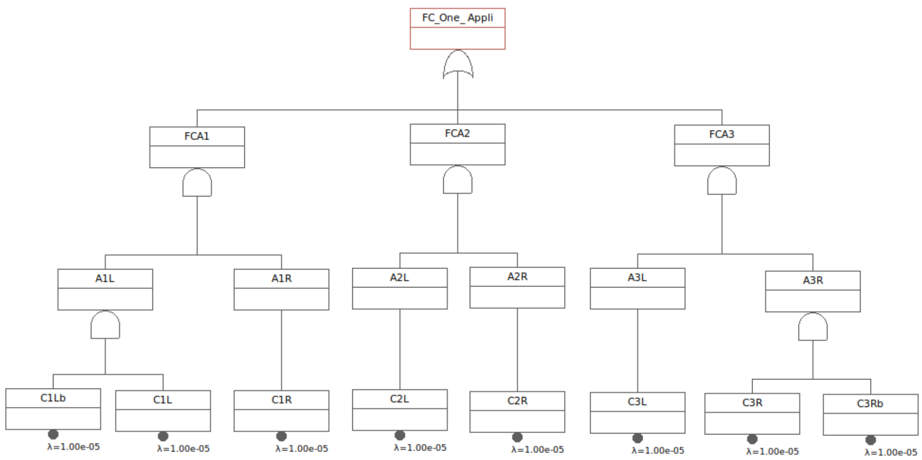


Figure 8: Solution 2 - The fault-tree

2. the Minimal Cut Sets for FC_{A_i} and FC_One_Appli is:

