Safety modeling and assessment with AltaRica 3.0

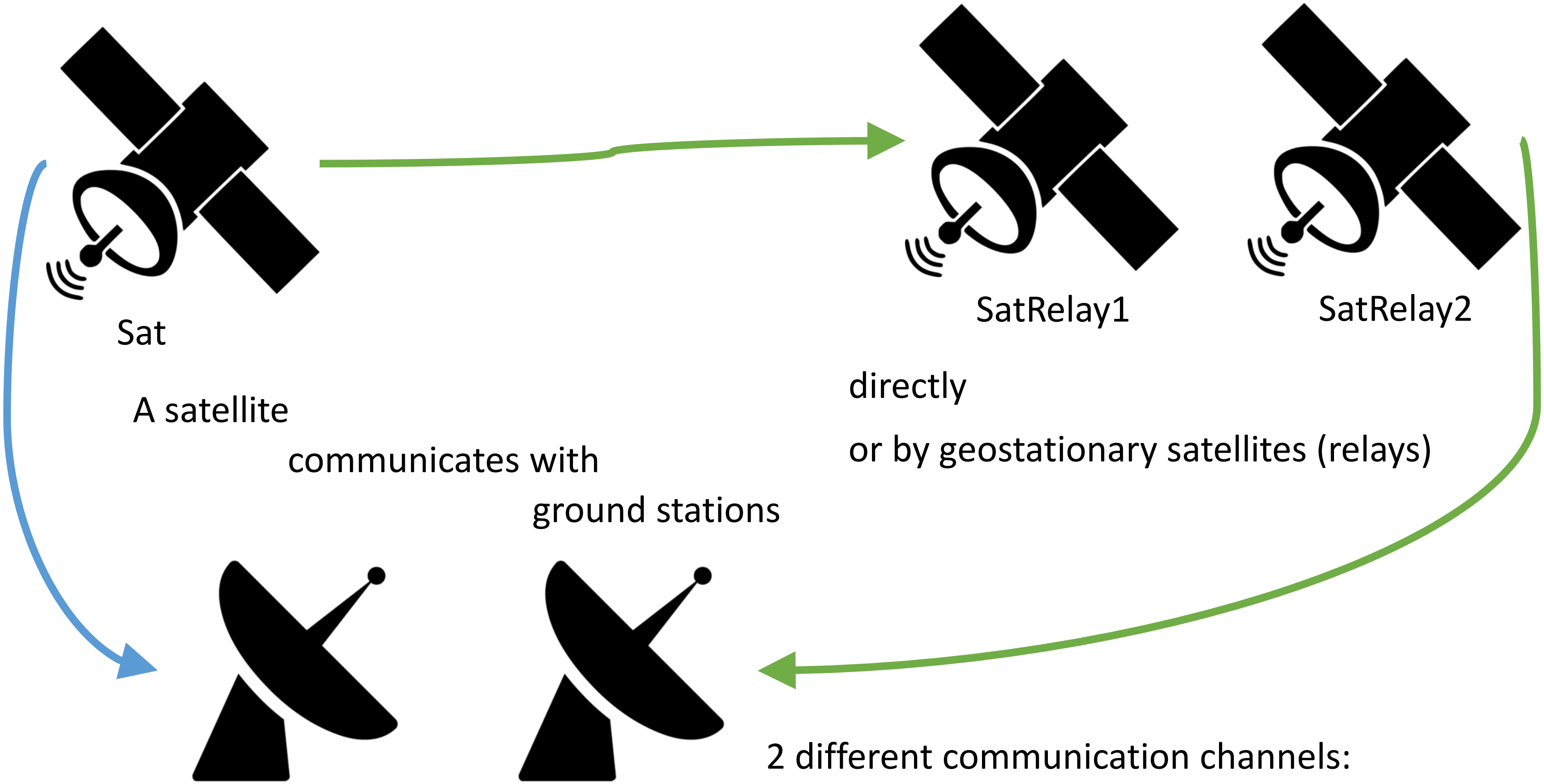
Michel BATTEUX (IRT SystemX), michel.batteux@irt-systemx.fr

Tatiana PROSVIRNOVA (ONERA), tatiana.prosvirnova@onera.fr

Antoine RAUZY (NTNU)

IMBSA2019

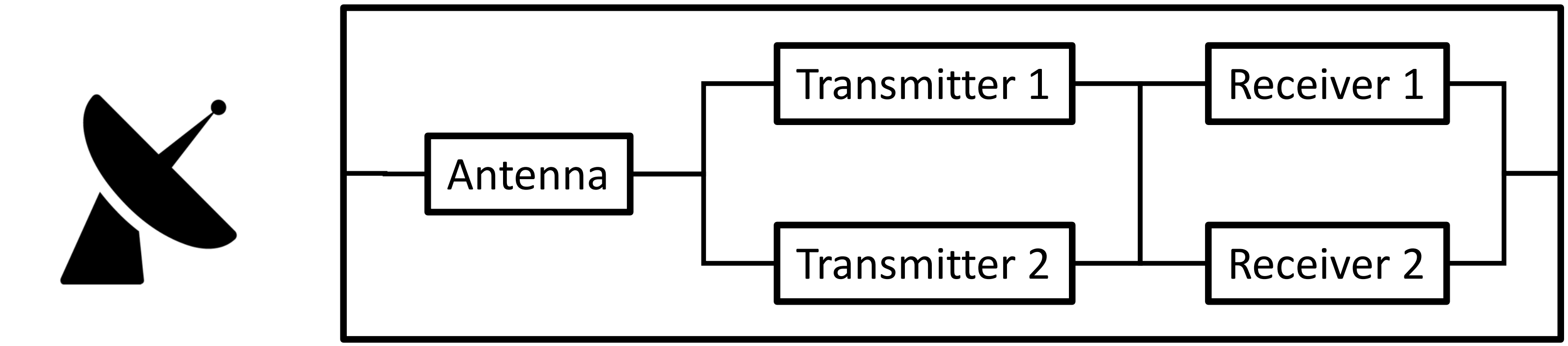
Case Study – a satellite communication system

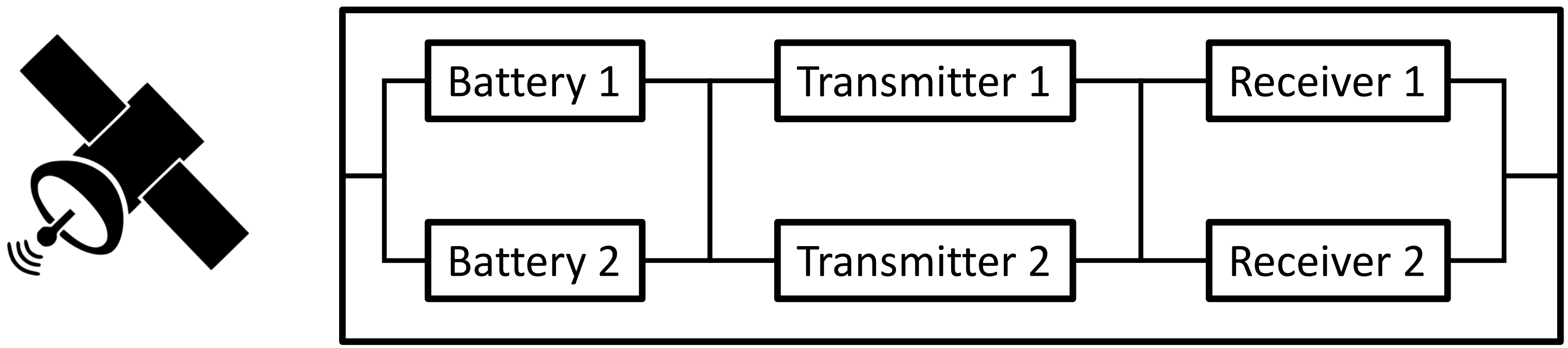


2 different communication channels:

