System Dependability Lab
Exercises on Safety Assessment of Static Systems

Guohao DAI

Friday 28th October, 2022

1. Introduction

I have studied and compared three Computing Platform Designs that should 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. We are interested in the following Failure Conditions:

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?
Response: The reason of all the FC are classified *CATASTROPHIC*, the qualitative and quantitative safety requirements associated to the FCs are:

Criticality	Qualitative requirement	Quantitative requirement
CATASTROPHIC	$order \geq 2$	$\overline{\Lambda} \leq 10^{-9}$ / $flight\ hour$

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 $\lambda = 10^{-5}.h^{-1}$.

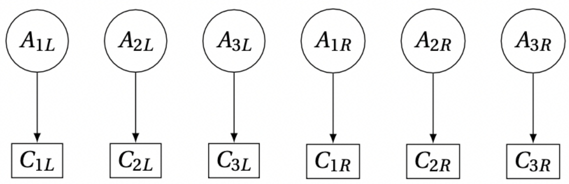
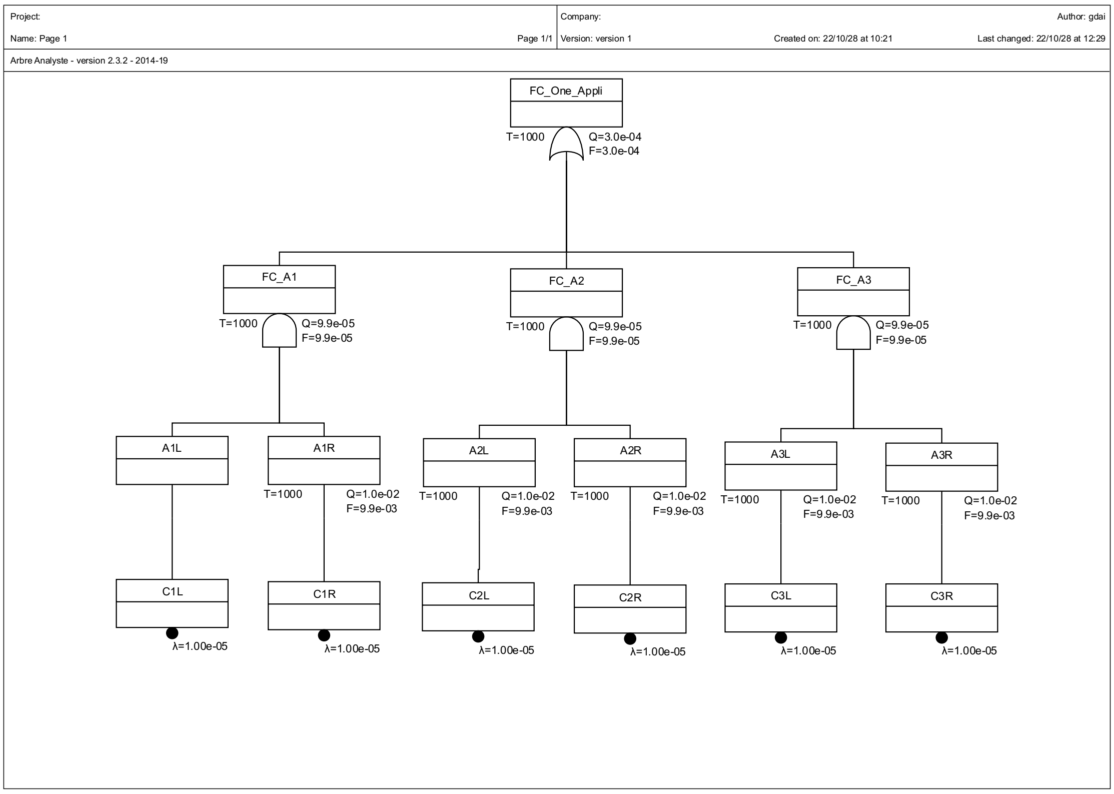


Figure 1: Solution 1 - one computer per task

Question 2

1. Create a new file and build the fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.



2. Compute the ***Minimal Cut Sets*** for FC_{A_i} and FC_One_Appli.

(1) The ***Minimal Cut Sets*** for FC_One_Appli:

No.	Quantity	Probability	Percent	Events	
1	2	9.90058e-05	0.333333	C3L	C3R
2	2	9.90058e-05	0.333333	C2L	C2R
3	2	9.90058e-05	0.333333	C1L	C1R

(2) The ***Minimal Cut Sets*** for FC_{A_1}:

No.	Quantity	Probability	Percent	Events	
1	2	9.90058e-05	1	C1L	C1R

(3) The ***Minimal Cut Sets*** for FC_{A_2}:

No.	Quantity	Probability	Percent	Events	
1	2	9.90058e-05	1	C2L	C2R

(4) The ***Minimal Cut Sets*** for FC_{A_3}:

No.	Quantity	Probability	Percent	Events	
1	2	9.90058e-05	1	C3L	C3R

3. Compute the ***mean failure rate*** of FC_{A_i} and FC_One_Appli.

(1) The ***mean failure rate*** of FC_One_Appli is:

$$\overline{\Lambda}_{One\_Appli} = \frac{P(FC_{A_1}) + P(FC_{A_2}) + P(FC_{A_3})}{T} = 3 \times \frac{9.90 \times 10^{-5}}{10^3} \approx 3 \times 10^{-7}$$

(2) The ***mean failure rate*** of FC_{A_i} is:

$$\overline{\Lambda}_{FC_{A_1}} = \frac{P(FC_{A_1})}{T} \approx \frac{9.90 \times 10^{-5}}{10^3} = 9.90 \times 10^{-8} \approx 10^{-7}$$

$$\overline{\Lambda}_{FC_{A_2}} = \frac{P(FC_{A_2})}{T} \approx \frac{9.90 \times 10^{-5}}{10^3} = 9.90 \times 10^{-8} \approx 10^{-7}$$

$$\overline{\Lambda}_{FC_{A_3}} = \frac{P(FC_{A_3})}{T} \approx \frac{9.90 \times 10^{-5}}{10^3} = 9.90 \times 10^{-8} \approx 10^{-7}$$

4. Are the Qualitative and Quantitative requirements enforced for failure conditions FC_{A_i} and FC_One_Appli? Justify the answer.

Response:

The Qualitative and Quantitative requirements are not enforced for failure conditions FC_{A_i} and FC_One_Appli. Because **the order of each FC equals 2** $(= \mathbf{2})$ and **mean failure rate $\overline{\boldsymbol{\Lambda}}$ is more than $\mathbf{10^{-9}}$** $(\geq \mathbf{10^{-9}})$.

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.