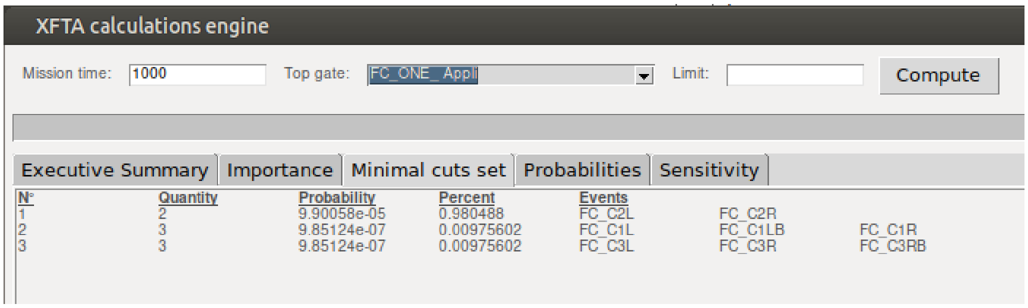


Figure 9: Solution 2 - the Minimal Cut Sets for FC_One_Appli

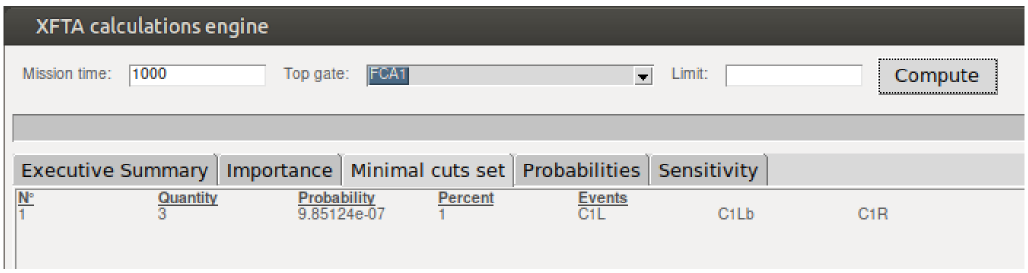


Figure 10: Solution 2 - the Minimal Cut Sets for FC_{A_1}

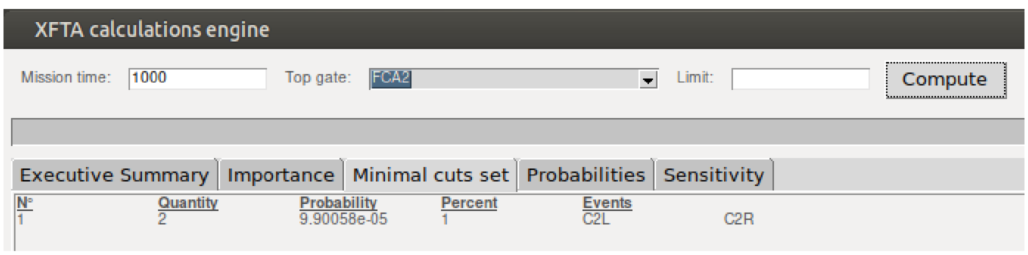


Figure 11: Solution 2 - the Minimal Cut Sets for FC_{A_2}

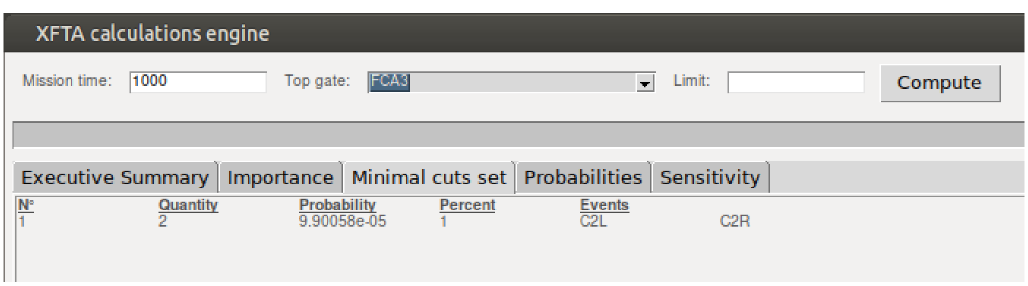


Figure 12: Solution 2 - the Minimal Cut Sets for FC_{A_3}

3. The mean failure rate of FC_{A_i} and FC_One_Appli is:

$$mean_{FC\_One\_Appli} = \frac{Q}{T} = \frac{1.10^{-4}}{1000} = 1.10^{-7}$$

$$mean_{FC_{A_2}} = \frac{Q}{T} = \frac{9,9.10^{-5}}{1000} = 9,9.10^{-8}$$

$$\forall i \in \{1, 3\}, \quad mean_{FC_{A_i}} = \frac{Q}{T} = \frac{9,9.10^{-7}}{1000} = 9,9.10^{-10}$$

4. The qualitative and quantitative requirements are not enforced for failure conditions FC_{A_2} and FC_One_Appli, because $order \geq 2$ (Qualitative) and the mean failure rate is greater than 10^{-9}.
   On the other hand, The qualitative and quantitative requirements are enforced for failure conditions FC_{A_2} and FC_{A_3}, because $order = 3$ (Qualitative) and the mean failure rate is less than 10^{-9}.

4 Computing Platform Design – solution 3

The solution 3 of the computing platform design is described by the figure 3. In this solution the application fails if its computer fails and if the spare computer Sp_L (resp. Sp_R) cannot be used as a backup. The spare Sp_L (resp. Sp_R) can be used by:

- A_{1L} (resp. A_{1R}) if C_{1L} (resp. C_{1R}) fails,
- A_{2L} (resp. A_{2R}) if C_{2L} (resp. C_{2R}) fails and not used by A_{1L} (resp. A_{1R}),
- A_{3L} (resp. A_{3R}) if C_{3L} (resp. C_{3R}) fails and not used by A_{1L} or A_{2L} (resp. A_{1R} or A_{2R}).