- Sat -> {GS1,GS2}
- Sat -> {SatRelay1,SatRelay2} -> {GS1,GS2}

Case Study – a satellite communication system



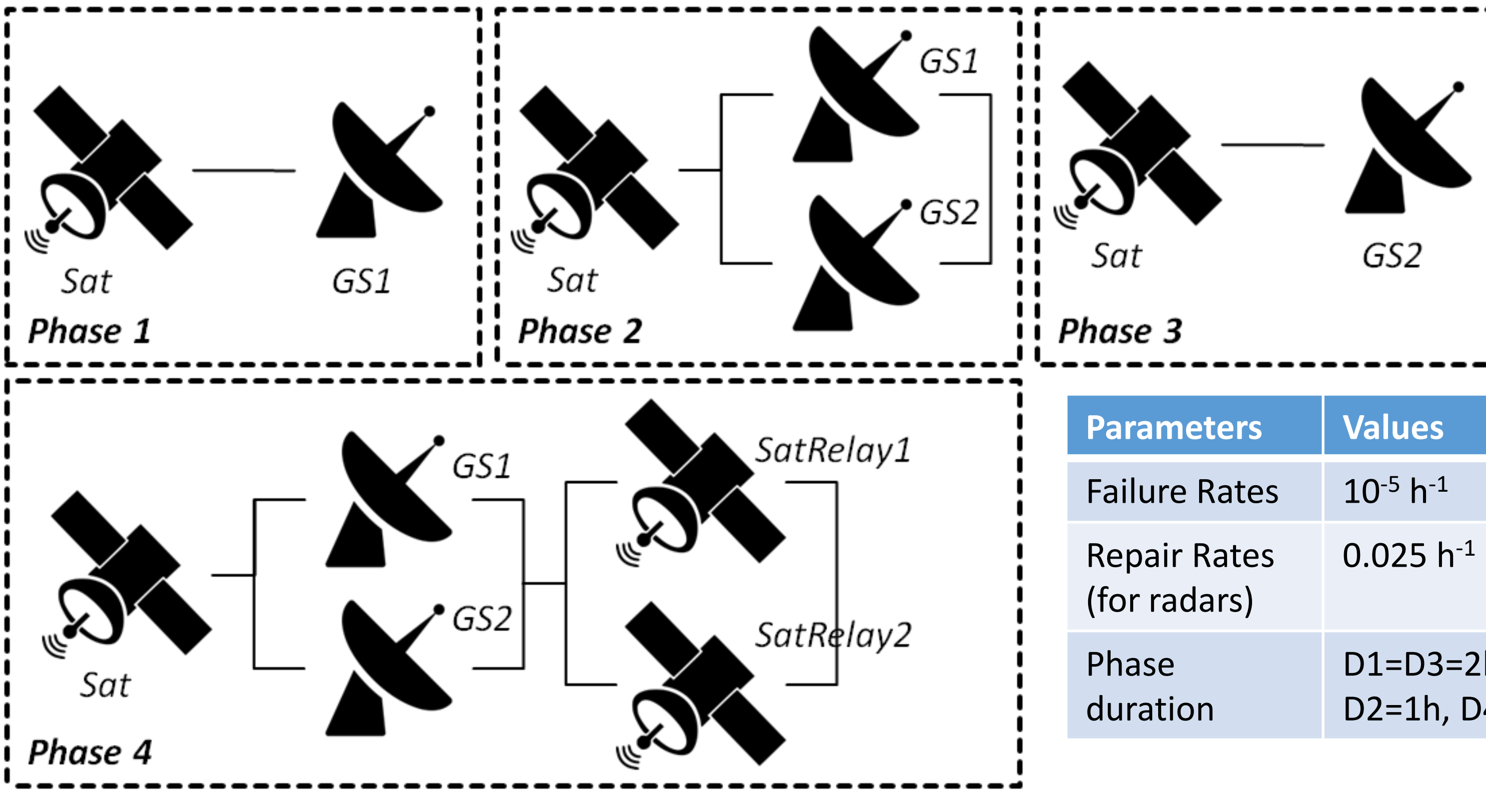


Communication channels can be considered as subsystems which may contain several components (antennas, batteries, transmitters, receivers)
=> reliability block diagram point of view

Parameters	Values
Failure Rates	10^{-5} h^{-1}
Repair Rates (for radars)	0.025 h^{-1}

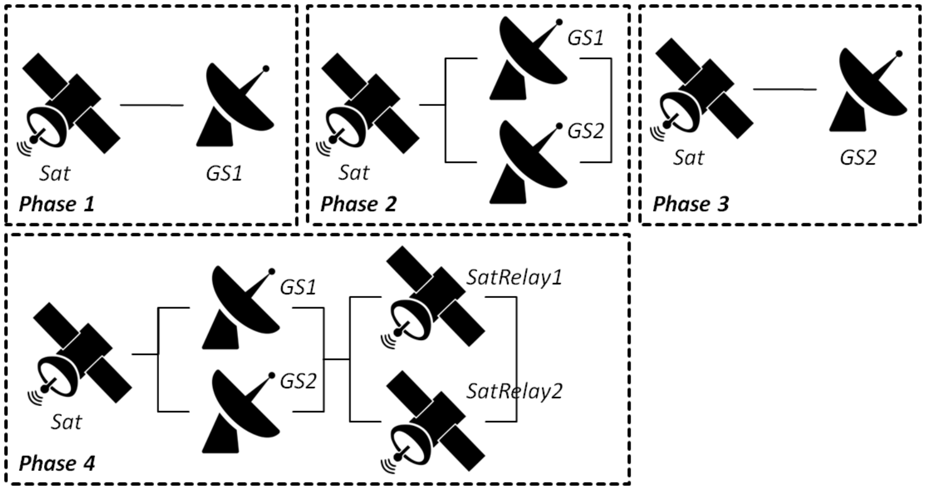
Case Study – a satellite communication system

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



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

Objective of the study

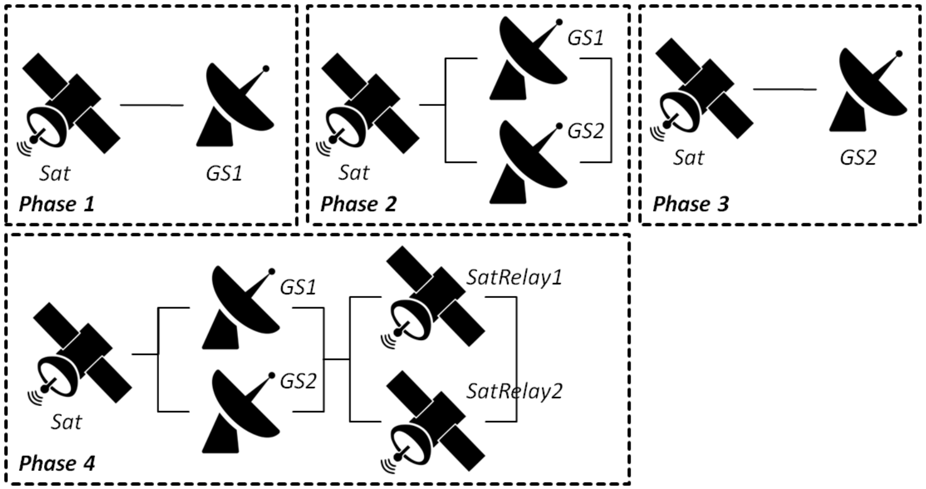


Failure condition (FC):
Loss of communication between the ground stations and the satellite Sat

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

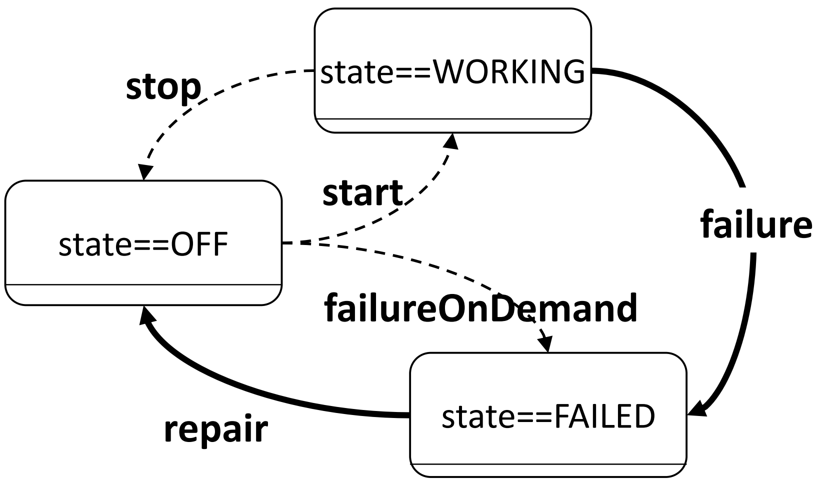
Case study: a satellite communication system



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)

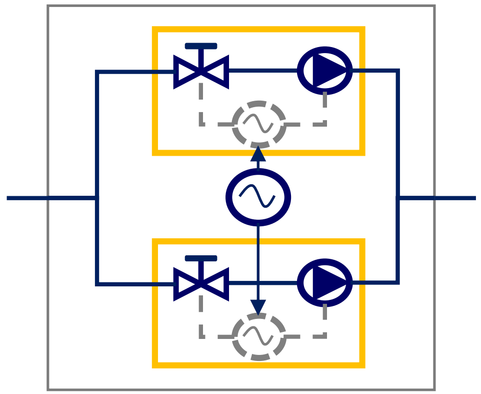
AltaRica 3.0

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

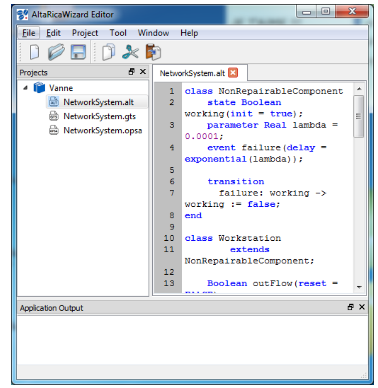
S2ML: System Structure Modeling Language
Set of structuring mechanisms stemmed from object-oriented and prototype-oriented programming



Modeling and assessment tools

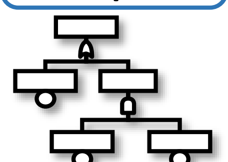
AltaRica 3.0

Guarded Transition Systems



AltaRica Wizard

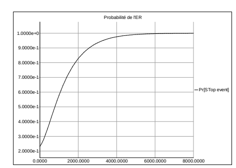
Fault Tree compiler



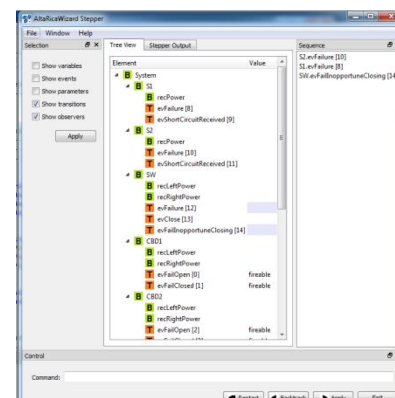
XFTA

Sequence generator*

Stochastic simulator



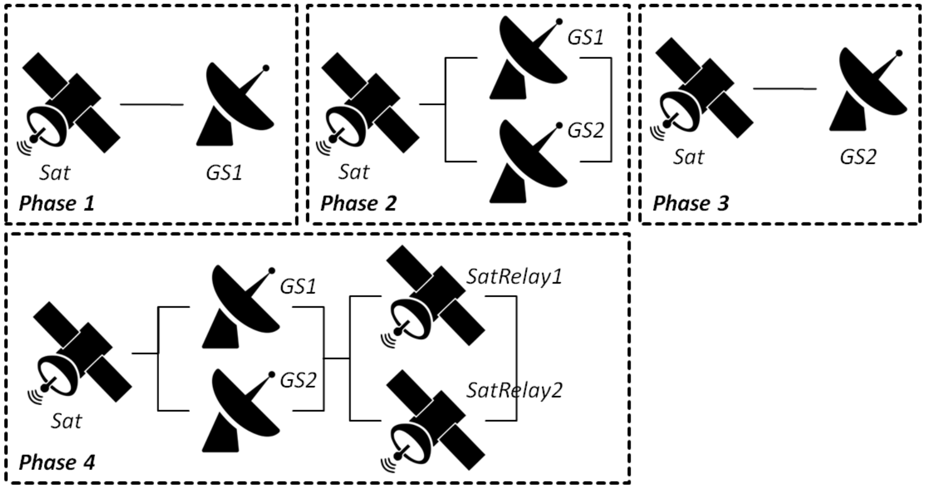
Stepwise simulator



** Coming soon*

https://www.openaltarica.fr/docs-downloads/

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)

Modeling of components

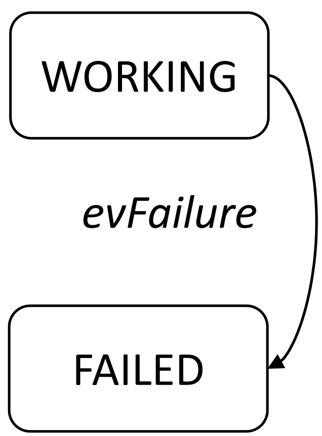
Battery

Transmitter

Receiver

Exercise 1.a: **A non repairable unit**

- Represent in AltaRica 3.0 a component which can fail in operation with a failure rate *pLambda* and cannot be repaired.



