System Dependability Lab
Exercises on Safety Assessment of Static Systems

Friday 13th January, 2023

Report must be named **SURNAME1_SURNAME2.pdf**
and uploaded on moodle before
Friday 27th January, 2023

1 Preliminaries

1.1 Installation of Arbre Analyste

Download the **initialSystem.opsa** project from moodle `https://moodle.insa-toulouse.fr/course/view.php?id=264` and open it.

1.2 Lab reporting instructions

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 the scene interpretation (SI), visual odometry (VO) and absolute localisation (Loc) applications. Each application A is implemented by two tasks A_L and A_R. The application A fails if **both** tasks A_L and A_R fail. A task fails if all the computers that can host it fail. We are interested in the following Failure Conditions:

HAZ_FC loss of the absolute localisation, the initial fault tree performed during the lesson has already been built on the first page

The FC is classified HAZARDOUS for an operation time of $T = 10^3 h$.

Question 1 What are the qualitative and quantitative safety requirements associated to the FC?

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

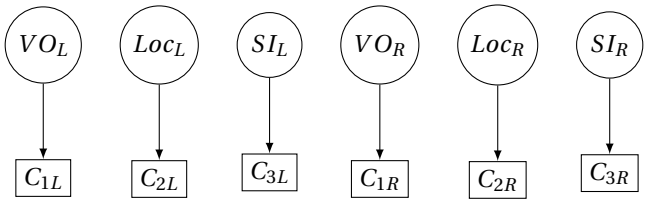

Figure 1: Solution 1 - one computer per task

Question 2

1. Open the B - Computing Platform 1 page and complete the fault-tree for the intermediate events VO_1, Loc_1 and SI_1.
   ⚠Do not forget to put the screenshot of the fault tree in your report.
2. Compute the Minimal Cut Sets for HAZ_FC (Menu **Calculations > XFTA calculation**)
   ⚠Do not forget to put the MCS computation results in your report.
3. Compute the mean failure rate of HAZ_FC.
   ⚠Do not forget to put the mean failure rate computation results in your report.
4. Are the Qualitative and Quantitative requirements enforced for HAZ_FC ? 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 VO_L (resp. SI_R) that fails **if both the computers** C_{1L} and C_{1Lb} (resp. C_{3R} and C_{3Rb}) fail.

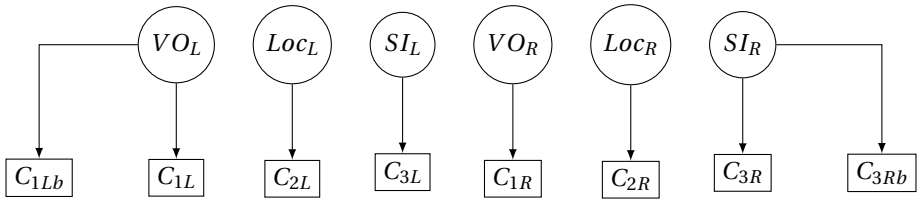

Figure 2: Solution 2 - backup computers for tasks VO_l and SI_R

Question 3

1. Open the C - Computing Platform 2 page and complete the fault-tree for the intermediate events VO_2, Loc_2 and SI_2.
   ⚠Do not forget to put the screenshot of the fault tree in your report.
2. Compute the Minimal Cut Sets for HAZ_FC.
   ⚠Do not forget to update the transfert gates in the main fault-tree.
   ⚠Do not forget to put the MCS computation results in your report.
3. Compute the mean failure rate of HAZ_FC.
   ⚠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 condition HAZ_FC? 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:

- VO_L (resp. VO_R) if C_{1L} (resp. C_{1R}) fails,
- Loc_L (resp. Loc_R) if C_{2L} (resp. C_{2R}) fails and not used by VO_L (resp. VO_R),
- SI_L (resp. SI_R) if C_{3L} (resp. C_{3R}) fails and not used by VO_L or Loc_L (resp. VO_R or Loc_R).

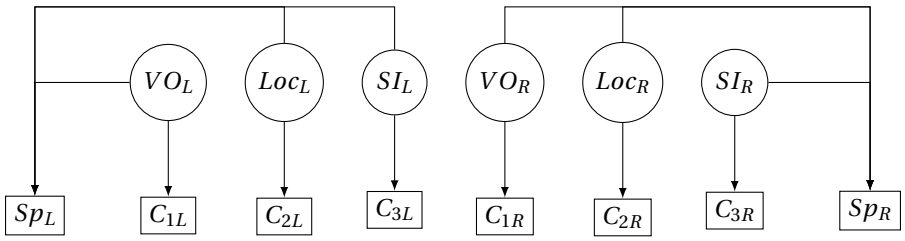

Figure 3: Solution 3 - one computer per task and one spare per side

Question 4

1. Open the D - Computing Platform 3 page and complete the fault-tree for the intermediate events VO_3, Loc_3 and SI_3.
   ⚠Do not forget to update the transfert gates in the main fault-tree.
   ⚠Do not forget to put the screenshot of the fault tree in your report.
2. Compute the Minimal Cut Sets for HAZ_FC.
   ⚠Do not forget to put the MCS computation results in your report.
3. Compute the mean failure rate of HAZ_FC.
   ⚠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 condition HAZ_FC? Justify your answer.

6 Computing Platform Design – Application Allocation

The applications can be freely allocated to basic, back-up and spare computers.

Question 5 For the computing platform 2 and 3, is there an allocation of the VO_L, VO_R, SI_L, SI_R, Loc_L, Loc_R applications enhancing the safety indicators (order or mean failure rate)? If yes, provide your allocation, the cutsets and the mean failure rate to prove it. If not explain why.

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.

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 1: Acceptable failed components

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

Table 2: Solution comparison

Question 7 Duplicate the table 1 in your report and complete :

- the first one considering the qualitative requirement (i.e. satisfy HAZ_FC order bound);
- the second one considering the quantitative requirement (i.e. satisfy HAZ_FC 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.

Question 8 Copy and complete the table 2 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?