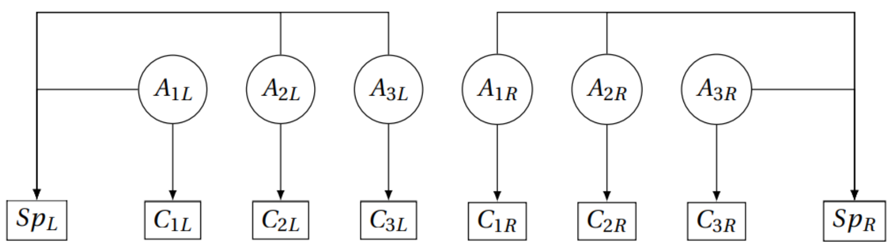


Figure 13: Solution 3 - one computer per task and one spare per side

Question 4

1. The fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.

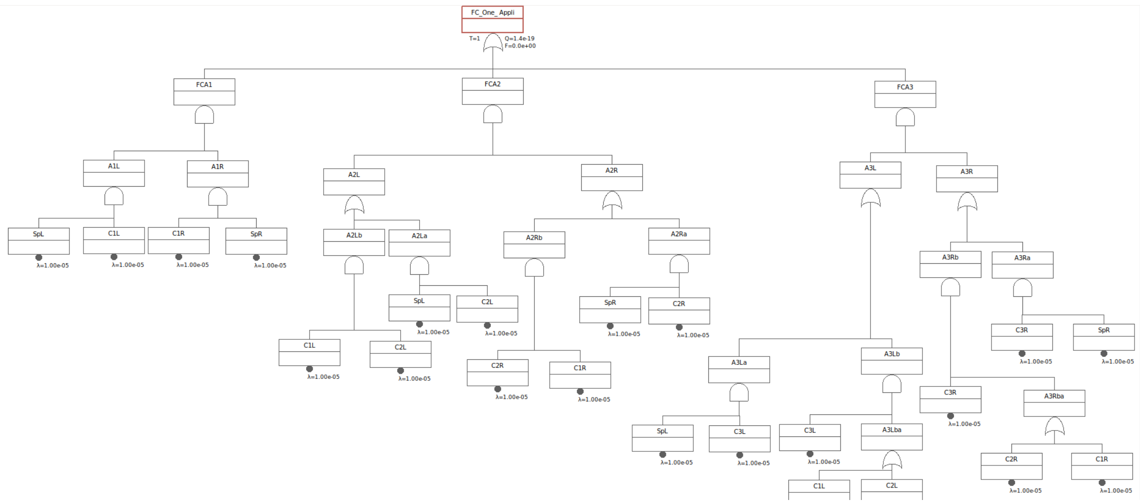
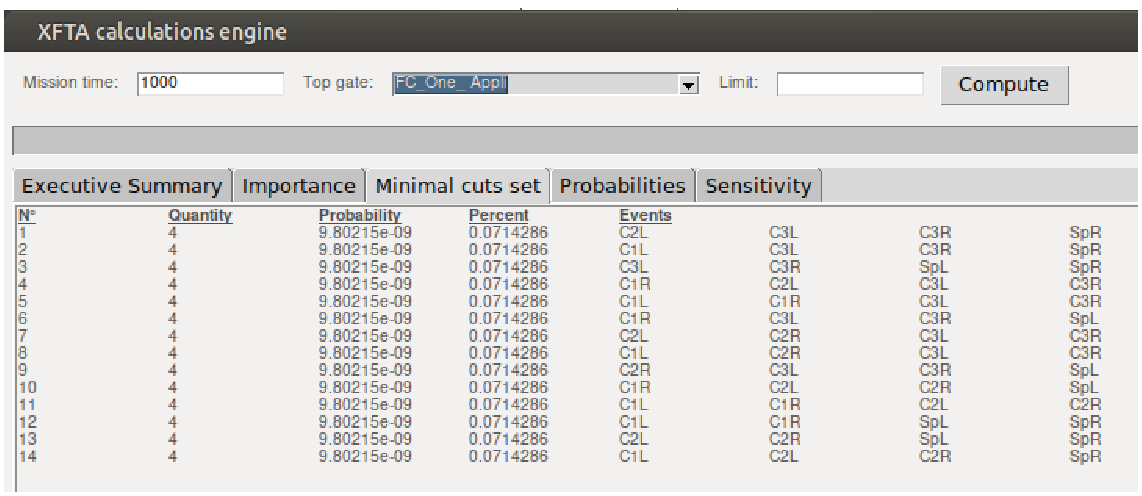