Modeling of components:
a non repairable unit

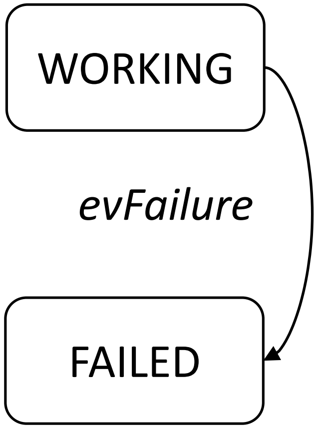
Battery

Transmitter

Receiver

```

/* 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

```

- **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

Battery

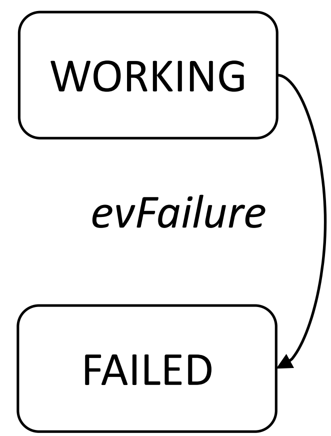
Transmitter

Receiver

```

/* 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

```

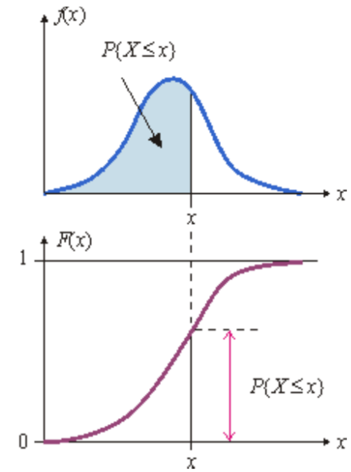
- **Events** are associated with **delays**

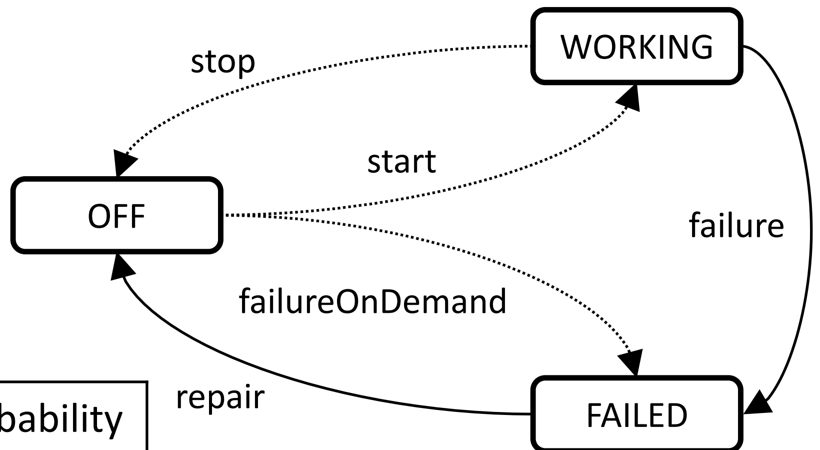
- A **transition** is a triple <e, G, P>, where e is an **event**, G is a **guard** (a Boolean expression), P is an action (an instruction which modifies the value of state variables)



Stochastic and determinist events

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





Event	Rate	Probability
failure	λ	
repair	μ	
start		$1-\gamma$
failureOnDemand		γ
stop		1

Probability distribution
Dirac(T)
Exponential (λ)
Weibull
UniformDeviate(μ, ν)
Empirical distribution

Modeling of components

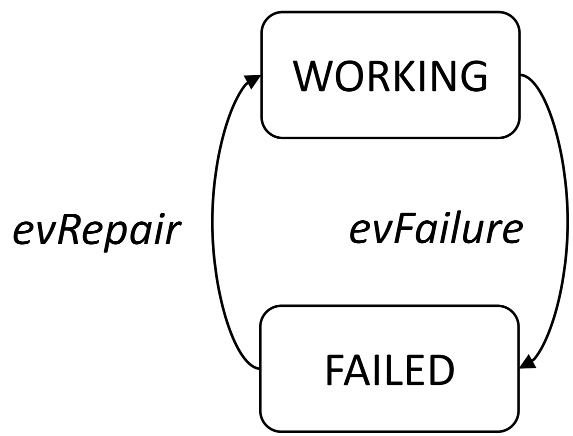
Exercise 1.b: **A repairable unit**

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

Antenna

Transmitter

Receiver



Modeling of components

Antenna

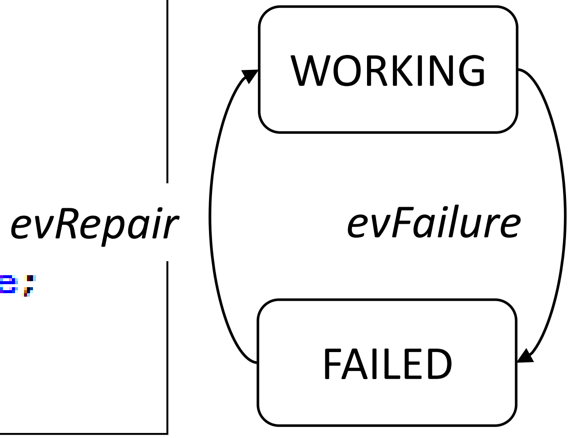
Transmitter

Receiver

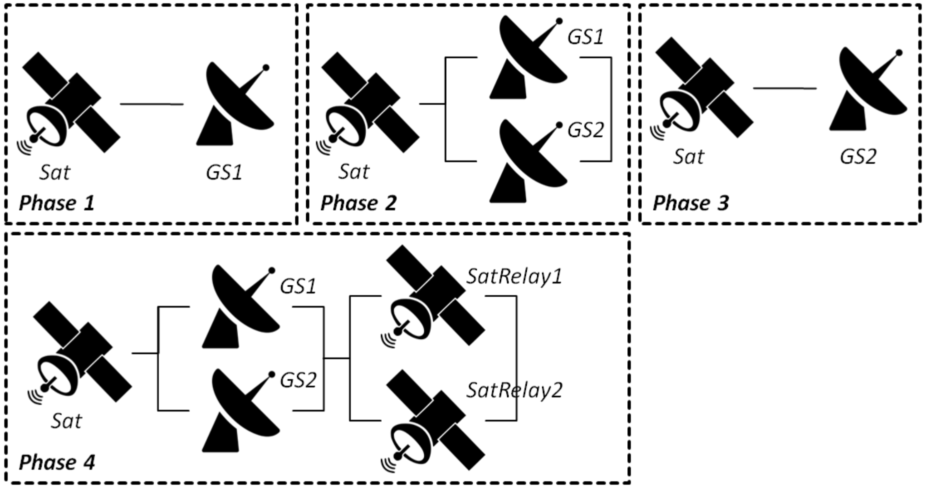
Exercise 1.b: **A repairable unit**

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

```

class RepairableComponent
  extends NonRepairableComponent;
  parameter Real pMu = 1.0e-2;
  event evRepair (delay = exponential(pMu));

  transition
    evRepair: not vsWorking -> vsWorking := true;

end
```