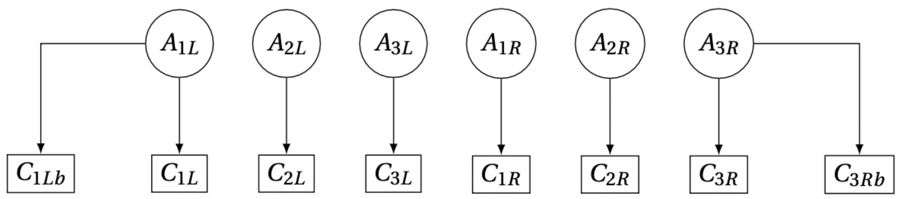
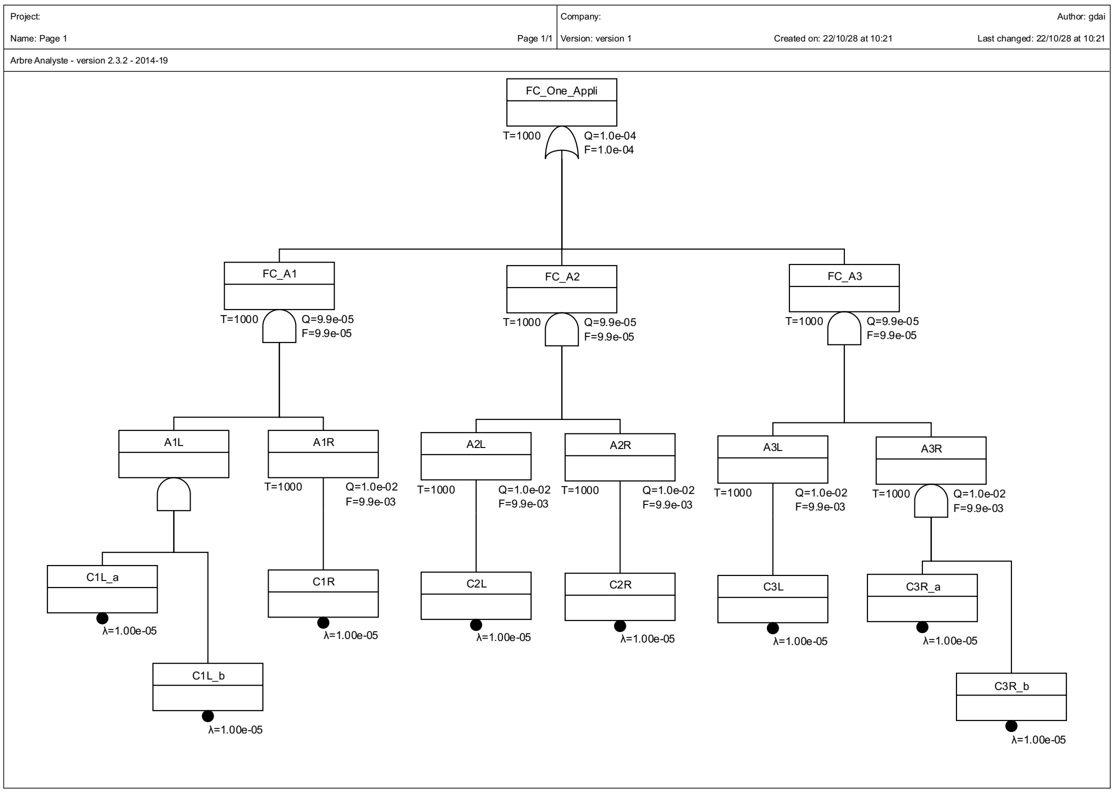


Figure 2: Solution 2 - backup computers for tasks A_{1L} and A_{3R}

Question 3

1. Create a new file and build the fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.



2. Compute the ***Minimal Cut Sets*** for FC_{A_i} and FC_One_Appli.

(1) The ***Minimal Cut Sets*** for FC_One_Appli:

No.	Quantity	Probability	Percent	Events		
1	2	9.90058e-05	0.980488	C2L	C2R	
2	3	9.85124e-07	0.00975602	C3L	C3R_a	C3R_b
3	3	9.85124e-07	0.00975602	C1L_a	C1L_b	C1R

(2) The ***Minimal Cut Sets*** for FC_{A_1}:

No.	Quantity	Probability	Percent	Events		
1	3	9.85124e-07	1	C1L_a	C1L_b	C1R

(3) The ***Minimal Cut Sets*** for FC_{A_2}:

No.	Quantity	Probability	Percent	Events		
1	2	9.90058e-05	1	C2L	C2R	

(4) The ***Minimal Cut Sets*** for FC_{A_3}:

No.	Quantity	Probability	Percent	Events		
1	3	9.85124e-07	1	C3L	C3R_a	C3R_b

3. Compute the ***mean failure rate*** of FC_{A_i} and FC_One_Appli.

(1) The ***mean failure rate*** of FC_One_Appli is:

$$\overline{\Lambda}_{One\_Appli} = \frac{P(FC_{A_1}) + P(FC_{A_2}) + P(FC_{A_3})}{T} \approx \frac{P(FC_{A_2})}{T} \approx 10^{-7}$$

(2) The ***mean failure rate*** of FC_{A_i} is:

$$\bar{\Lambda}_{FC_{A_1}} = \frac{P(FC_{A_1})}{T} \approx \frac{9.85 \times 10^{-7}}{10^3} = 9.85 \times 10^{-10} \approx 10^{-9}$$

$$\bar{\Lambda}_{FC_{A_2}} = \frac{P(FC_{A_2})}{T} \approx \frac{9.90 \times 10^{-5}}{10^3} = 9.90 \times 10^{-8} \approx 10^{-7}$$

$$\bar{\Lambda}_{FC_{A_3}} = \frac{P(FC_{A_3})}{T} \approx \frac{9.85 \times 10^{-7}}{10^3} = 9.85 \times 10^{-10} \approx 10^{-9}$$

4. Are the Qualitative and Quantitative requirements enforced for failure conditions FC_{A_i} and FC_One_Appli? Justify the answer.

