System Dependability Lab
Exercises on Safety Assessment of Dynamic Systems

Thursday 1st December, 2022

Report must be posted on Moodle on the:
Thursday 15th December, 2022

Preliminaries

Installation of AltaRica Wizard

1. Run Altarica Wizard from `/applications/OARPlatform-lin64-v1.1.1/AltaRicaWizard/AltaRicaWizard`
2. Download the file TD2-AltaRica.zip from `http://moodle-n7.inp-toulouse.fr` and unzip it.

Lab reporting instructions

Each question clarifies what are the expected report inputs. Concise answers are welcome.

A satellite communication system

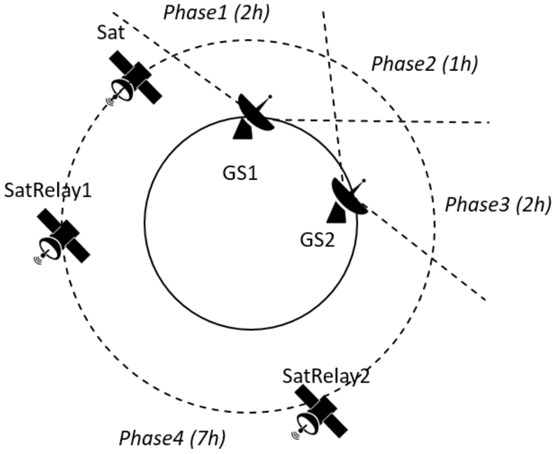

Figure 1: Satellite communication system.

You will study and assess a phased-mission system, which represents the communication mission between a given satellite **Sat** and the ground stations **GS1** and **GS2** as shown Figure1. Communications between the satellite **Sat** and the ground stations rely on different equipment at different periods of time. Generally there are two channels available for **Sat** to communicate with the stations:

- The first channel uses geostationary satellites **SatRelay1** and **SatRelay2** as the relay (and then **SatRelay1** or **SatRelay2** retransmit images to the stations).
- The second channel allows the satellite **Sat** to communicate directly with the stations when they are visible to each other.

The communication channel can be considered as a subsystem which may contain antennas, batteries, transmitters, and receivers as shown, for example, in the reliability block diagram Figure 3.

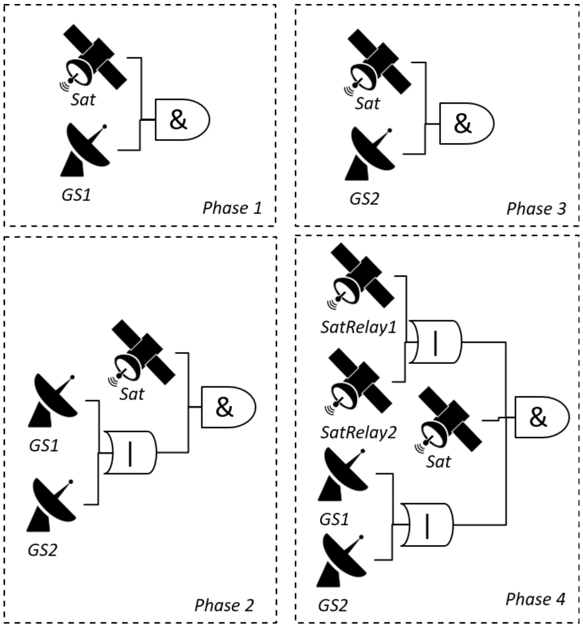

Figure 2: Phases of the satellite communication system.

The satellite **Sat** orbits the Earth for 300 laps, each orbital lap contains four phases. The subsystems used in each phase are shown Figure 2. The durations of the different phases are given in Table 1. The satellite communication system is thus a Phased-Mission System (PMS) made of 28 independent components and operating through 1200 successive phases.

Table 1: Parameters

Parameters	**Values**
Failure rates	$10^{-5}h^{-1}$
Repair rates for radars	$0.025h^{-1}$
Phase duration	$D1 = D3 = 2h$, $D2 = 1h$, $D4 = 7h$

We are interested in the following Failure Condition:

FC**:** loss of the communication between the satellite Sat and the ground stations $GS1$ and $GS2$.

Question 1: Basic modeling components

Double click on the file "Exercise2.ar3w" in TD2-AltaRica and then in AltaRica Wizard open the file "Components/BasicComponents.alt". It contains the class **NonRepairableComponent** which represents the behavior of a component which may fail in operation with a failure rate **pLambda** equal to $10^{-5}h^{-1}$ and cannot be repaired.

1. Complete the class **RepairableComponent** to represent the behavior of a component which may fail in operation with a failure rate $\lambda = 10^{-5}h^{-1}$ and may be repaired with a repair rate $\mu = 0.025h^{-1}$. Use inheritance to implement this class. Put the commented model in your report.
2. Complete the class **NonRepairableInOutComponent** which represents the behavior of a non repairable component with an input and an output. Input and output are Boolean variables, the value "true" means working and the value "false" means failed. Use inheritance to implement this class. Put the commented model in your report.
3. Complete the class **RepairableInOutComponent** which represents the behavior of a repairable component with an input and an output. Input and output are Boolean variables, the value "true" means working and the value "false" means failed. Use inheritance to implement this class. Put the commented model in your report.