Case study: a satellite communication system

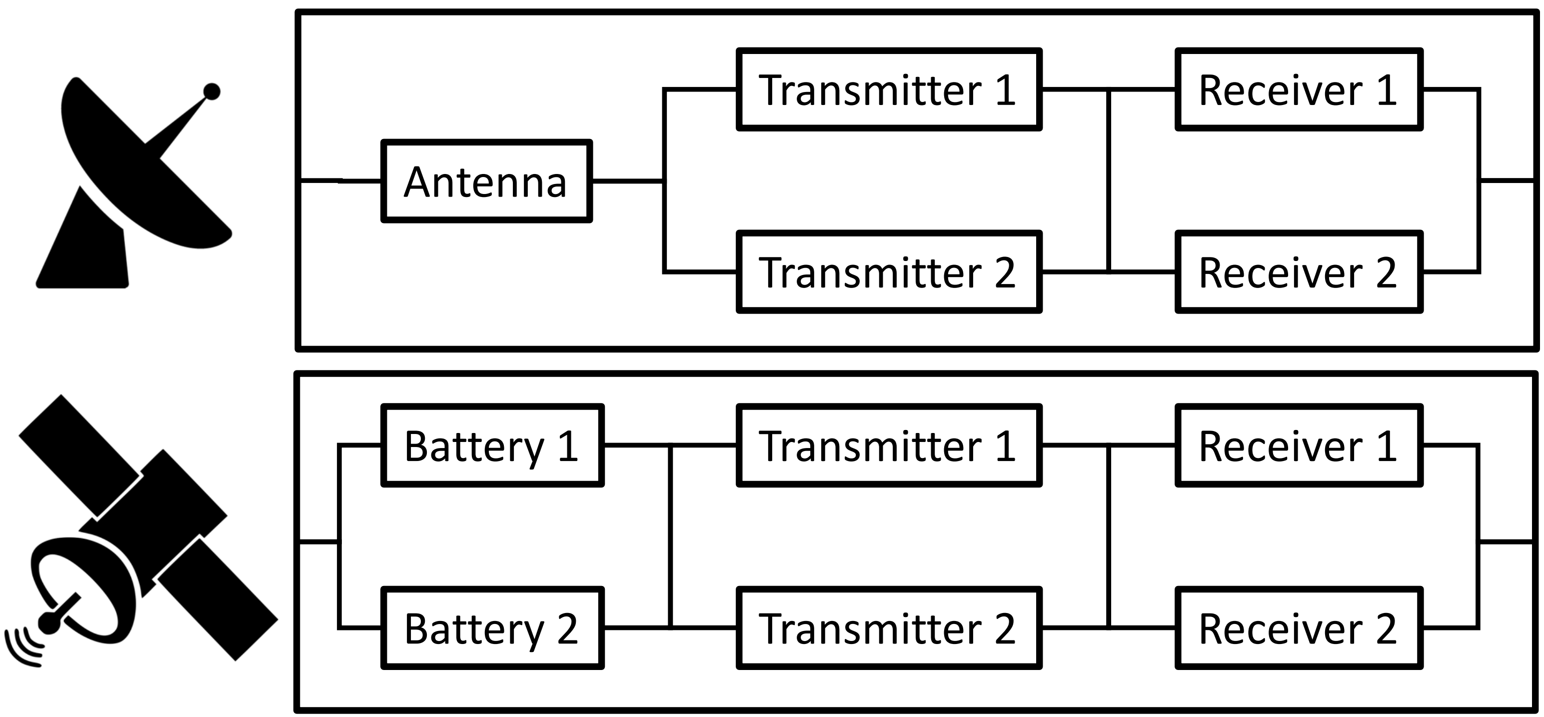


1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. **Modeling of reliability block diagrams**
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. Modeling of common cause failures
4. Modeling and assessment of static satellite communication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

Modeling of reliability block diagrams

Exercise 2:

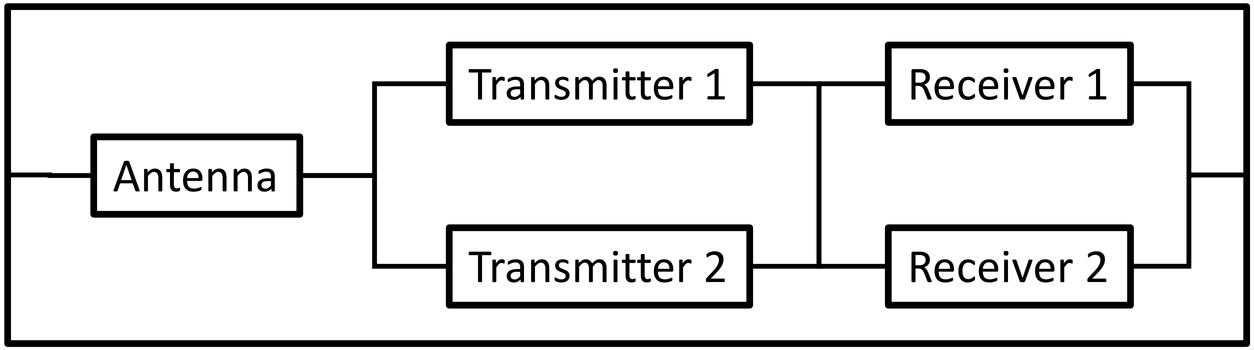
- Represent the following Reliability Block Diagrams in AltaRica 3.0



Guarded Transition Systems: composition

- The model for the system is obtained by **composing** smaller models of subsystems and components

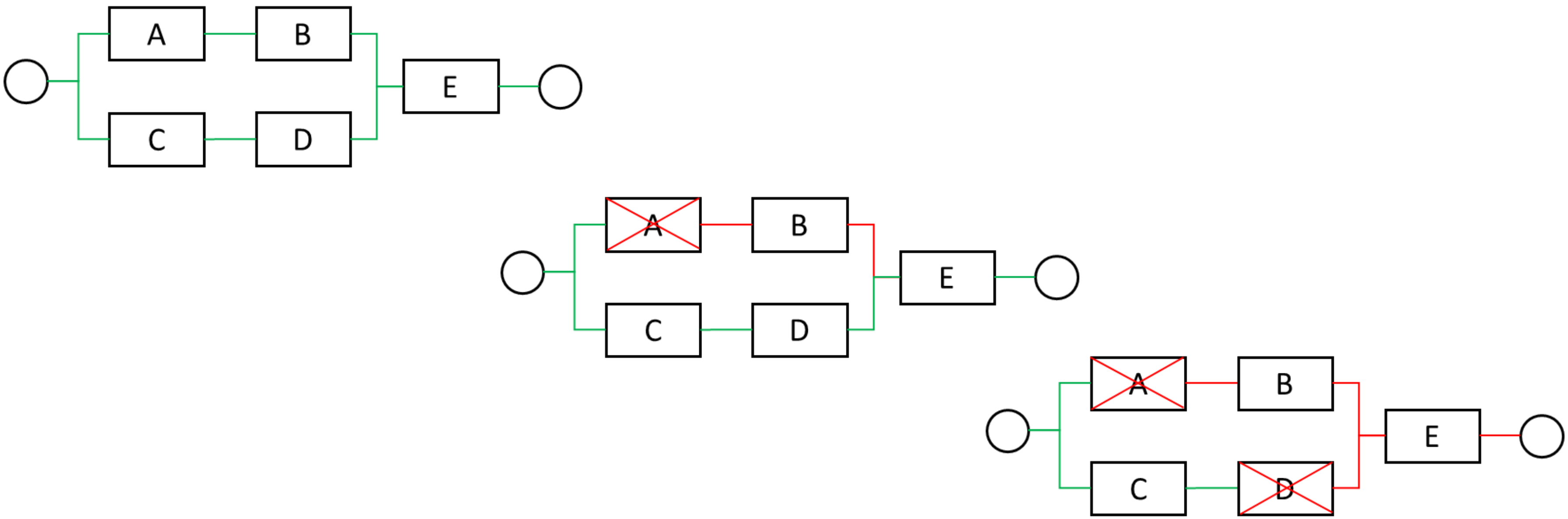
- This means that the model is an **implicit** representation of the state space



- Composition of two (or more) Guarded Transition Systems is also a Guarded Transition System

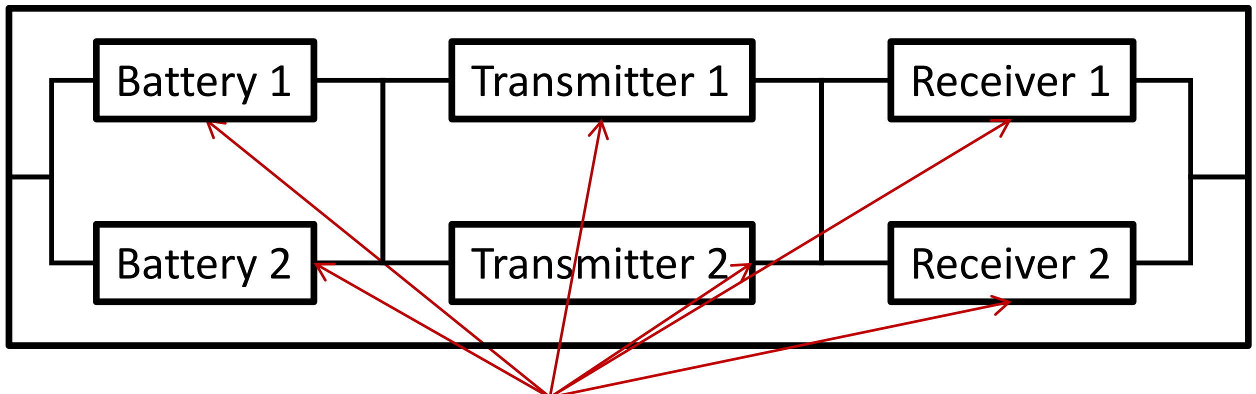
Guarded Transition Systems: flow propagation

- 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

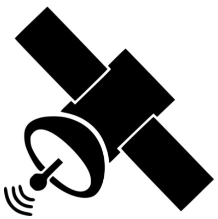


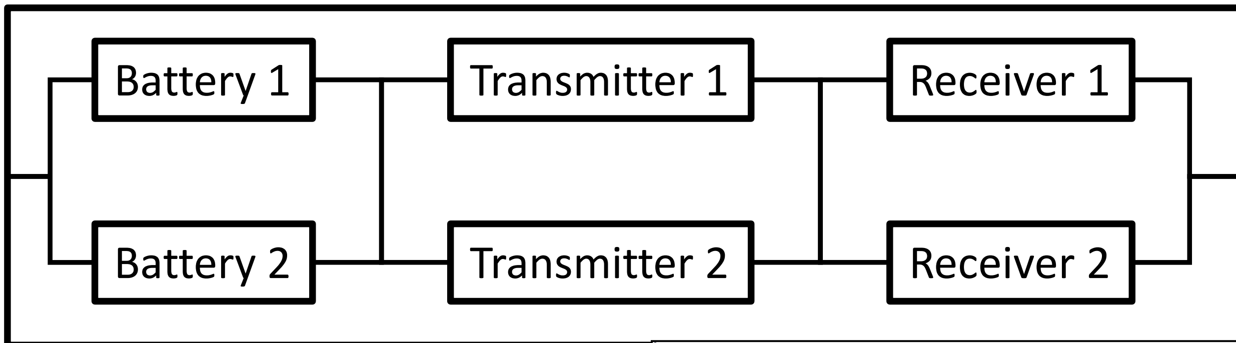

```
class NonRepairableInOutComponent
  extends NonRepairableComponent;
  Boolean vfInput, vfOutput(reset = false);
  assertion
    vfOutput := vsWorking and vfInput;
end
```

