**System Dependability Lab**

**Exercises on Safety Assessment of Static Systems**

**Guohao DAI**

Friday 28th October, 2022

DDL: 2022/11/19 00:00

**1. Introduction**

I have studied and compared three Computing Platform Designs that should support three applications (, and ). Each application is implemented by two tasks and . The application fails if both tasks and fail. A task fails if all the computers that can host it fail. We are interested in the following Failure Conditions:

loss of application , with .

loss of at least one application.

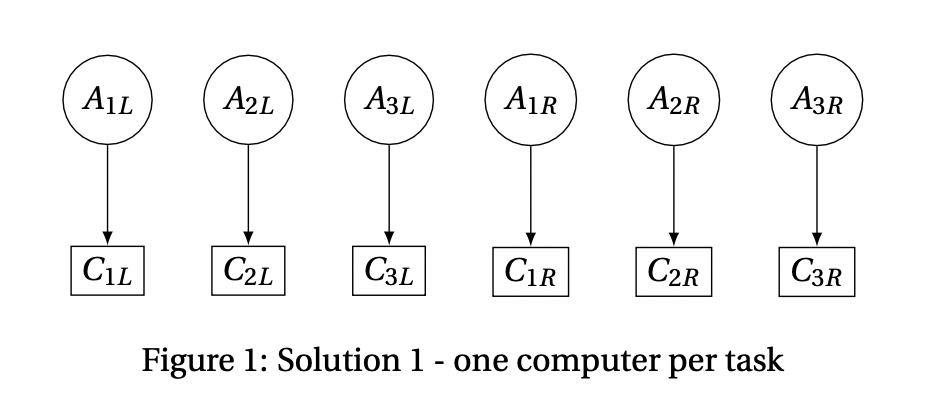
All the are classified *CATASTROPHIC* for an operation time of .

**Question 1.** What are the qualitative and quantitative safety requirements associated to the s?

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

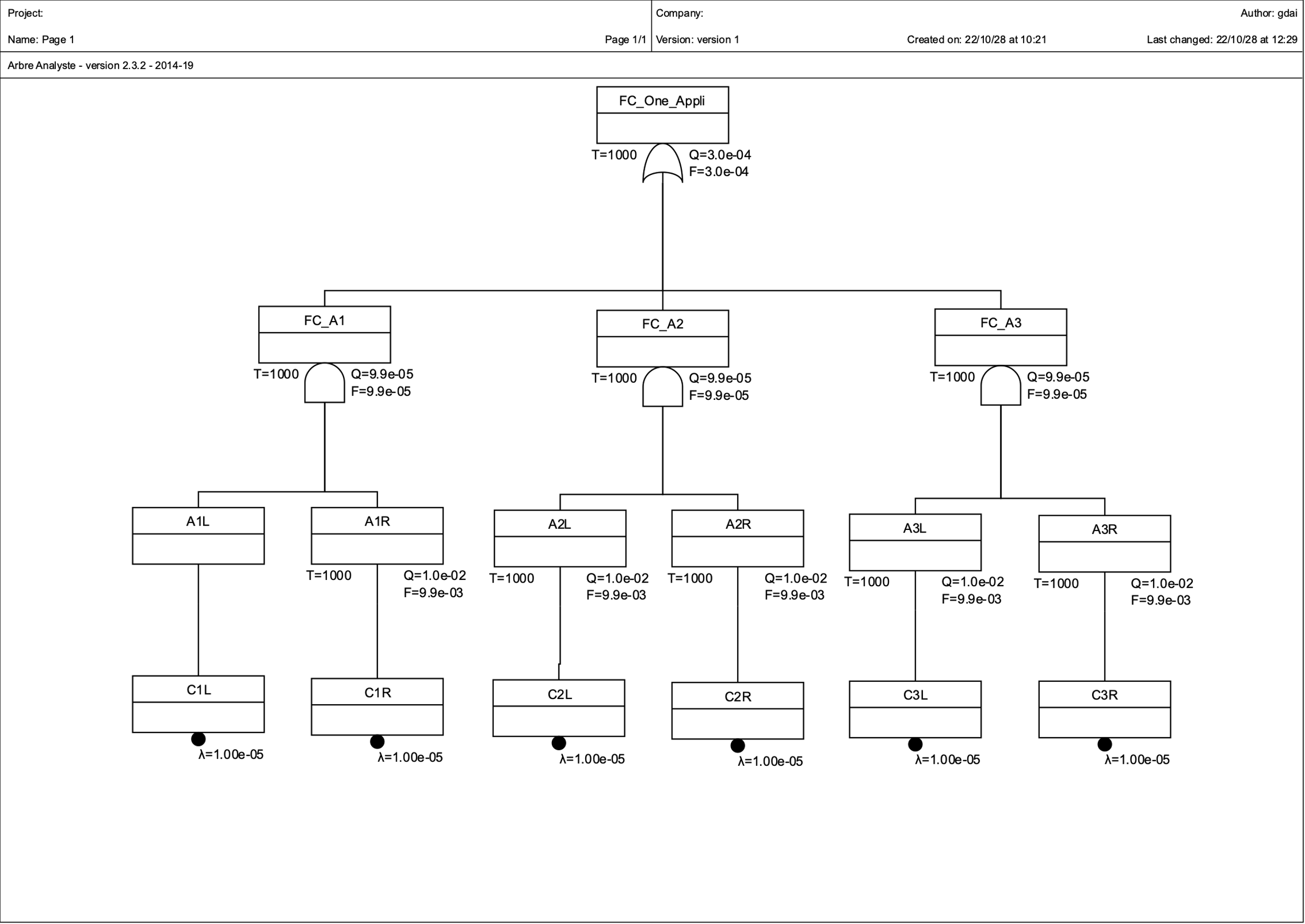
|  |  |  |
| --- | --- | --- |
| **Criticality** | **Qualitative requirement** | **Quantitative requirement** |
| *CATASTROPHIC* |  |  |