Question 2: Reliability Block Diagrams

A reliability block diagram (RBD) is a diagrammatic method for showing how component reliability contributes to the success or failure of a system. A reliability block diagram is drawn as a series of blocks connected in parallel or in series configuration. Each block represents a component of the system with a failure rate. Parallel paths are redundant: all of the parallel paths must fail for the system to fail. By contrast, any failure along a series path causes the entire series path to fail.
For example, in the reliability block diagram given Figure 3 the system fails when both transmitters fail or both receivers fail or the antenna fails.

Question 2.1: Ground station reliability block diagram

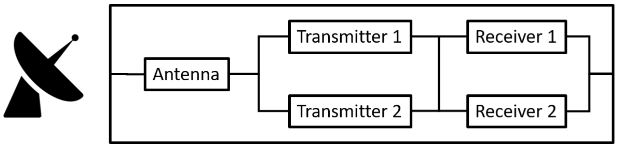

Figure 3: Ground station Reliability Block Diagram.

Figure 3 describes the reliability block diagram of the ground stations. In this exercise we assume that in the diagram all the components may fail in operation with failure rates given in Table 1.

1. Open the file "Components/GroundStation-RBD.alt" and complete the class **GroundStationSubSystem** to represent the reliability block diagram given Figure 3. Use the classes defined in the previous exercise.
2. Compile your model to verify that it is written correctly (Menu Tool > Flattening). Put the commented model in your report.

Question 2.2: Satellite reliability block diagram

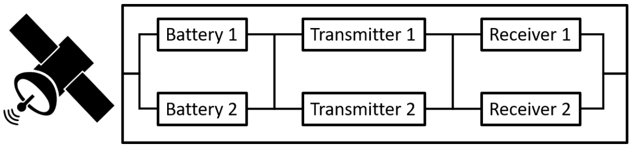

Figure 4: Satellite Reliability Block Diagram.

Figure 4 describes the reliability block diagram of the satellites. In this diagram all the components may fail in operation and cannot be repaired. Failure rates are given in Table 1.

1. Open the file "Components/Satellite-RBD.alt" and complete the class **SatelliteSubSystem** to represent the reliability block diagram given Figure 4. Use the classes defined in the previous exercise.

2. In the file "Exercise2/Exercise2.alt" uncomment **SatelliteSubSystem Sat;**. Compile your model to verify that it is written correctly (Menu Tool > Flattening). Put the commented model in your report.

Question 3: Static phased mission system modeling and assessment

Figure 2 shows which subsystems of the satellite communication system are used in different phases. The model of each satellite is represented by the reliability block diagram given Figure 4 and defined in the class **SatelliteSubSystem**. The model of each ground station is represented by the reliability block diagram given Figure 3 and defined in the class **GroundStationSubSystem**.
The objective of this exercise is to model the satellite communication system in each phase using advanced structuring constructs (composition, aggregation) and to assess it by compilation into Fault Trees. To do that:

1. Double click the file "Exercise3.ar3w" and open the file "Exercise3/System.alt". In the block **System** :

   (a) Define the elements that compose the system (see Figure 2).

   (b) Define the components of the system used in each phase: complete blocks "Phase1", "Phase2", "Phase3", "Phase4" (use the aggregation relation).

   (c) Complete the assertion of the main block "System".

   (d) Define the observer representing the Failure Condition: loss of communication between the satellite Sat and the ground stations $GS1$ and $GS2$.

   ⚠In this exercise you do not need to modify the block **PhaseController**.

2. Compile your model to verify that it is written correctly (Menu Tool > Flattening).

3. Validate your model by simulation (Menu Tool > Stepwise simulation). Put the commented model in your report.

4. Assess your model by compilation into Fault Trees in each phase. To do that change the initial value of the variable **vsPhase** of the block **PhaseController**, compile your model and launch Fault Tree generation (Menu Tool > Compilation into Fault Tree).

   (a) Compute Minimal Cuts Set for the Failure Condition (FC) for each phase (1, 2, 3, 4). Put the results in your report.

5. What are the most critical components of the system? Justify your answer.

Question 4: Dynamic phased mission system modeling and assessment

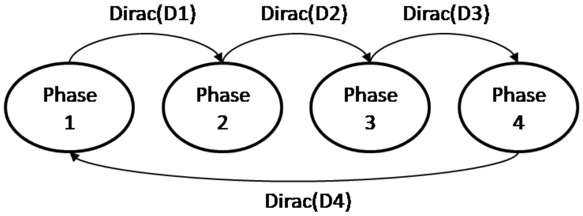

Figure 5: State machine modeling the changes of phases.

Figure 5 represents the changes of phases of the satellite communication system. Durations of each phase are given in Table 1. Now we also assume that in the ground station subsystem all the components may fail in operation and be repaired with a repair rate given in Table 1. The objective of this exercise is to integrate the changes of phases in the previous model and to assess the reliability of the system by stochastic simulation. To do that:

1. Open the project "Exercise4.ar3w".
2. Change the model of ground station subsystem to take into account the repairs of the components. Put the commented model in your report.
3. In the file "Exercise4/System.alt copy the block **System** of the previous exercise.
4. Modify the block **PhaseController** to represent the behavior of the phase controller given Figure 5.
5. Compile and validate your model by simulation. Put the commented model in your report.

Question 5: Common cause failures

In the satellite subsystem given Figure 4 batteries are subjected to a common cause failure with a failure rate $\lambda_{CCF} = 10^{-6} h^{-1}$.

1. Open the project "Exercise5.ar3w" and open the file "Exercise5/Satellite-RBD-ccf.alt". Modify the previous model of the satellite subsystem to integrate the common cause failure of batteries.
2. Compile your model to verify that it is written correctly.