- **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



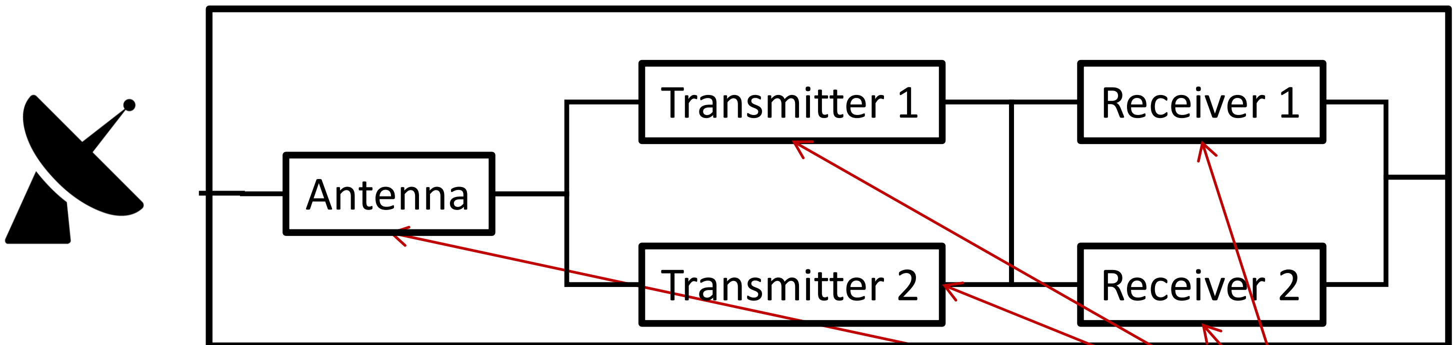



```
/*  Satellite subsystem
 *  represented by a block diagram modeling pattern with non
 */

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

    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

```

```

class NonRepairableInOutComponent
  extends NonRepairableComponent;
  Boolean vfInput, vfOutput(reset = false);
  assertion
    vfOutput := vsWorking and vfInput;
end

```

Modeling of Reliability Block Diagrams

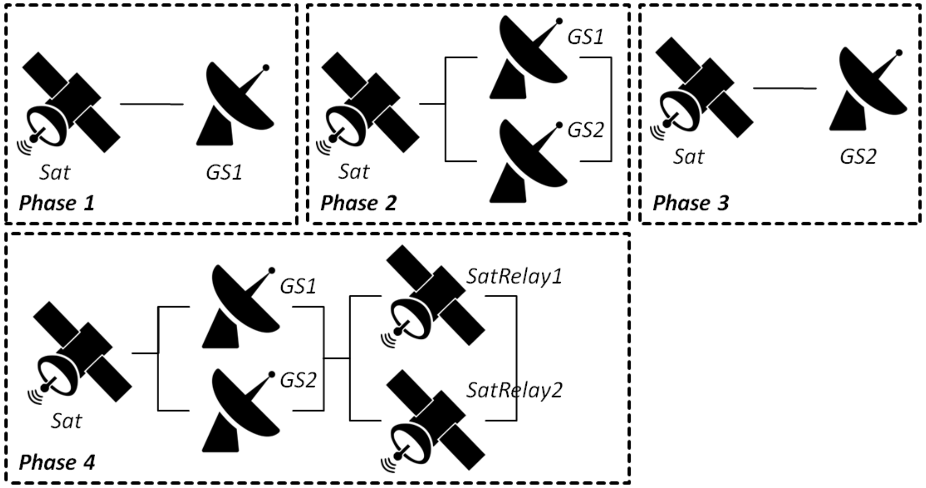
Exercise 2.b: Radar Reliability Block Diagram




```
/* Radar subsystem
*  represented by a block diagram modeling pattern with repair
*
*/
class RadarSubSystem
    parameter Real mu = 0.025;
    RepairableInOutComponent Antenna(pMu = mu);
    RepairableInOutComponent Transmitter1, Transmitter2(pMu = mu);
    RepairableInOutComponent 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;
end
```

```

class RepairableInOutComponent
  extends RepairableComponent;
  Boolean vfInput, vfOutput(reset = false);
  assertion
    vfOutput := vsWorking and vfInput;
end
```

Case study: a satellite communication system



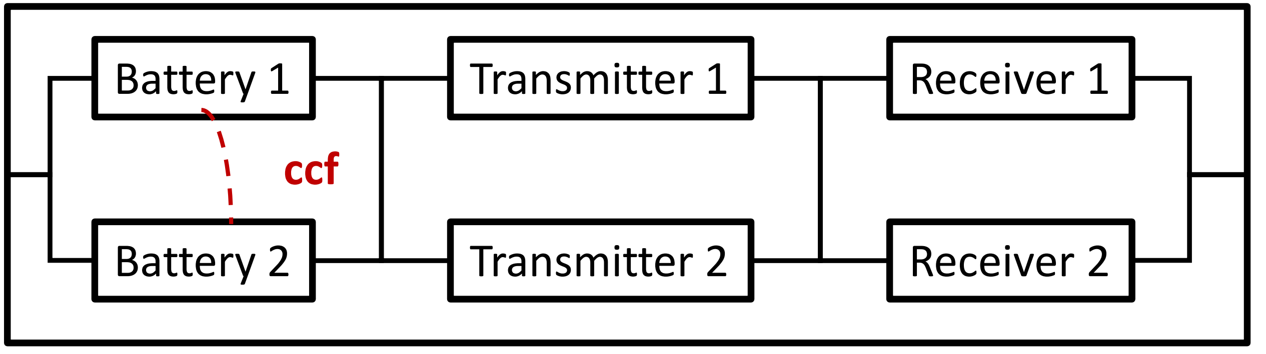
1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. Modeling of reliability block diagrams
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. **Modeling of common cause failures**
4. Modeling and assessment of static satellite communication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

Modeling of common cause failures

Exercise 3:

In the satellite subsystem given below batteries are subjected to a common cause failure with a failure rate ***ccfLambda = 1.0e-6***

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



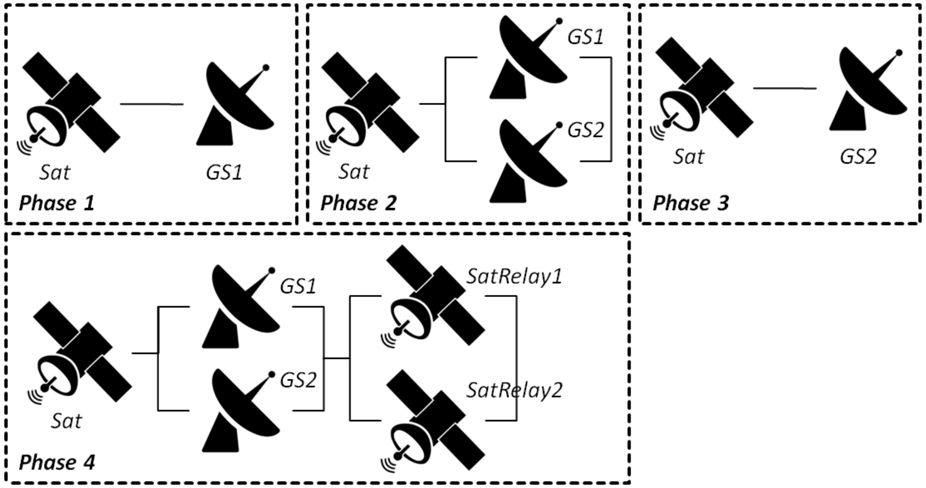
Modeling of common cause failures

Exercise 3: Common cause failure modeling

```

/*  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
        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
```

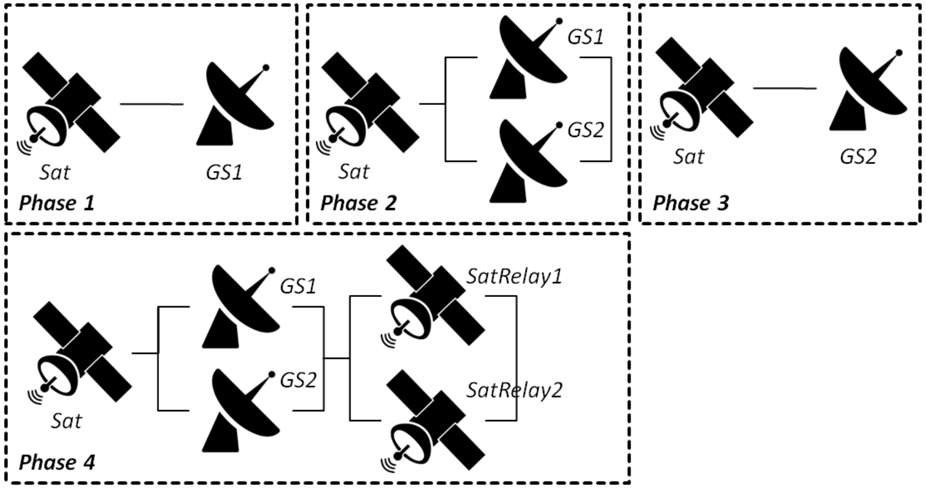
Synchronization

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)

Modeling and assessment of static satellite communication system



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

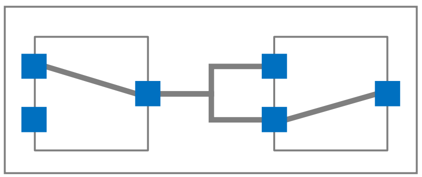
Exercise 4:

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

System Structure Modeling Language (S2ML)

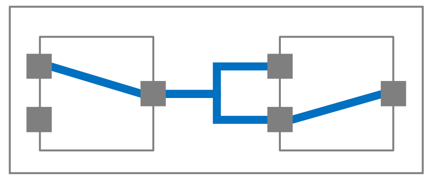
S2ML: a **structuring paradigm** that unifies **object** and **prototype-orientation**.