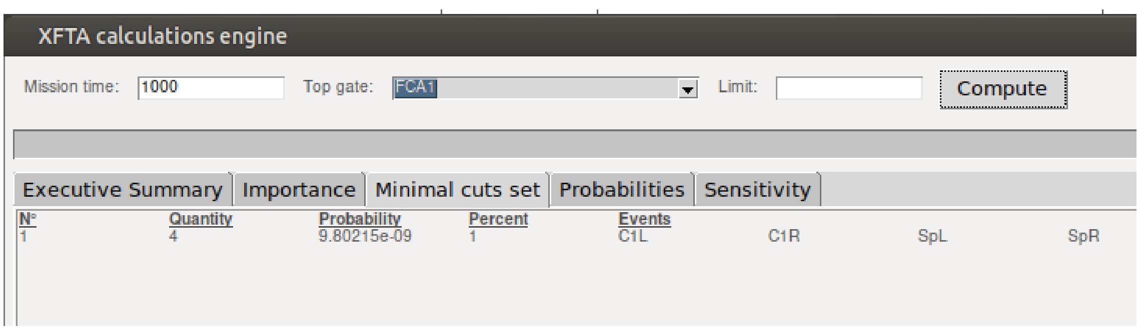
Figure 14: Solution 3 - The fault-tree

2. the Minimal Cut Sets for FC_{A_i} and FC_One_Appli is:



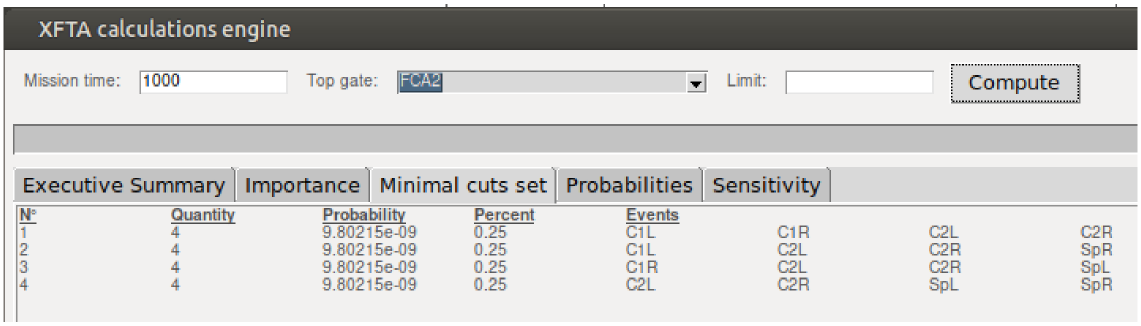
N°	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	0.0714286	C2L	C3L	C3R	SpR
2	4	9.80215e-09	0.0714286	C1L	C3L	C3R	SpR
3	4	9.80215e-09	0.0714286	C3L	C3R	SpL	SpR
4	4	9.80215e-09	0.0714286	C1R	C2L	C3L	C3R
5	4	9.80215e-09	0.0714286	C1L	C1R	C3L	C3R
6	4	9.80215e-09	0.0714286	C1R	C3L	C3R	SpL
7	4	9.80215e-09	0.0714286	C2L	C2R	C3L	C3R
8	4	9.80215e-09	0.0714286	C1L	C2R	C3L	C3R
9	4	9.80215e-09	0.0714286	C2R	C3L	C3R	SpL
10	4	9.80215e-09	0.0714286	C1R	C2L	C2R	SpL
11	4	9.80215e-09	0.0714286	C1L	C1R	C2L	C2R
12	4	9.80215e-09	0.0714286	C1L	C1R	SpL	SpR
13	4	9.80215e-09	0.0714286	C2L	C2R	SpL	SpR
14	4	9.80215e-09	0.0714286	C1L	C2L	C2R	SpR

