Safety modeling and assessment with AltaRica 3.0

Michel BATTEUX (IRT SystemX), michel.batteux@irt-systemx.fr
Tatiana PROSVIRNOVA (ONERA), tatiana.prosvirnova@onera.fr
Antoine RAUZY (NTNU)
Case Study – a satellite communication system

A satellite communicates with ground stations directly or by geostationary satellites (relays).

2 different communication channels:
- Sat -> {GS1,GS2}
- Sat -> {SatRelay1, SatRelay2} -> {GS1, GS2}
Case Study – a satellite communication system

Communication channels can be considered as subsystems which may contain several components (antennas, batteries, transmitters, receivers) => reliability block diagram point of view

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Rates</td>
<td>$10^{-5}$ h$^{-1}$</td>
</tr>
<tr>
<td>Repair Rates</td>
<td>0.025 h$^{-1}$</td>
</tr>
</tbody>
</table>
Case Study – a satellite communication system

Sat orbits the Earth for 300 laps, each orbital lap contains four phases.
Subsystems used in each phase are represented by the reliability block diagrams.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Rates</td>
<td>$10^{-5} \text{ h}^{-1}$</td>
</tr>
<tr>
<td>Repair Rates (for radars)</td>
<td>$0.025 \text{ h}^{-1}$</td>
</tr>
<tr>
<td>Phase duration</td>
<td>$D_1=D_3=2\text{h}$, $D_2=1\text{h}$, $D_4=7\text{h}$</td>
</tr>
</tbody>
</table>
Objective of the study

Failure condition (FC):
Loss of communication between the ground stations and the satellite Sat

Assess the reliability of this phased-mission system for a 3600 hours mission

Activities
1. Model the system
2. Perform calculations on reliability indicators of the models thanks to calculation engines
1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. Modeling of reliability block diagrams
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. Modeling of common cause failures
4. Modeling and assessment of static satellite communication system (demo)
5. Modeling and assessment of dynamic satellite communication system (demo)
AltaRica 3.0

Behaviors + Structures = Models

GTS + S2ML = AltaRica 3.0

GTS: Guarded Transition Systems
Generalization of states/transitions formalisms such as (multiphase) Markov chains and stochastic Petri nets

S2ML: System Structure Modeling Language
Set of structuring mechanisms stemmed from object-oriented and prototype-oriented programming
Modeling and assessment tools

Altarica 3.0

Guarded Transition Systems

Fault Tree compiler

Sequence generator*

Stochastic simulator

Stepwise simulator

* Coming soon

https://www.openaltarica.fr/docs-downloads/
1. **Modeling of components**
   a. Non repairable unit
   b. Repairable unit

2. **Modeling of reliability block diagrams**
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram

3. **Modeling of common cause failures**

4. **Modeling and assessment of static satellite communication system (demo)**

5. **Modeling and assessment of dynamic satellite communication system (demo)**
Modeling of components

Exercise 1.a: A non repairable unit

- Represent in AltaRica 3.0 a component which can fail in operation with a failure rate $p\lambda$ and cannot be repaired.
Modeling of components: a non repairable unit

• **State** variables are used to model the state of the systems.

• Variables can take their values into predefined domains (Boolean, Integer, Real, Symbol) or used defined domain (sets of symbolic constants)
Modeling of components: a non repairable unit

- **Events** are associated with **delays**

- A **transition** is a triple <e, G, P>, where e is an **event**, G is a **guard** (a Boolean expression), P is an action (an instruction which modifies the value of state variables)

```java
/* Basic classes for non repairable and repairable components */
class NonRepairableComponent
  Boolean vsWorking (init = true);
  event evFailure (delay = exponential(pLambda));
  parameter Real pLambda = 1.0e-5;

  transition
  evFailure: vsWorking -> vsWorking := false;
end
```
Stochastic and determinist events

- Events are associated with determinist or stochastic delays and/or probabilities (weights).