Port



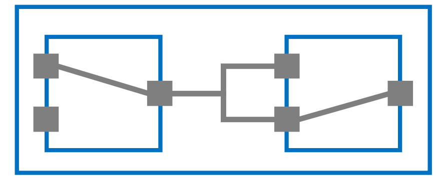
Variable, event…

Connection



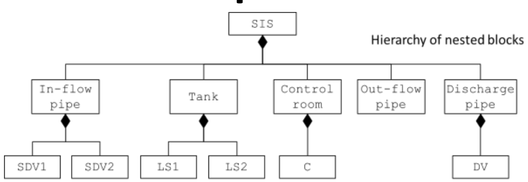
Equation, transition…

Container



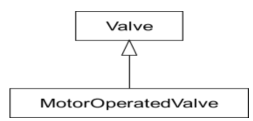
Model, component…

Composition



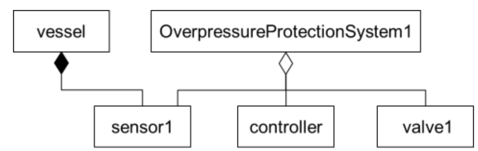
Is-part-of

Inheritance



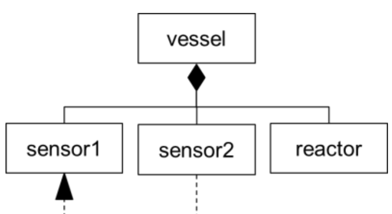
Is-a

Aggregation

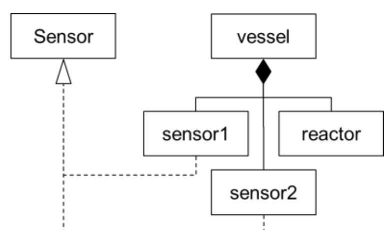


Uses

Prototype/Clone



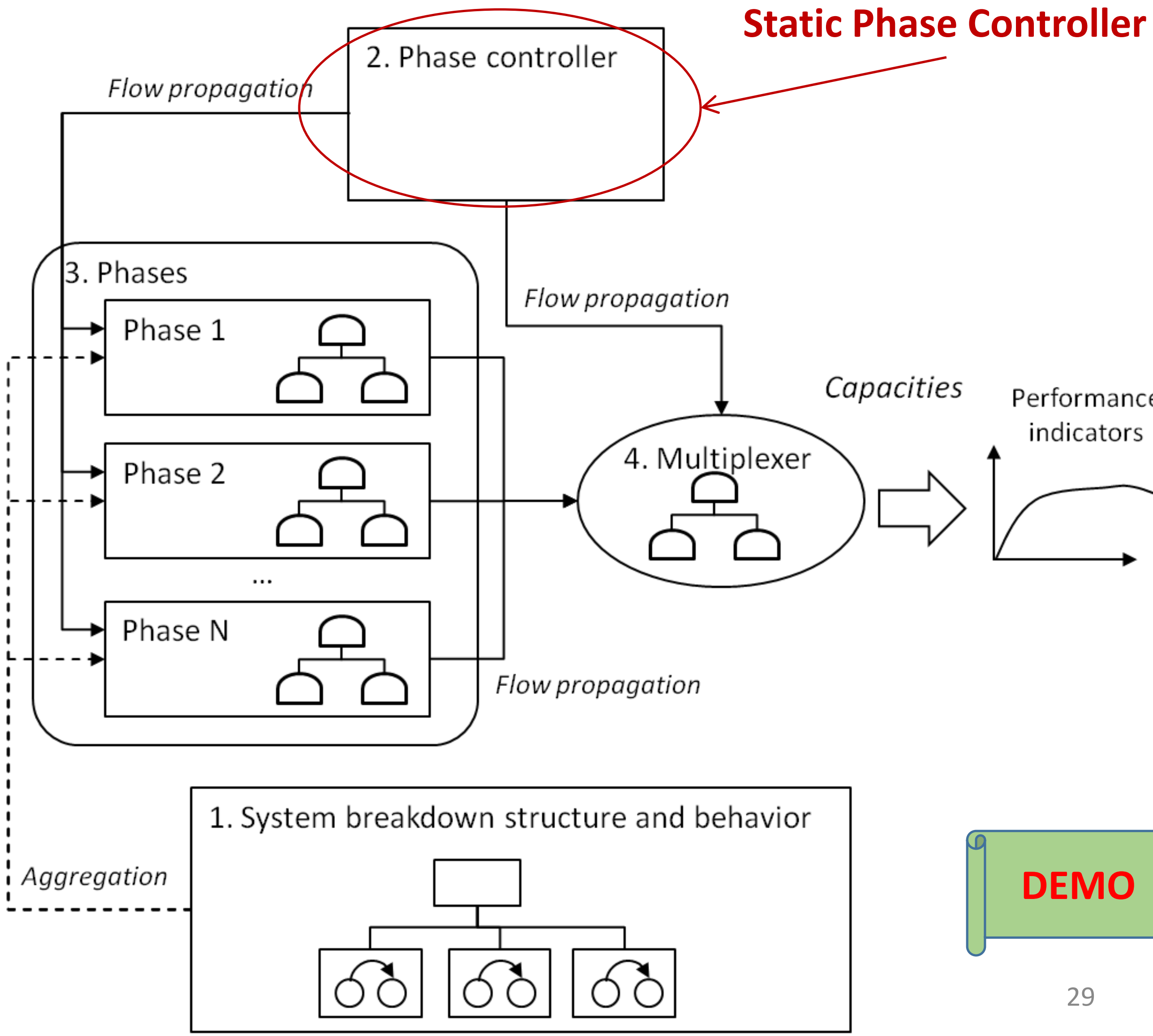
Class/Instance



M. Batteux, T. Prosvirnova, A. Rauzy, « From models of structures to structures of models », 4th IEEE International Symposium on Systems Engineering, Rome, Italy, 2018. **Best paper award.**

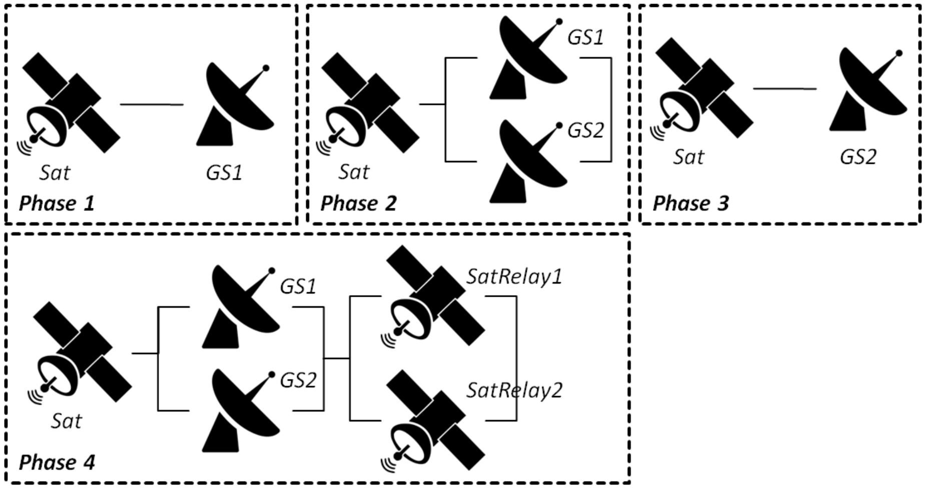
Exercise 4: Modeling and assessment

An **architectural pattern**



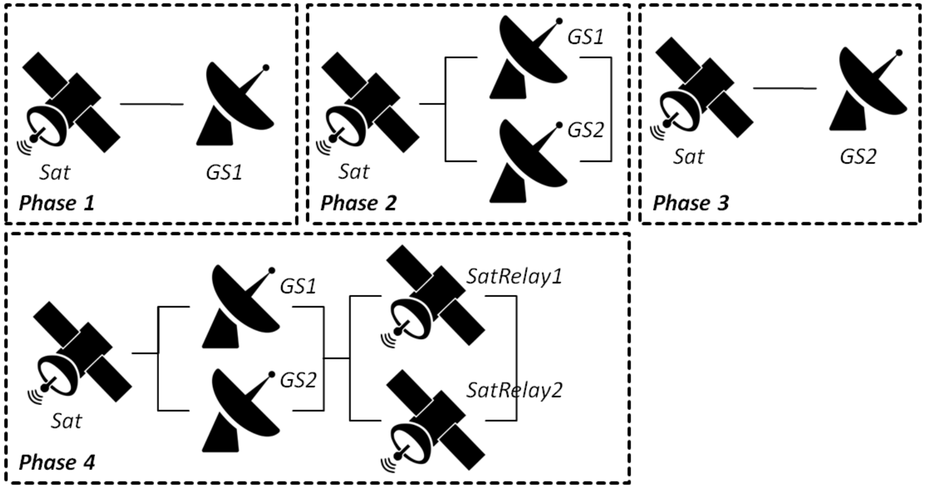
DEMO

Case study: a satellite communication system

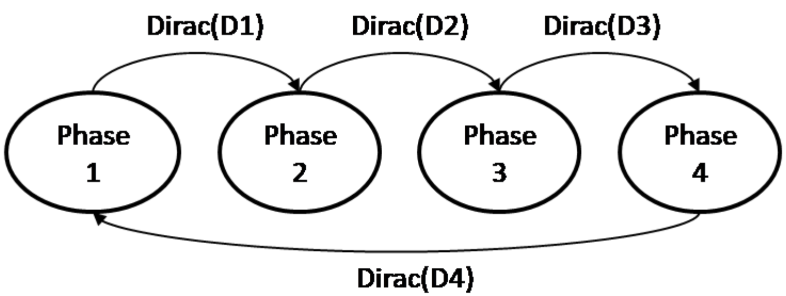


1. Modeling of components
   a. Non repairable unit
   b. Repairable unit
2. Modeling of reliability block diagrams
   a. Satellite reliability block diagram
   b. Ground station reliability block diagram
3. Modeling of common cause failures
4. Modeling and assessment of static satellite communication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