Figure 15: Solution 3 - the Minimal Cut Sets for FC_One_Appli



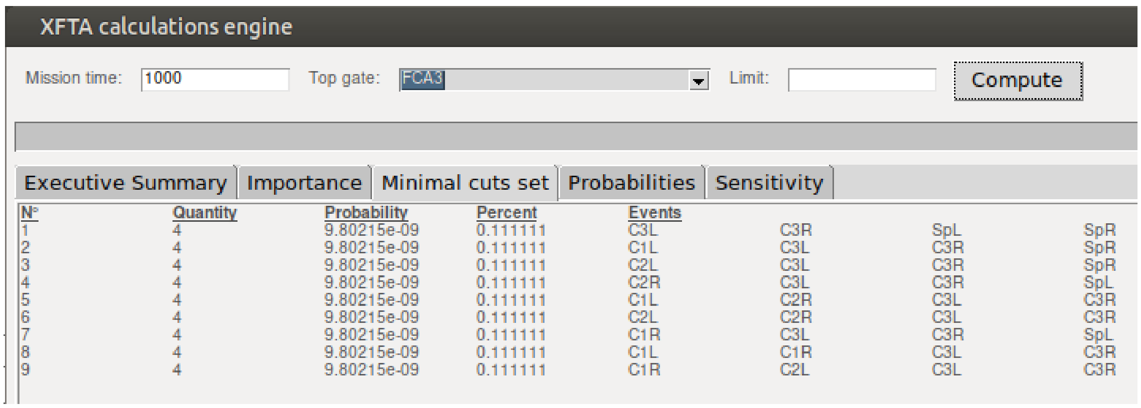
N°	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	1	C1L	C1R	SpL	SpR

Figure 16: Solution 3 - the Minimal Cut Sets for FC_{A_1}



N°	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	0.25	C1L	C1R	C2L	C2R
2	4	9.80215e-09	0.25	C1L	C2L	C2R	SpR
3	4	9.80215e-09	0.25	C1R	C2L	C2R	SpL
4	4	9.80215e-09	0.25	C2L	C2R	SpL	SpR

Figure 17: Solution 3 - the Minimal Cut Sets for FC_{A_2}



N°	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	0.111111	C3L	C3R	SpL	SpR
2	4	9.80215e-09	0.111111	C1L	C3L	C3R	SpR
3	4	9.80215e-09	0.111111	C2L	C3L	C3R	SpR
4	4	9.80215e-09	0.111111	C2R	C3L	C3R	SpL
5	4	9.80215e-09	0.111111	C1L	C2R	C3L	C3R
6	4	9.80215e-09	0.111111	C2L	C2R	C3L	C3R
7	4	9.80215e-09	0.111111	C1R	C3L	C3R	SpL
8	4	9.80215e-09	0.111111	C1L	C1R	C3L	C3R
9	4	9.80215e-09	0.111111	C1R	C2L	C3L	C3R

Figure 18: Solution 3 - the Minimal Cut Sets for FC_{A_3}

3. The mean failure rate of FC_{A_i} and FC_One_Appli is:

$$mean_{FC\_One\_Appli} = \frac{Q}{T} = \frac{1,4.10^{-7}}{1000} = 1,4.10^{-10}$$

$$mean_{FC_{A_1}} = \frac{Q}{T} = \frac{9,8.10^{-9}}{1000} = 9,8.10^{-12}$$

$$mean_{FC_{A_2}} = \frac{Q}{T} = \frac{3,9.10^{-8}}{1000} = 3,9.10^{-11}$$

$$mean_{FC_{A_3}} = \frac{Q}{T} = \frac{8,8.10^{-8}}{1000} = 8,8.10^{-11}$$

4. The qualitative and quantitative requirements are enforced for failure conditions FC_{A_i} and FC_One_Appli, because the order is equal to 4 (Qualitative) and the mean failure rate is less than 10^{-9}.

5 Computing Platform Design – DAL Allocation

The group of Basic Computers is independent from Spare Computers:

- Basic Computers $= C_{1L}, C_{2L}, C_{3L}, C_{1Lb}, C_{1R}, C_{2R}, C_{3R}, C_{3Rb}$
- Spare Computers $= Sp_L, Sp_R$

Within a group Basic or Spare, all computers are dependent.