**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.

**Question 2**

1. Create a new file and build the fault-tree for the failure conditions and .



2. Compute the ***Minimal Cut Sets*** for and .

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 :

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

(3) The ***Minimal Cut Sets*** for :

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

(4) The ***Minimal Cut Sets*** for :

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

3. Compute the ***mean failure rate*** of and .

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

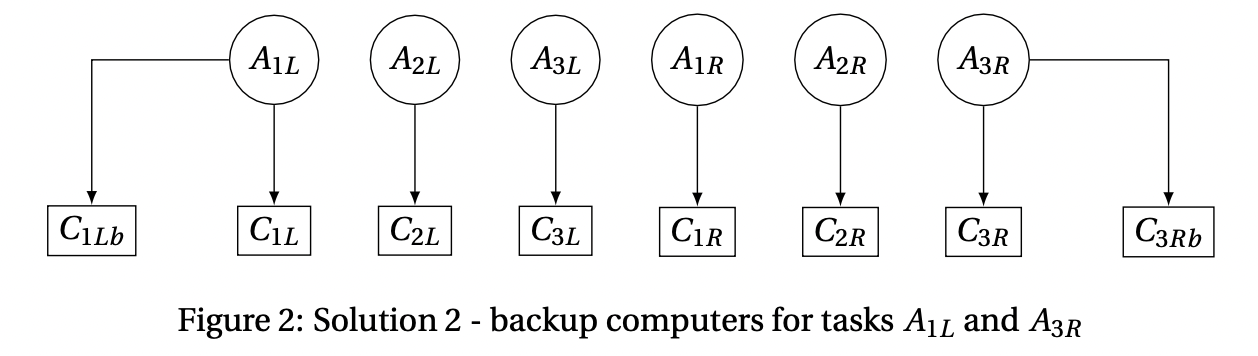
(2) The ***mean failure rate*** of is:

4. Are the Qualitative and Quantitative requirements enforced for failure conditions and ? Justify the answer.

Response:

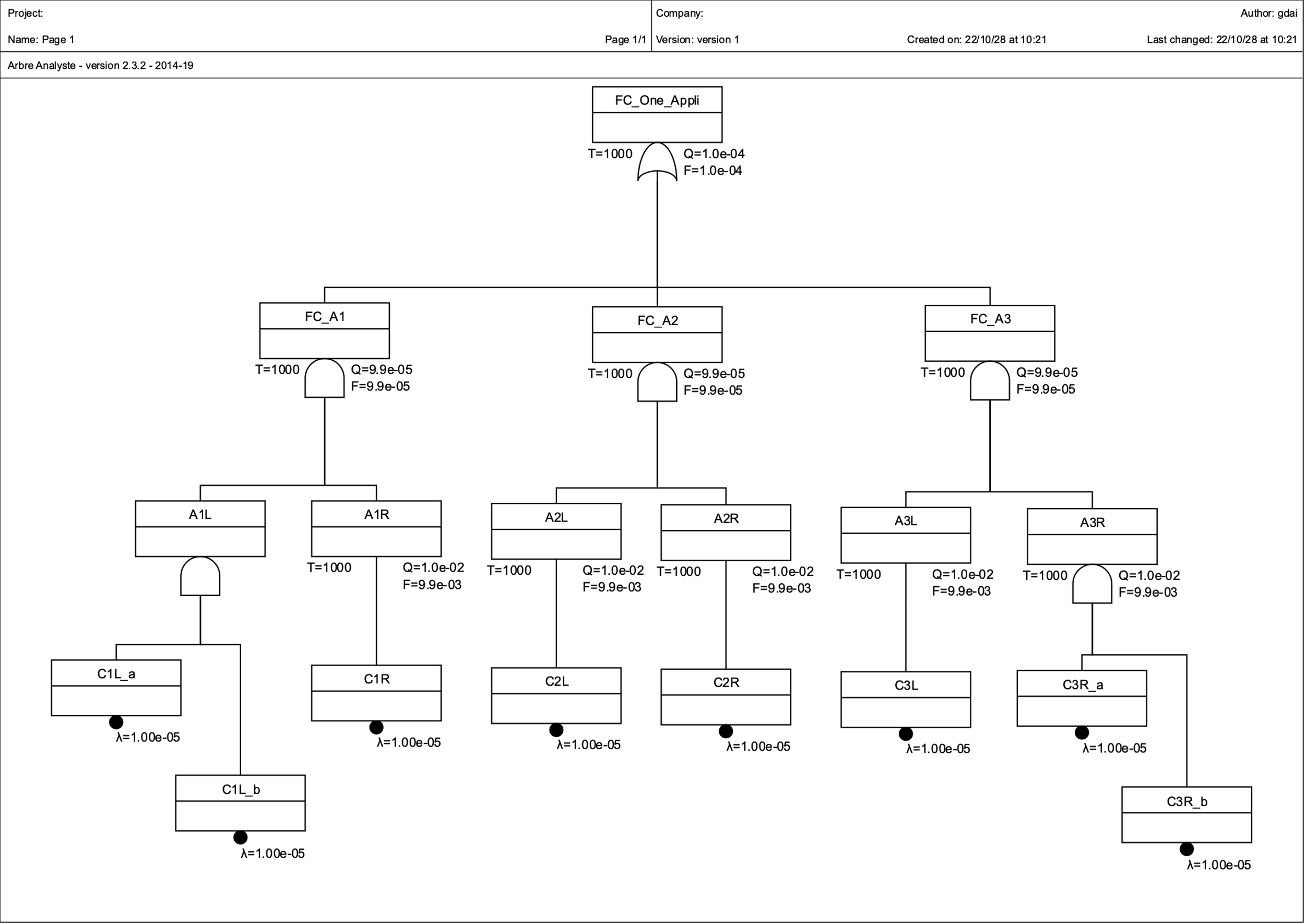
The Qualitative and Quantitative requirements are not enforced for failure conditions and . Because **the order of each equals 2** and **mean failure rate is more than** .