Response:

- The Qualitative and Quantitative requirements are not enforced for failure conditions FC_{A_2} and FC_One_Appli. Because the **order of FC_{A_2} and FC_One_Appli are both equal 2**, moreover, **their mean failure rate $\bar{\Lambda}$ is more than 10^{-9}.**
- The Qualitative and Quantitative requirements are enforced for failure conditions FC_{A_1} and FC_{A_3}. Because **the order of each FC equals 3 (≥ 2)** and **mean failure rate $\bar{\Lambda}$ is less than 10^{-9} ($\leq 10^{-9}$).**

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 S_{pL} (resp. S_{pR}) cannot be used as a backup. The spare S_{pL} (resp. S_{pR}) 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}).

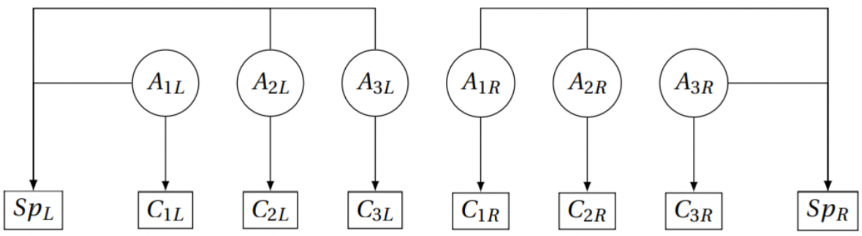
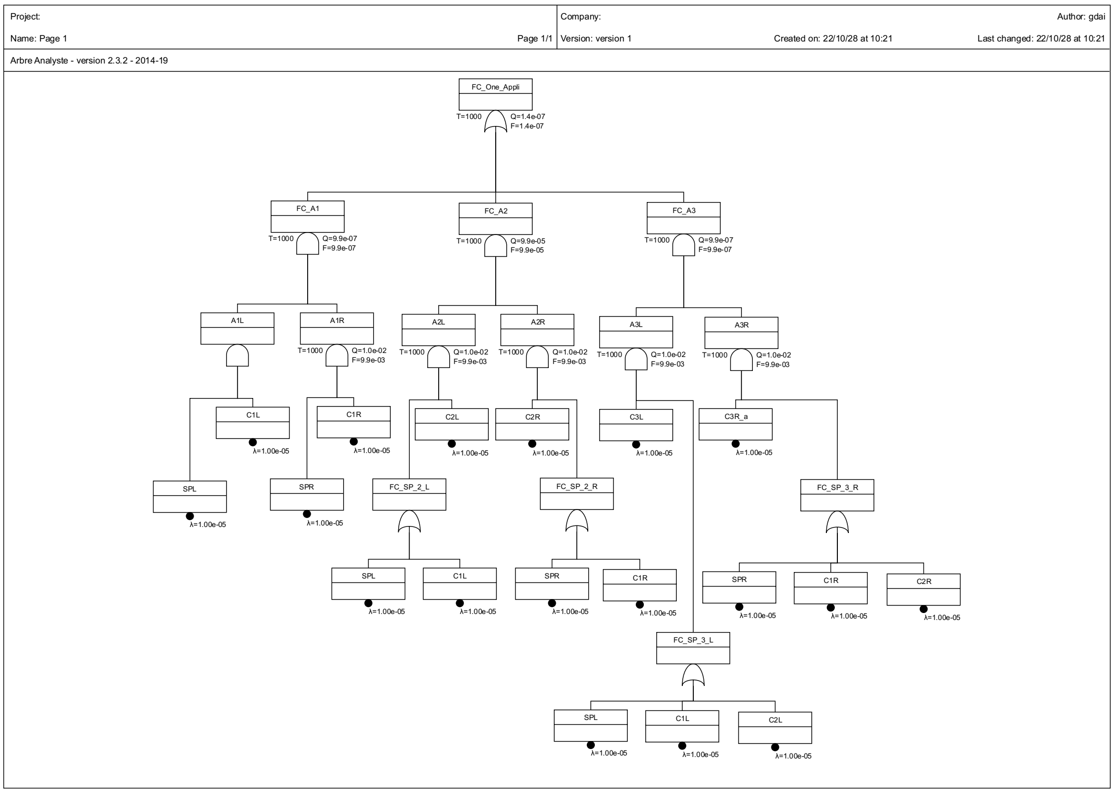