Question 5 Knowing the independent group, for each solution complete the DAL allocation table 1 to allocate a DAL to the computers of the platform.

The DAL allocation for solution 1

FC	INITIAL DAL	MCS	C_{1L}	C_{2L}	C_{3L}	C_{1R}	C_{2R}	C_{3R}
FC_A_1	A	$\{C_{1R}, C_{1L}\}$	A			A		
FC_A_2	A	$\{C_{2R}, C_{2L}\}$		A			A	
FC_A_3	A	$\{C_{3R}, C_{3L}\}$						A
FC_One_Appli	A	$\{C_{1R}, C_{1L}\}$	A			A		
		$\{C_{2R}, C_{2L}\}$		A			A	
		$\{C_{3R}, C_{3L}\}$			A			A
Final			A	A	A	A	A	A

The DAL allocation for solution 2

FC	INITIAL DAL	MCS	C_{1L}	C_{2L}	C_{3L}	C_{1LB}	C_{1R}	C_{2R}	C_{3R}	C_{3RB}
FC_A_1	A	$\{C_{1R}, C_{1L}, C_{1LB}\}$	A			A	A			
FC_A_2	A	$\{C_{2R}, C_{2L}\}$		A				A		
FC_A_3	A	$\{C_{3R}, C_{3L}, C_{3RB}\}$			A				A	A
FC_One_Appli	A	$\{C_{1R}, C_{1L}, C_{1LB}\}$	A			A	A			
		$\{C_{2R}, C_{2L}\}$		A				A		
		$\{C_{3R}, C_{3L}, C_{3RB}\}$			A				A	A
Final			A	A	A	A	A	A	A	A

The DAL allocation for solution 3

FC	INITIAL DAL	MCS	C_{1L}	C_{2L}	C_{3L}	C_{1R}	C_{2R}	C_{3R}	Sp_L	Sp_R
FC_A_1	A	$\{C_{1R}, C_{1L}, Sp_L, Sp_R\}$	A			A			C	C
FC_A_2	A	$\{C_{1L}, C_{1R}, C_{2L}, C_{2R}\}$	A	A		A	A			
		$\{C_{1R}, C_{2L}, C_{2R}, Sp_L\}$		A		A	A		C	
		$\{C_{1L}, C_{2L}, C_{2R}, Sp_R\}$	A	A			A			C
		$\{C_{2L}, C_{2R}, Sp_L, Sp_R\}$		A			A		C	C
FC_A_3	A	$\{C_{2L}, C_{3L}, C_{3R}, Sp_L\}$		A	A			A	C	
		$\{C_{2L}, C_{2R}, C_{3L}, C_{3R}\}$		A	A		A	A		
		$\{C_{1R}, C_{2L}, C_{3L}, C_{3R}\}$		A	A	A		A		
		$\{C_{1L}, C_{3L}, C_{3R}, Sp_R\}$	A		A			A		C
		$\{C_{1L}, C_{2R}, C_{3L}, C_{3R}\}$	A		A		A	A		
		$\{C_{1L}, C_{1R}, C_{3L}, C_{3R}\}$	A		A	A		A		
		$\{C_{3L}, C_{3R}, Sp_L, Sp_R\}$			A			A	C	C
		$\{C_{2R}, C_{3L}, C_{3R}, Sp_L\}$			A		A	A	C	
		$\{C_{1R}, C_{3L}, C_{3R}, Sp_L\}$			A	A		A	C	
FC_One_Appli	A	$\{C_{1R}, C_{1L}, Sp_L, Sp_R\}$	A			A			C	C
		$\{C_{1L}, C_{1R}, C_{2L}, C_{2R}\}$	A	A		A	A			
		$\{C_{1R}, C_{2L}, C_{2R}, Sp_L\}$		A		A	A		C	
		$\{C_{1L}, C_{2L}, C_{2R}, Sp_R\}$	A	A			A			C
		$\{C_{2L}, C_{2R}, Sp_L, Sp_R\}$		A			A		C	C
		$\{C_{2L}, C_{3L}, C_{3R}, Sp_L\}$		A	A			A	C	
		$\{C_{2L}, C_{2R}, C_{3L}, C_{3R}\}$		A	A		A	A		
		$\{C_{1R}, C_{2L}, C_{3L}, C_{3R}\}$		A	A	A		A		
		$\{C_{1L}, C_{3L}, C_{3R}, Sp_R\}$	A		A			A		C
		$\{C_{1L}, C_{2R}, C_{3L}, C_{3R}\}$	A		A		A	A		
		$\{C_{1L}, C_{1R}, C_{3L}, C_{3R}\}$	A		A	A		A		
		$\{C_{3L}, C_{3R}, Sp_L, Sp_R\}$			A			A	C	C
		$\{C_{2R}, C_{3L}, C_{3R}, Sp_L\}$			A		A	A	C	
		$\{C_{1R}, C_{3L}, C_{3R}, Sp_L\}$			A	A		A	C	
Final			A	A	A	A	A	A	C	C