**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 (resp. ) that fails **if both the computers** and (resp. and ) fail.

**Question 3**

1. Create a new file and build the fault-tree for the failure conditions and .



2. Compute the ***Minimal Cut Sets*** for and .

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Quantity** | **Probability** | **Percent** | **Events** | | |
| 1 | 3 | 9.85124e-07 | 1 | C1L\_a | C1L\_b | C1R |

(3) The ***Minimal Cut Sets*** for :

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

(4) The ***Minimal Cut Sets*** for :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Quantity** | **Probability** | **Percent** | **Events** | | |
| 1 | 3 | 9.85124e-07 | 1 | C3L | C3R\_a | C3R\_b |

3. Compute the ***mean failure rate*** of and .

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

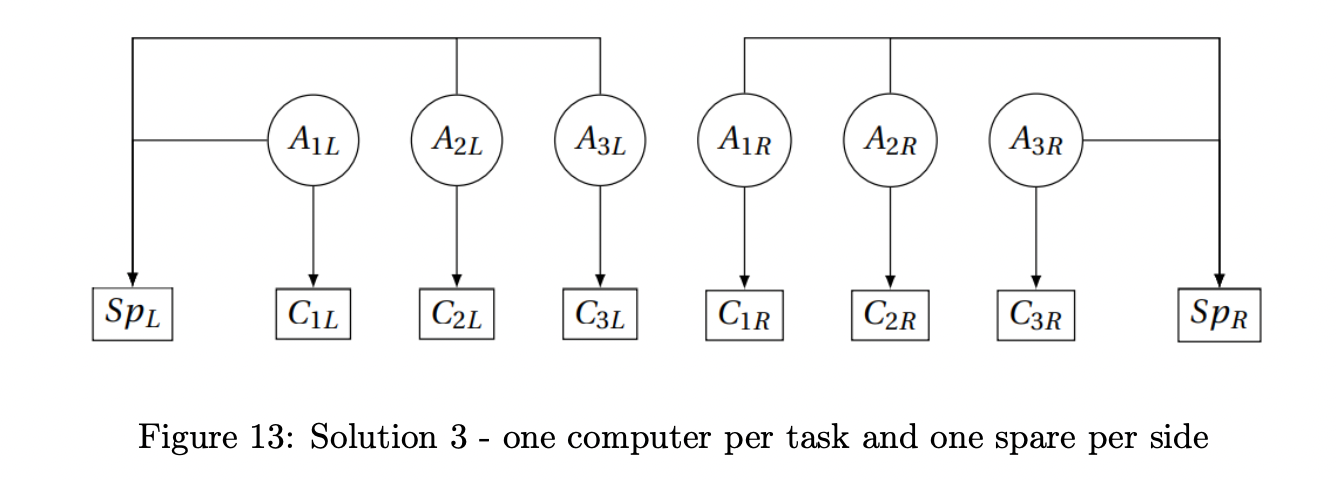
(2) The ***mean failure rate*** of is:

4. Are the Qualitative and Quantitative requirements enforced for failure conditions and ? Justify the answer.

Response:

* The Qualitative and Quantitative requirements are not enforced for failure conditions and . Because the **order of and are both equal 2**, moreover, **their mean failure rate is more than .**
* The Qualitative and Quantitative requirements are enforced for failure conditions and . Because **the order of each equals 3 ()** and **mean failure rate is less than .**