Figure 13: Solution 3 - one computer per task and one spare per side

Question 4.

1. Create a new file and build the fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.



2. Compute the ***Minimal Cut Sets*** for FC_{A_i} and FC_One_Appli.

(1) The ***Minimal Cut Sets*** for FC_One_Appli:

No.	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	0.0714286	C2L	C2R	SPL	SPR
2	4	9.80215e-09	0.0714286	C1R	C2L	C2R	SPL
3	4	9.80215e-09	0.0714286	C1L	C2L	C2R	SPR
4	4	9.80215e-09	0.0714286	C1L	C1R	C2L	C2R
5	4	9.80215e-09	0.0714286	C2L	C2R	C3L	C3R_a
6	4	9.80215e-09	0.0714286	C2R	C3L	C3R_a	SPL
7	4	9.80215e-09	0.0714286	C1L	C2R	C3L	C3R_a
8	4	9.80215e-09	0.0714286	C1L	C1R	SPL	SPR
9	4	9.80215e-09	0.0714286	C1L	C3L	C3R_a	SPR
10	4	9.80215e-09	0.0714286	C1L	C1R	C3L	C3R_a
11	4	9.80215e-09	0.0714286	C3L	C3R_a	SPL	SPR
12	4	9.80215e-09	0.0714286	C1R	C3L	C3R_a	SPL
13	4	9.80215e-09	0.0714286	C2L	C3L	C3R_a	SPR
14	4	9.80215e-09	0.0714286	C1R	C2L	C3L	C3R_a

(2) The ***Minimal Cut Sets*** for FC_{A_1}:

No.	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	1	C1L	C1R	SPL	SPR

(3) The ***Minimal Cut Sets*** for FC_{A_2}:

No.	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	0.25	C2L	C2R	SPL	SPR
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	C1L	C1R	C2L	C2R

(4) The ***Minimal Cut Sets*** for FC_{A_3}:

No.	Quantity	Probability	Percent	Events			
1	4	9.80215e-09	0.1111111	C2L	C2R	C3L	C3R_a
2	4	9.80215e-09	0.1111111	C2R	C3L	C3R_a	SPL
3	4	9.80215e-09	0.1111111	C1L	C2R	C3L	C3R_a
4	4	9.80215e-09	0.1111111	C1L	C3L	C3R_a	SPR
5	4	9.80215e-09	0.1111111	C1L	C1R	C3L	C3R_a
6	4	9.80215e-09	0.1111111	C3L	C3R_a	SPL	SPR
7	4	9.80215e-09	0.1111111	C1R	C3L	C3R_a	SPL
8	4	9.80215e-09	0.1111111	C2L	C3L	C3R_a	SPR
9	4	9.80215e-09	0.1111111	C1R	C2L	C3L	C3R_a

3. Compute the ***mean failure rate*** of FC_{A_i} and FC_One_Appli.

(1) The ***mean failure rate*** of FC_One_Appli is:

$$\overline{\Lambda}_{One\_Appli} = \frac{P(FC_{A_1}) + P(FC_{A_2}) + P(FC_{A_3})}{T} \approx 14 \times \frac{9.80 \times 10^{-9}}{T} \approx 1.4 \times 10^{-10}$$