Modeling and assessment of dynamic satellite communication system



Parameters	Values
Phase duration	D1=D3=2h, D2=1h, D4=7h

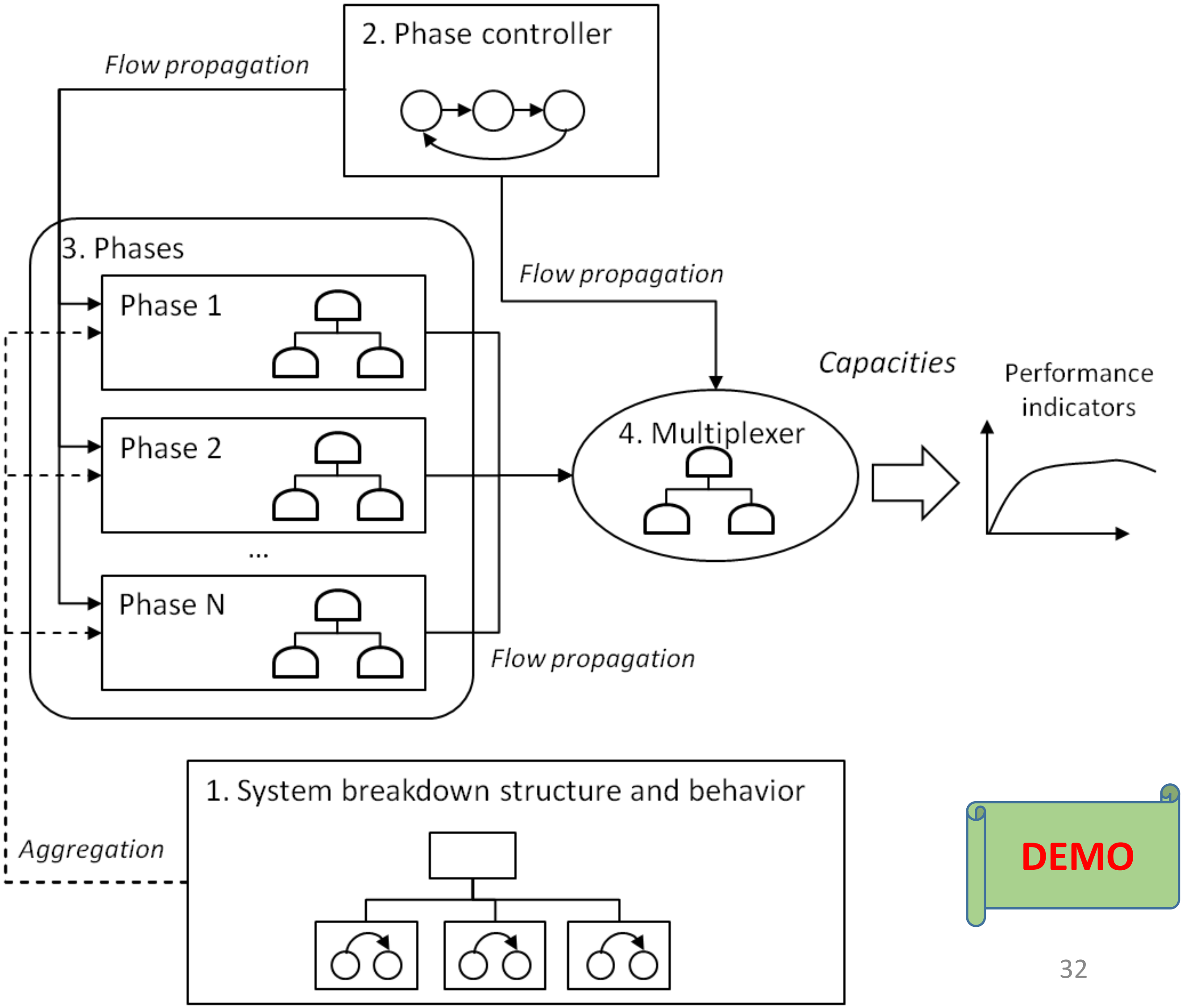


Exercise 5:

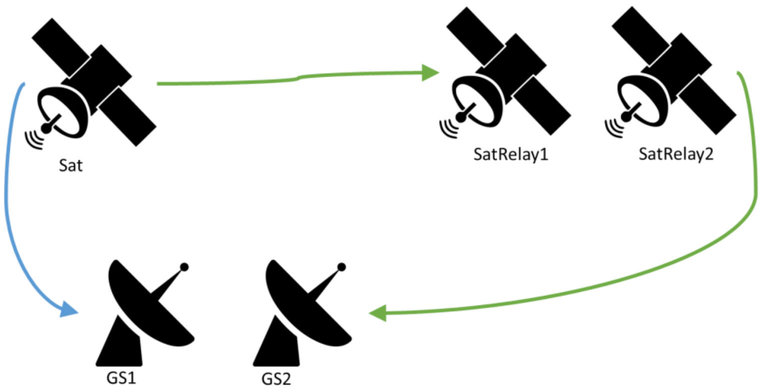
1. Modify the previous model of the satellite communication system to represent the behavior of the phase controller
2. Validate your model by simulation
3. Assess the reliability by stochastic simulation