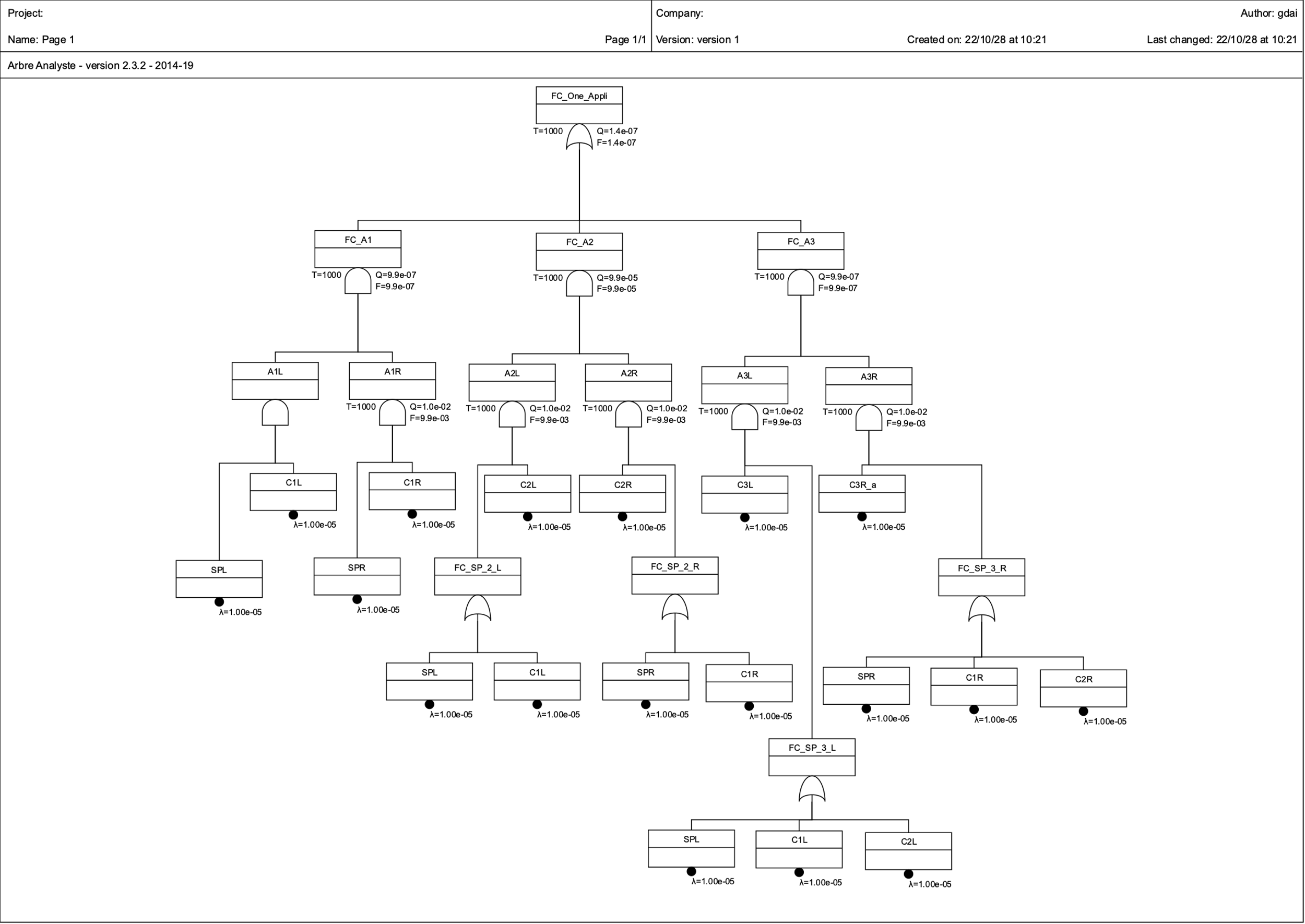
**4. Computing Platform Design – solution 3**

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 (resp. ) cannot be used as a backup. The spare (resp. ) can be used by:

* (resp. ) if (resp. ) fails,
* (resp. ) if (resp. ) fails and not used by (resp. ),
* (resp. ) if (resp. ) fails and not used by , or (resp. , or ).

**Question 4.**

1. Create a new file and build the fault-tree for the failure conditions and .



2. Compute the ***Minimal Cut Sets*** for and .

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 :

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

(3) The ***Minimal Cut Sets*** for :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 and .