(2) The ***mean failure rate*** of FC_{A_i} is:

$$\overline{\Lambda}_{FC_{A_1}} = \frac{P(FC_{A_1})}{T} \approx \frac{9.80 \times 10^{-9}}{10^3} = 9.80 \times 10^{-12}$$

$$\overline{\Lambda}_{FC_{A_2}} = \frac{P(FC_{A_2})}{T} \approx 4 \times \frac{9.80 \times 10^{-9}}{10^3} = 3.92 \times 10^{-11}$$

$$\overline{\Lambda}_{FC_{A_3}} = \frac{P(FC_{A_3})}{T} \approx 9 \times \frac{9.80 \times 10^{-9}}{10^3} = 8.82 \times 10^{-11}$$

4. Are the Qualitative and Quantitative requirements enforced for failure conditions FC_{A_i} and FC_One_Appli? Justify the answer.

Response:

The Qualitative and Quantitative requirements are enforced for failure conditions FC_{A_i} and FC_One_Appli. Because **the order of each FC equals 4** (**≥ 2**) and **mean failure rate $\overline{\Lambda}$ is less than 10^{-9}** (**$\leq 10^{-9}$**).

5. Computing Platform Design – DAL Allocation

The group of Basic Computers is independent from Spare Computers:

$$BasicComputers = \{C_{1L}, C_{2L}, C_{3L}, C_{1Lb}, C_{1R}, C_{2R}, C_{3R}, C_{3Rb}\}$$
$$SpareComputers = \{S_{pL}, S_{pR}\}$$

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.

Severity (FC)	**DAL(FC)**	**Acceptable Frequency** (Order of Magnitude)
CAT	A	10^{-9}
HAZ	B	10^{-7}
MAL	C	10^{-5}
MIN	D	10^{-3}
NSE	E	-

Table – Link between severity and DAL

(1) The DAL allocation table of Solution 1:

FC	**Initial DAL**	**MCS**	**Components**					
			C_{1L}	C_{2L}	C_{3L}	C_{1R}	C_{2R}	C_{3R}
$\boldsymbol{FC_{A_1}}$	A	$\{C_{1L}, C_{1R}\}$	$\geq A$	-	-	$\geq A$	-	-
$\boldsymbol{FC_{A_2}}$	A	$\{C_{2L}, C_{2R}\}$	-	$\geq A$	-	-	$\geq A$	-
$\boldsymbol{FC_{A_3}}$	A	$\{C_{3L}, C_{3R}\}$	-	-	$\geq A$	-	-	$\geq A$
$\boldsymbol{FC\_One\_Appli}$	A	$\{C_{1L}, C_{1R}\}$	$\geq A$	-	-	$\geq A$	-	-
		$\{C_{2L}, C_{2R}\}$	-	$\geq A$	-	-	$\geq A$	-
		$\{C_{3L}, C_{3R}\}$	-	-	$\geq A$	-	-	$\geq A$
Final			$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$

(2) The DAL allocation table of Solution 2:

FC	**Initial DAL**	**MCS**	**Components**							
			C_{1L}	C_{2L}	C_{3L}	C_{1L_b}	C_{1R}	C_{2R}	C_{3R}	C_{3R_b}
$\boldsymbol{FC_{A_1}}$	A	$\{C_{1L}, C_{1R}, C_{1L\_b}\}$	$\geq A$	-	-	$\geq A$	$\geq A$	-	-	-
$\boldsymbol{FC_{A_2}}$	A	$\{C_{2L}, C_{2R}\}$	-	$\geq A$	-	-	-	$\geq A$	-	-
$\boldsymbol{FC_{A_3}}$	A	$\{C_{3L}, C_{3R}, C_{3R\_b}\}$	-	-	$\geq A$	-	-	-	$\geq A$	$\geq A$
$\boldsymbol{FC\_One\_Appli}$	A	$\{C_{1L}, C_{1R}, C_{1L\_b}\}$	$\geq A$	-	-	$\geq A$	$\geq A$	-	-	-
		$\{C_{2L}, C_{2R}\}$		$\geq A$	-	-	-	$\geq A$	-	-
		$\{C_{3L}, C_{3R}, C_{3R\_b}\}$	-	-	$\geq A$	-	-	-	$\geq A$	$\geq A$
Final			$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$