<table>
<thead>
<tr>
<th>Event</th>
<th>Rate</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>failure</td>
<td>$\lambda$</td>
<td></td>
</tr>
<tr>
<td>repair</td>
<td>$\mu$</td>
<td></td>
</tr>
<tr>
<td>start</td>
<td>$1 - \gamma$</td>
<td></td>
</tr>
<tr>
<td>failureOnDemand</td>
<td>$\gamma$</td>
<td></td>
</tr>
<tr>
<td>stop</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Probability distribution

- Dirac($T$)
- Exponential ($\lambda$)
- Weibull
- UniformDeviate($\mu$, $\nu$)
- Empirical distribution
Modeling of components

Exercise 1.b: **A repairable unit**

- Modify the previous model to represent a repairable unit with a repair rate $pMu$. 

![Diagram](image.png)
Modeling of components

Exercise 1.b: A repairable unit
- Modify the previous model to represent a repairable unit with a repair rate $pMu$. 

```plaintext
12 13 class RepairableComponent
14 15 extends NonRepairableComponent;
15 16 parameter Real $pMu = 1.0e-2$;
16 17 event evRepair (delay = exponential($pMu$));
18
19 transition
20 21 evRepair: not vsWorking -> vsWorking := true;
22
end
```
1. Modeling of components  
   a. Non repairable unit  
   b. Repairable unit  

2. **Modeling of reliability block diagrams**  
   a. Satellite reliability block diagram  
   b. Ground station reliability block diagram  

3. Modeling of common cause failures  
4. Modeling and assessment of static satellite communication system (demo)  
5. Modeling and assessment of dynamic satellite communication system (demo)
Modeling of reliability block diagrams

Exercise 2:
- Represent the following Reliability Block Diagrams in AltaRica 3.0
Guarded Transition Systems: composition

• The model for the system is obtained by composing smaller models of subsystems and components.

• This means that the model is an implicit representation of the state space.

• Composition of two (or more) Guarded Transition Systems is also a Guarded Transition System.
Guarded Transition Systems: flow propagation

• After each transition firing, a mechanism propagates the change of state through the network of components.
Modeling of Reliability Block Diagrams

Exercise 2.a: Satellite Reliability Block Diagram

- **Flow** variables are used to model flows circulating through the model.
- They are updated by means of the **assertion** after each transition firing.
Modeling of Reliability Block Diagrams

Exercise 2.a: Satellite Reliability Block Diagram
Modeling of Reliability Block Diagrams

Exercise 2.b: Radar Reliability Block Diagram

```
/* Radar subsystem
   * represented by a block diagram modeling pattern with repair
   */
class RadarSubSystem
  parameter Real mu = 0.025;
  ReparableInOutComponent Antenna(pMu = mu);
  ReparableInOutComponent Transmitter1, Transmitter2(pMu = mu);
  ReparableInOutComponent Receiver1, Receiver2 (pMu = mu);
  Boolean vfOutput ( reset = false );

assertion
  Antenna.vfInput := true;
  Transmitter1.vfInput := Antenna.vfOutput;
  Transmitter2.vfInput := Antenna.vfOutput;
  Receiver1.vfInput := Transmitter1.vfOutput or Transmitter2.vfOutput;
  Receiver2.vfInput := Transmitter1.vfOutput or Transmitter2.vfOutput;
  vfOutput := Receiver1.vfOutput or Receiver2.vfOutput;
```

1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. Modeling of reliability block diagrams
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. **Modeling of common cause failures**
4. Modeling and assessment of static satellite communication system (demo)
5. Modeling and assessment of dynamic satellite communication system (demo)
Exercise 3:

In the satellite subsystem given below batteries are subjected to a common cause failure with a failure rate $ccf\Lambda = 1.0e^{-6}$

- Modify the previous model of the satellite subsystem to integrate the common cause failure of batteries
Modeling of common cause failures