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

(2) The ***mean failure rate*** of is:

4. Are the Qualitative and Quantitative requirements enforced for failure conditions and ? Justify the answer.

Response:

The Qualitative and Quantitative requirements are enforced for failure conditions and . Because **the order of each equals 4 ()** and **mean failure rate is less than .**

**5. Computing Platform Design – DAL Allocation**

The group of Basic Computers is independent from Spare Computers:

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 ()** | **DAL()** | **Acceptable Frequency**  (Order of Magnitude) |
| CAT | A |  |
| HAZ | B |  |
| MAL | C |  |
| MIN | D |  |
| NSE | E | - |

Table – Link between severity and DAL

(1) The DAL allocation table of Solution 1:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FC** | **Initial DAL** | **MCS** | **Components** | | | | | |
|  |  |  |  |  |  |
|  | A |  |  | - | - |  | - | - |
|  | A |  | - |  | - | - |  | - |
|  | A |  | - | - |  | - | - |  |
|  | A |  |  | - | - |  | - | - |
|  | - |  | - | - |  | - |
|  | - | - |  | - | - |  |
| **Final** | | |  |  |  |  |  |  |

(2) The DAL allocation table of Solution 2:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FC** | **Initial DAL** | **MCS** | **Components** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | A |  |  | - | - |  |  | - | - | - |
|  | A |  | - |  | - | - | - |  | - | - |
|  | A |  | - | - |  | - | - | - |  |  |
|  | A |  |  | - | - |  |  | - | - | - |
|  |  |  | - | - | - |  | - | - |
|  | - | - |  | - | - | - |  |  |
| **Final** | | |  |  |  |  |  |  |  |  |

(3) The DAL allocation table of Solution 3:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FC** | **Initial DAL** | **MCS** | **Components** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | A |  |  | - | - |  | - | - |  |  |
|  | A |  | - |  | - | - |  | - |  |  |
|  |  |  | - | - |  | - | - |  |
|  | - |  | - |  |  | - |  | - |
|  |  |  | - |  |  | - | - | - |
|  | A |  | - |  |  | - |  |  | - | - |
|  | - | - |  | - |  |  |  | - |
|  |  | - |  | - |  |  | - | - |
|  |  | - |  | - | - |  | - |  |
|  |  | - |  |  | - |  | - | - |
|  | - | - |  | - | - |  |  |  |
|  | - | - |  |  | - |  |  | - |
|  | - |  |  | - | - |  | - |  |
|  | - |  |  |  | - |  | - | - |
|  | A |  | - |  | - | - |  | - |  |  |
|  |  |  | - | - |  | - | - |  |
|  | - |  | - |  |  | - |  | - |
|  |  |  | - |  |  | - | - | - |
|  | - |  |  | - |  |  | - | - |
|  | - | - |  | - |  |  |  | - |
|  |  | - |  | - |  |  | - | - |
|  |  | - | - |  | - | - |  |  |
|  |  | - |  | - | - |  | - |  |
|  |  | - |  |  | - |  | - | - |
|  | - | - |  | - | - |  |  |  |
|  | - | - |  |  | - |  |  | - |
|  | - |  |  | - | - |  | - |  |
|  | - |  |  |  | - |  | - | - |
| **Final** | | |  |  |  |  |  |  |  |  |

**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 i order bound);

Response: if (number of components ) then (“OK”) else (“KO”)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Solution** | **components** | | | | | | | | | |
|  |  |  |  |  |  | / |  |  |  |
| 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 i mean failure rate bound).

Response: if (mean failure rate ) then (“OK”) else (“KO”)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Solution** | **components** | | | | | | | | | |
|  |  |  |  |  |  | / |  |  |  |
| 1 | KO | KO | KO | - | KO | KO | KO | - | - | - |
| 2 | KO | KO | KO | KO | KO | KO | KO | KO | - | - |
| 3 | 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:).

**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 |

To be continues