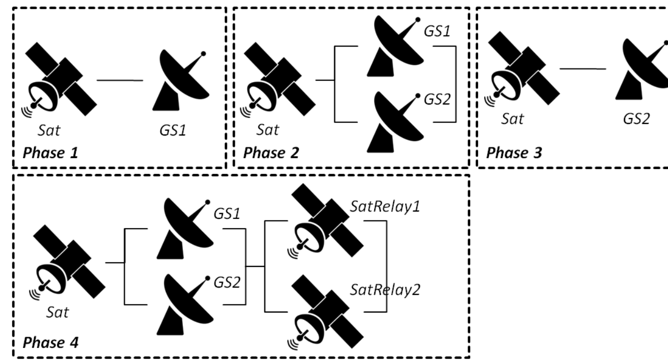
Exercise 5: Modeling and assessment

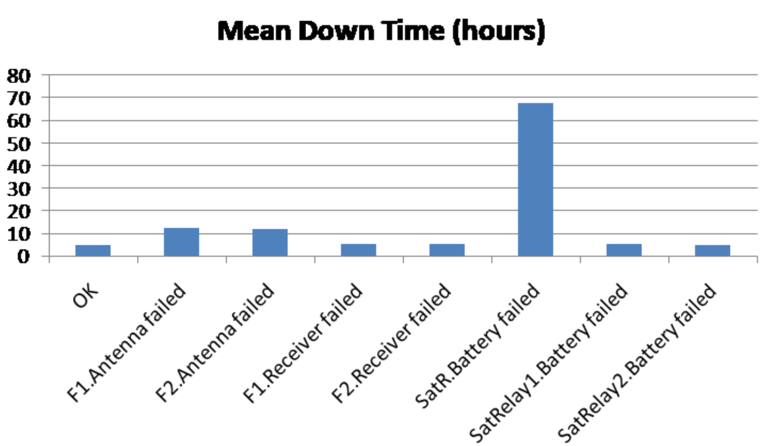
An **architectural pattern**

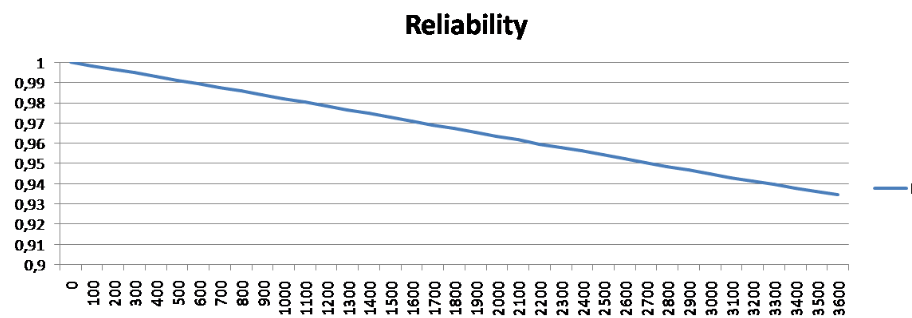


Exercise 5: Stochastic simulation





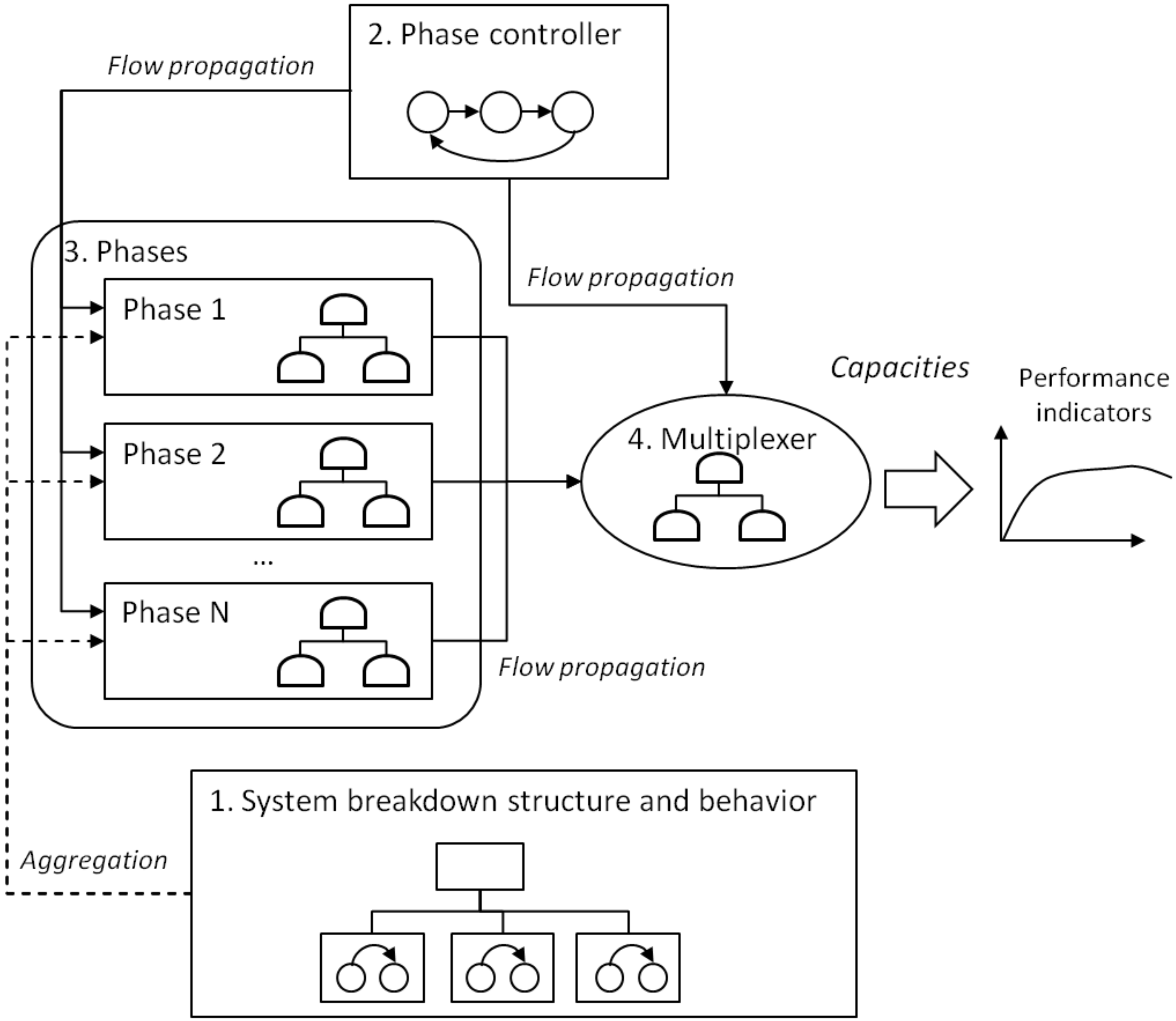




M. Batteux, T. Prosvirnova, A. Rauzy, and L. Yang. *Reliability assessment of phased-mission systems with AltaRica 3.0*. International Conference on System Reliability and Safety, Barcelona, Spain, November, 2018.

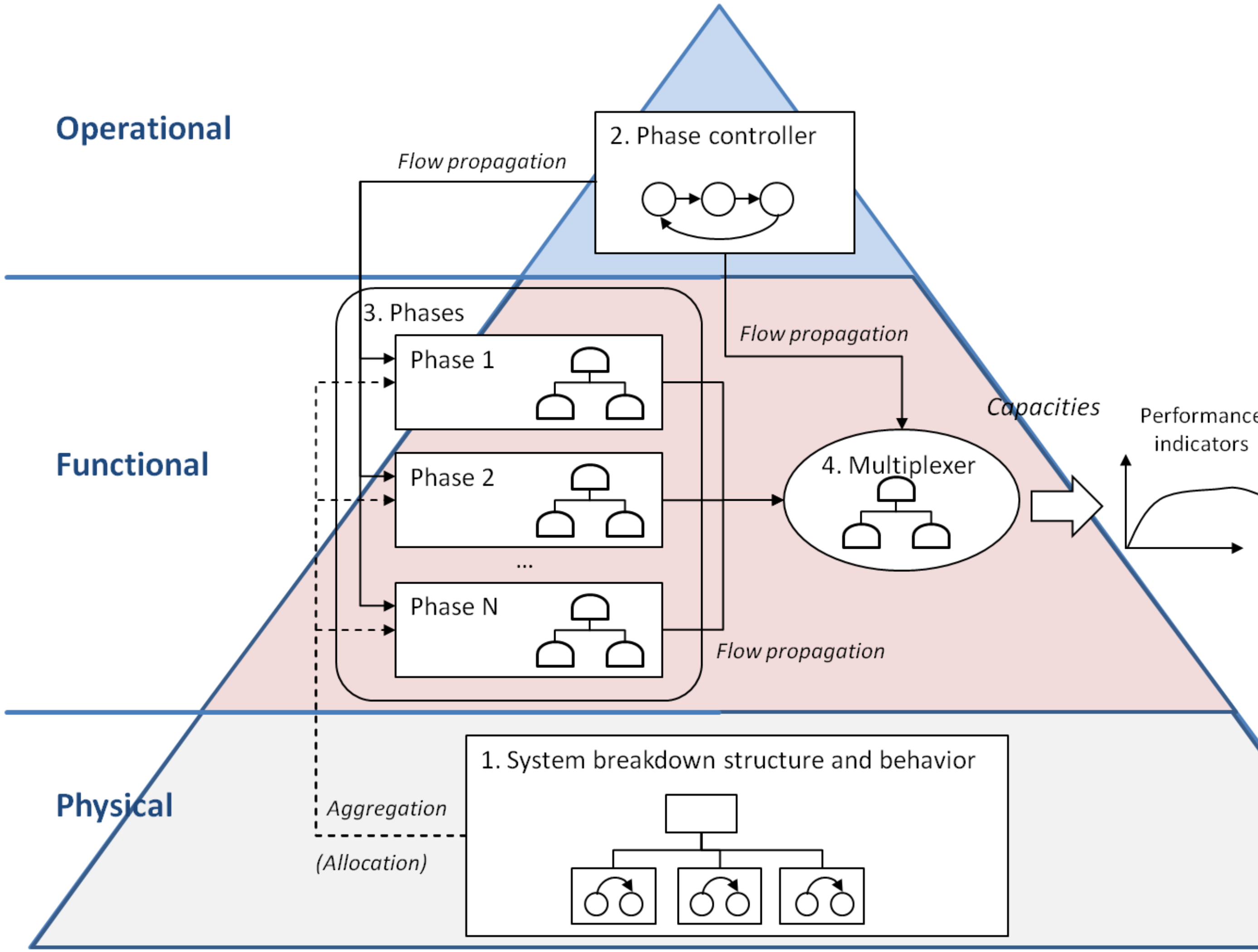
Links between System Architectures and Safety Analyses

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/

- Presented models and this presentation are available at http://www.altarica-association.org/contents/imbsa2019.html

References

- Antoine Rauzy. *Guarded Transition Systems: a new States/Events Formalism for Reliability Studies.* Journal of Risk and Reliability. Professional Engineering Publishing. 222:4. pp. 495–505. 2008. doi:10.1243/1748006XJRR177.
- Antoine Rauzy. *AltaRica 3.0 Specification*. Working Document (on demand).
- Michel Batteux, Tatiana Prosvirnova and Antoine Rauzy. *AltaRica 3.0 in 10 Modeling Patterns.* International Journal of Critical Computer-Based Systems (ISCCBS), 2018, in press.
- M. Batteux, T. Prosvirnova, A. Rauzy. *From models of structures to structures of models*, 4th IEEE International Symposium on Systems Engineering, Rome, Italy, 2018.

Tutorial examples of AltaRica 3.0

- Frédéric Milcent, Tatiana Prosvirnova and Antoine Rauzy. *Modélisation des réseaux en AltaRica 3.0*. Actes du congrès Lambda-Mu 19 (actes électroniques). Institut pour la Maîtrise des Risques. ISBN 978-2-35147-037-4. Dijon, France. October, 2014.
- Hala Mortada, Tatiana Prosvirnova and Antoine Rauzy. *Safety Assessment of an Electrical System.* Proceedings of the 4th International Symposium on Model-Based Safety Assessment, IMBSA 2014. Springer Verlag. 8822. pp. 181–194. Munich, Germany. October, 2014.
- Abraham Cherfi, Michel Leeman and Antoine Rauzy. *AltaRica 3.0 Based Models for ISO 26262 Automotive Safety Mechanisms.* Proceedings of the 4th International Symposium on Model-Based Safety Assessment, IMBSA 2014. Springer Verlag. 8822. pp. 123–136. Munich, Germany. October, 2014.
- M. Batteux, T. Prosvirnova, A. Rauzy, and L. Yang. *Reliability assessment of phased-mission systems with AltaRica 3.0* . International Conference on System Reliability and Safety, Barcelona, Spain, November, 2018.

References

Compilation of AltaRica (GTS) into Fault Trees

- Antoine Rauzy. *Modes Automata and their Compilation into Fault Trees.* Reliability Engineering and System Safety. Elsevier. 78:1. pp. 1–12. October, 2002.doi:10.1016/S0951-8320(02)00042-X.
- Tatiana Prosvirnova and Antoine Rauzy. *Automated generation of Minimal Cutsets from AltaRica 3.0 models.* International Journal of Critical Computer-Based Systems. Inderscience Publishers. 6:1. pp. 50–79. 2015.doi:10.1504/IJCCBS.2015.068852.
- Michel Batteux, Tatiana Prosvirnova and Antoine Rauzy. *Advances in the simplification of Fault Trees automatically generated from AltaRica 3.0 models. 28th European Safety and Reliability Conference ESREL (ESREL 2018)*, Trondheim, Norway, June, 2018.

Compilation of AltaRica (GTS) into Markov chains

- Pierre-Antoine Brameret, Antoine Rauzy and Jean-Marc Roussel. *Automated generation of partial Markov chain from high level descriptions.* Reliability Engineering and System Safety. Elsevier. 139. pp. 179–187. July, 2015. doi:10.1016/j.ress.2015.02.009.

AltaRica tools

- Michel Batteux, Tatiana Prosvirnova and Antoine Rauzy. *AltaRica Wizard: an integrated modeling and simulation environment for AltaRica 3.0*. Actes du congrès Lambda-Mu 21 (actes électroniques). Institut pour la Maîtrise des Risques, Reims, Octobre, 2018.