System Dependability Lab
Exercises on Safety Assessment of Static Systems

Friday 28th October, 2022

Report must be named **SURNAME1_SURNAME2.pdf**
and uploaded on moodle before
Friday 18th November, 2022

1 Preliminaries

1.1 Installation of Arbre Analyste

1.2 Lab reporting instructions

Start the tool by running `/usr/local/bin/arbre-analyste` in a terminal. Each question clarifies what are the expected report inputs. Concise answers are welcome.

2 Introduction

You will study and compare 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?

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

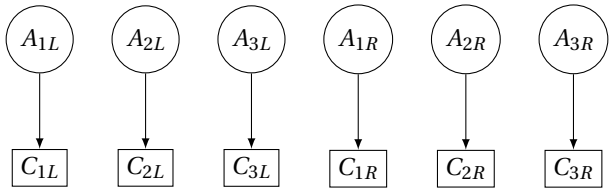

Figure 1: Solution 1 - one computer per task

Question 2

1. Create new file (Menu **File > New**) and build the fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the screenshot of the fault tree in your report.
2. Compute the Minimal Cut Sets for FC_{A_i} and FC_One_Appli (Menu **Calculations > XFTA calculation**)
   ⚠Do not forget to put the MCS computation results in your report.
3. Compute the mean failure rate of FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the mean failure rate computation results in your report.
4. Are the Qualitative and Quantitative requirements enforced for failure conditions FC_{A_i} and FC_One_Appli ? Justify your answer.

4 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.

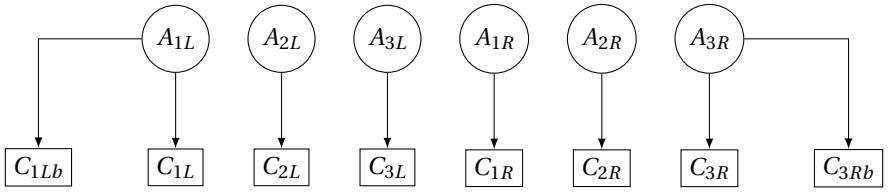

Figure 2: Solution 2 - backup computers for tasks A_{1L} and A_{3R}

Question 3

1. Create new file and build the fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the screenshot of the fault tree in your report.
2. Compute the Minimal Cut Sets for FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the MCS computation results in your report.
3. Compute the mean failure rate of FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the mean failure rate computation results in your report.
4. Are the Qualitative and Quantitative requirements enforced for the failure conditions FC_{A_i} and FC_One_Appli? Justify your answer.

5 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}).

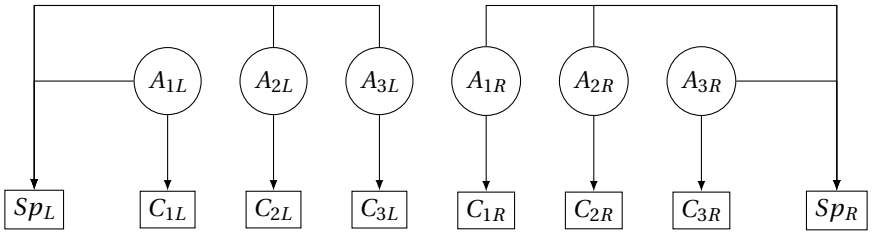

Figure 3: Solution 3 - one computer per task and one spare per side

Question 4

1. Create new file and build the fault-tree for the failure conditions FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the screenshot of the fault tree in your report.
2. Compute the Minimal Cut Sets for FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the MCS computation results in your report.
3. Compute the mean failure rate of FC_{A_i} and FC_One_Appli.
   ⚠Do not forget to put the mean failure rate computation results in your report.
4. Are the Qualitative and Quantitative requirements enforced for the failure conditions FC_{A_i} and FC_One_Appli? Justify your answer.

6 Computing Platform Design – DAL Allocation

The group of Basic Computers is independent from Spare Computers:

$$\begin{array}{ll} \text{Basic Computers} = & \{C_{1L}, C_{2L}, C_{3L}, C_{1Lb}, C_{1R}, C_{2R}, C_{3R}, C_{3Rb}\} \\ \text{Spare Computers} = & \{Sp_L, Sp_R\} \end{array}$$

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.

FC	Initial DAL	MCS	Components									
			C_{1L}	C_{2L}	C_{3L}	C_{1Lb}	C_{1R}	C_{2R}	C_{3R}	C_{3Rb}	Sp_L	Sp_R
FC_One_appli	?	?	$\geq$?	...								
FC_A_i	?	?	$\geq$?	...								
Final			?	...								

Table 1: DAL allocation table

Solution	Components									
	C_{1L}	C_{2L}	C_{3L}	C_{1Lb}	C_{1R}	C_{2R}	C_{3R}	C_{3Rb}	Sp_L	Sp_R
1	OK/KO									
2										
3										

Table 2: Acceptable failed components

7 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 order bound);
- the second one considering the quantitative requirement (i.e. satisfy FC_One_appli mean failure rate bound).

For each solution, deduce from these tables if it is possible to fly safely with one computer failed.
⚠Tips: if a solution

- does not initially fulfil its objectifs, then it will not fulfil them with a component already failed.
- contains symmetrical contributors to the the FCs then one computation can be used to demonstrate the acceptability of the symmetrical contributors.

8 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?

Solution	Fulfilled safety requirement		acceptable with failed component	cost
	Qualitative	Quantitative		
1				
2				
3				

Table 3: Solution comparison