6 Computing Platform Design – Failed components

It is not possible to repair failed components in any airport so it should be possible to fly the aircraft safely with some components failed.
Question 6 Duplicate the table 2 in your report and complete :

- The first one considering the qualitative requirement (i.e. satisfy FC_One_appl i order bound);
- The second one considering the quantitative requirement (i.e. satisfy FC_One_appl i mean failure rate bound).

For the qualitative part, if it needs 2 more components to fail it's OK, otherwise KO. For the

Solution	C_{1L}	C_{2L}	C_{3L}	C_{1R}	C_{2R}	C_{3R}	C_{1LB}	C_{3RB}	Sp_L	Sp_R
1	KO	KO	KO	KO	KO	KO				
2	OK	KO	OK	OK	KO	OK	OK	OK		
3	OK	OK	OK	OK	OK	OK			OK	OK

quantitative part, we set the probability of failure to 1 then calculate the mean failure rate again, if $\overline{\Lambda} \leq 10^{-9}$ it's OK, otherwise KO.

Solution	C_{1L}	C_{2L}	C_{3L}	C_{1R}	C_{2R}	C_{3R}	C_{1LB}	C_{3RB}	Sp_L	Sp_R
1	KO $[10^{-5}]$	KO $[10^{-5}]$	KO $[10^{-5}]$	KO $[10^{-5}]$	KO $[10^{-5}]$	KO $[10^{-5}]$				
2	KO $[2.10^{-7}]$	KO $[10^{-5}]$	KO $[2.10^{-7}]$	KO $[2.10^{-7}]$	KO $[10^{-5}]$	KO $[2.10^{-7}]$	KO $[2.10^{-7}]$	KO $[2.10^{-7}]$		
3	KO $[6.10^{-9}]$	KO $[7.10^{-9}]$	KO $[8,9.10^{-9}]$	KO $[6.10^{-9}]$	KO $[7.10^{-9}]$	KO $[8,9.10^{-9}]$			KO $[6.10^{-9}]$	KO $[6.10^{-9}]$

It is not possible to fly safely with one computer failed according to the last 2 tables.

7 Computing Platform Design – Comparison

We suppose that the cost of a solution mainly depends on the number of computers and their associated DAL (i.e. costs are: $DALA = 20$, $DALB = 15$, $DALC = 5$; $DALD = 4$; $DALE = 0$).

Question 7 Copy and complete the table 3 to compare the three solutions with respect to their cost, safety and its capability to fly with a faulty computer. What is your preferred solution? Can you imagine a better solution? The last solution is more safe, but it's so expensive, so to enhance the efficiency of this

Solution	Qualitative	Quantitative	acceptable with failed component	cost
1	OK	KO	KO	120
2	OK	KO	KO	160
3	OK	OK	KO	130

solution, Increasing the backup infrastructure is a good solution but increasing the backup size is linked directly with the increasing the cost.