(3) The DAL allocation table of Solution 3:

FC	Initial DAL	MCS	Components							
			C_{1L}	C_{2L}	C_{3L}	C_{1R}	C_{2R}	C_{3R_a}	S_{pL}	S_{pR}
$\boldsymbol{FC_{A_1}}$	A	$\{C_{1L}, C_{1R}, S_{pL}, S_{pR}\}$	$\geq A$	-	-	$\geq A$	-	-	$\geq C$	$\geq C$
$\boldsymbol{FC_{A_2}}$	A	$\{C_{2L}, C_{2R}, S_{pL}, S_{pR}\}$	-	$\geq A$	-	-	$\geq A$	-	$\geq C$	$\geq C$
		$\{C_{1L}, C_{2L}, C_{2R}, S_{pR}\}$	$\geq A$	$\geq A$	-	-	$\geq A$	-	-	$\geq C$
		$\{C_{1R}, C_{2L}, C_{2R}, S_{pL}\}$	-	$\geq A$	-	$\geq A$	$\geq A$	-	$\geq C$	-
		$\{C_{1L}, C_{1R}, C_{2L}, C_{2R}\}$	$\geq A$	$\geq A$	-	$\geq A$	$\geq A$	-	-	-
$\boldsymbol{FC_{A_3}}$	A	$\{C_{2L}, C_{2R}, C_{3L}, C_{3R\_a}\}$	-	$\geq A$	$\geq A$	-	$\geq A$	$\geq A$	-	-
		$\{C_{2R}, C_{3L}, C_{3R\_a}, S_{pL}\}$	-	-	$\geq A$	-	$\geq A$	$\geq A$	$\geq C$	-
		$\{C_{1L}, C_{2R}, C_{3L}, C_{3R\_a}\}$	$\geq A$	-	$\geq A$	-	$\geq A$	$\geq A$	-	-
		$\{C_{1L}, C_{3L}, C_{3R\_a}, S_{pR}\}$	$\geq A$	-	$\geq A$	-	-	$\geq A$	-	$\geq C$
		$\{C_{1L}, C_{1R}, C_{3L}, C_{3R\_a}\}$	$\geq A$	-	$\geq A$	$\geq A$	-	$\geq A$	-	-
		$\{C_{3L}, C_{3R\_a}, S_{pL}, S_{pR}\}$	-	-	$\geq A$	-	-	$\geq A$	$\geq C$	$\geq C$
		$\{C_{1R}, C_{3L}, C_{3R\_a}, S_{pL}\}$	-	-	$\geq A$	$\geq A$	-	$\geq A$	$\geq C$	-
		$\{C_{2L}, C_{3L}, C_{3R\_a}, S_{pR}\}$	-	$\geq A$	$\geq A$	-	-	$\geq A$	-	$\geq C$
		$\{C_{1R}, C_{2L}, C_{3L}, C_{3R\_a}\}$	-	$\geq A$	$\geq A$	$\geq A$	-	$\geq A$	-	-
$\boldsymbol{FC\_One\_Appli}$	A	$\{C_{2L}, C_{2R}, S_{pL}, S_{pR}\}$	-	$\geq A$	-	-	$\geq A$	-	$\geq C$	$\geq C$
		$\{C_{1L}, C_{2L}, C_{2R}, S_{pR}\}$	$\geq A$	$\geq A$	-	-	$\geq A$	-	-	$\geq C$
		$\{C_{1R}, C_{2L}, C_{2R}, S_{pL}\}$	-	$\geq A$	-	$\geq A$	$\geq A$	-	$\geq C$	-
		$\{C_{1L}, C_{1R}, C_{2L}, C_{2R}\}$	$\geq A$	$\geq A$	-	$\geq A$	$\geq A$	-	-	-
		$\{C_{2L}, C_{2R}, C_{3L}, C_{3R\_a}\}$	-	$\geq A$	$\geq A$	-	$\geq A$	$\geq A$	-	-
		$\{C_{2R}, C_{3L}, C_{3R\_a}, S_{pL}\}$	-	-	$\geq A$	-	$\geq A$	$\geq A$	$\geq C$	-
		$\{C_{1L}, C_{2R}, C_{3L}, C_{3R\_a}\}$	$\geq A$	-	$\geq A$	-	$\geq A$	$\geq A$	-	-
		$\{C_{1L}, C_{1R}, S_{pL}, S_{pR}\}$	$\geq A$	-	-	$\geq A$	-	-	$\geq C$	$\geq C$
		$\{C_{1L}, C_{3L}, C_{3R\_a}, S_{pR}\}$	$\geq A$	-	$\geq A$	-	-	$\geq A$	-	$\geq C$
		$\{C_{1L}, C_{1R}, C_{3L}, C_{3R\_a}\}$	$\geq A$	-	$\geq A$	$\geq A$	-	$\geq A$	-	-
		$\{C_{3L}, C_{3R\_a}, S_{pL}, S_{pR}\}$	-	-	$\geq A$	-	-	$\geq A$	$\geq C$	$\geq C$
		$\{C_{1R}, C_{3L}, C_{3R\_a}, S_{pL}\}$	-	-	$\geq A$	$\geq A$	-	$\geq A$	$\geq C$	-
		$\{C_{2L}, C_{3L}, C_{3R\_a}, S_{pR}\}$	-	$\geq A$	$\geq A$	-	-	$\geq A$	-	$\geq C$
		$\{C_{1R}, C_{2L}, C_{3L}, C_{3R\_a}\}$	-	$\geq A$	$\geq A$	$\geq A$	-	$\geq A$	-	-
Final			$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq A$	$\geq C$	$\geq C$