Exercise 3: Common cause failure modeling

```plaintext
/* Satellite subsystem
* represented by a block diagram modeling pattern with non repairable components */

class SatelliteSubSystem
  NonRepairableInOutComponent Battery1, Battery2;
  NonRepairableInOutComponent Transmitter1, Transmitter2;
  NonRepairableInOutComponent Receiver1, Receiver2;
  Boolean vfOutput( reset = false );

  parameter Real pCCFRate = 1.0e-6;
  event ccfBatteries (delay = exponential(pCCFRate));

  transition
c    ccfBatteries: ? Battery1.evFailure & ? Battery2.evFailure;

  assertion
  Battery1.vfInput := true;
  Battery2.vfInput := true;
  Transmitter1.vfInput := Battery1.vfOutput or Battery2.vfOutput;
  Transmitter2.vfInput := Battery1.vfOutput or Battery2.vfOutput;
  Receiver1.vfInput := Transmitter1.vfOutput or Transmitter2.vfOutput;
  Receiver2.vfInput := Transmitter1.vfOutput or Transmitter2.vfOutput;
  vfOutput := Receiver1.vfOutput or Receiver2.vfOutput;

end
```
1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. Modeling of reliability block diagrams
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. Modeling of common cause failures
4. **Modeling and assessment of static satellite communication system (demo)**
5. Modeling and assessment of dynamic satellite communication system (demo)
Modeling and assessment of static satellite communication system

Exercise 4:

1. Model the satellite communication system in each phase
2. Define observers
3. Validate the model by simulation
4. Assess your model by comilation to Fault Trees in each phase

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Rates</td>
<td>$10^{-5} \text{ h}^{-1}$</td>
</tr>
<tr>
<td>Repair Rates (for radars)</td>
<td>$0.025 \text{ h}^{-1}$</td>
</tr>
<tr>
<td>Phase duration</td>
<td>$D1=D3=2\text{h}$, $D2=1\text{h}$, $D4=7\text{h}$</td>
</tr>
</tbody>
</table>
System Structure Modeling Language (S2ML)

S2ML: a **structuring paradigm** that unifies **object** and **prototype-orientation**.

- **Port**
  - Variable, event...

- **Connection**
  - Equation, transition...

- **Container**
  - Model, component...

- **Composition**
  - Is-part-of

- **Inheritance**
  - Is-a

- **Aggregation**
  - Uses

- **Prototype/Clone**

- **Class/Instance**

Exercise 4: Modeling and assessment

An architectural pattern

Flow propagation

2. Phase controller

3. Phases
   - Phase 1
   - Phase 2
   - ... Phase N

4. Multiplexer

1. System breakdown structure and behavior

Static Phase Controller

DEMO
Case study: a satellite communication system

1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. Modeling of reliability block diagrams
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. Modeling of common cause failures
4. Modeling and assessment of static satellite communication system (demo)
5. **Modeling and assessment of dynamic satellite communication system (demo)**
Exercise 5:

1. Modify the previous model of the satellite communication system to represent the behavior of the phase controller
2. Validate your model by simulation
3. Assess the reliability by stochastic simulation
Exercise 5: Modeling and assessment

An **architectural pattern**
Exercise 5: Stochastic simulation

An **architectural pattern**
From System Architectures to Safety Analyses

The architecture pattern of the phased-mission system as an implementation of the CESAMES method for systems architecting.
Summary

• AltaRica 3.0 = GTS + S2ML
  • **GTS: Guarded Transition Systems**
    Generalization of states/transitions formalisms such as (multiphase) Markov chains and stochastic Petri nets
  • **S2ML: System Structure Modeling Language**
    Set of structuring mechanisms stemmed from object-oriented and prototype-oriented programming

• AltaRica 3.0 tools
  • AltaRica Wizard
  • Fault Tree compiler
  • Stochastic simulator
  • Stepwise simulator
  • Download at [https://www.openaltarica.fr/docs-downloads/](https://www.openaltarica.fr/docs-downloads/)

References


**Tutorial examples of AltaRica 3.0**


References

Compilation of AltaRica (GTS) into Fault Trees


Compilation of AltaRica (GTS) into Markov chains


AltaRica tools