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_appli i order bound);
  Response: if (number of components > 2) then ("OK") else ("KO")

Solution	**components**									
	C_{1L}	C_{2L}	C_{3L}	C_{1L_b}	C_{1R}	C_{2R}	C_{3R} / C_{3R_a}	C_{3R_b}	S_{pL}	S_{pR}
1	KO	KO	KO	-	KO	KO	KO	-	-	-
2	OK	KO	OK	OK	OK	KO	KO	OK	-	-
3	OK	OK	OK	-	OK	OK	OK	-	OK	OK

- The second one considering the qualitative requirement (i.e. satisfy FC_One_appli i mean failure rate bound).
  Response: if (mean failure rate $\overline{\Lambda} \leq 10^{-9}$) then ("OK") else ("KO")

Solution		**components**									
		C_{1L}	C_{2L}	C_{3L}	C_{1L_b}	C_{1R}	C_{2R}	C_{3R} / C_{3R_a}	C_{3R_b}	S_{pL}	S_{pR}
1	$\overline{\Lambda}$	10^{-5}	10^{-5}	10^{-5}	-	10^{-5}	10^{-5}	10^{-5}	-	-	-
		KO	KO	KO	-	KO	KO	KO	-	-	-
2	$\overline{\Lambda}$	10^{-7}	10^{-5}	10^{-7}	10^{-7}	10^{-7}	10^{-5}	10^{-7}	10^{-7}	-	-
		KO	KO	KO	KO	KO	KO	KO	KO	-	-
3	$\overline{\Lambda}$	$> 10^{-9}$	$> 10^{-9}$	$> 10^{-9}$	-	$> 10^{-9}$	$> 10^{-9}$	$> 10^{-9}$	-	$> 10^{-9}$	$> 10^{-9}$
	sd	KO	KO	KO	-	KO	KO	KO	-	KO	KO

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: $DAL\_A = 20, DAL\_B = 15, DAL\_C = 5$; $DAL\_D = 4$; $DAL\_E = 0$).

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?

Response:

The table of solution comparison is shown as below:

Solution	**Fulfilled safety requirement**		**Acceptable with failed component**	**Cost**
	Qualitative	**Quantitative**		
1	OK	KO	KO	120
2	OK	KO	KO	160
3	OK	OK	KO	130

From a qualitative and quantitative point of view, it is beneficial to increase the spare node. But it also has a strong correlation with cost.