GROUPE RENAULT

10th EDITION EUROPEAN CONGRESS
ERTS 2020

TELECOM Paris
IP PARIS

TOWARDS FORMAL VERIFICATION IN AUTOMOTIVE

APPLIED TO THE AUTONOMOUS DRIVING SUPERVISION FUNCTION

ERTS 2020 - 30 JANUARY

Authors :

- **YASMINE ASSIOUA,** ***RENAULT SOFTWARE LABS & TELECOM PARIS***
- RABEA AMEUR-BOULIFA, *TELECOM PARIS*
- PATRICIA GUITTON-OUHAMOU, *RENAULT SOFTWARE LABS*

AGENDA

01 **CONTEXT**
INTRODUCTION

02 **APPROACH**
THE USE OF FORMAL SPECIFICATION AND FORMAL VERIFICATION TO PROVE THE RELIABILITY OF THE STUDIED SYSTEMS

03 **MODEL'S CONSTRUCTION**
THE DIFFERENT STEPS TO TRANSFORM INFORMAL REQUIREMENT INTO A FORMAL MODEL (STATE MACHINE) FOR FORMAL VERIFICATION APPLIED TO AD (AUTONOLOUS DRIVING) SUPERVISION

04 **VERIFICATION**
THE USE OF A MODEL CHECKER (UPPAAL) TO VERIFY IF THE GENERATED MODEL USING PROPERTIES AND SIMULATION

05 **CONCLUSION**
ACHIEVEMENTS & PERSPECTIVES

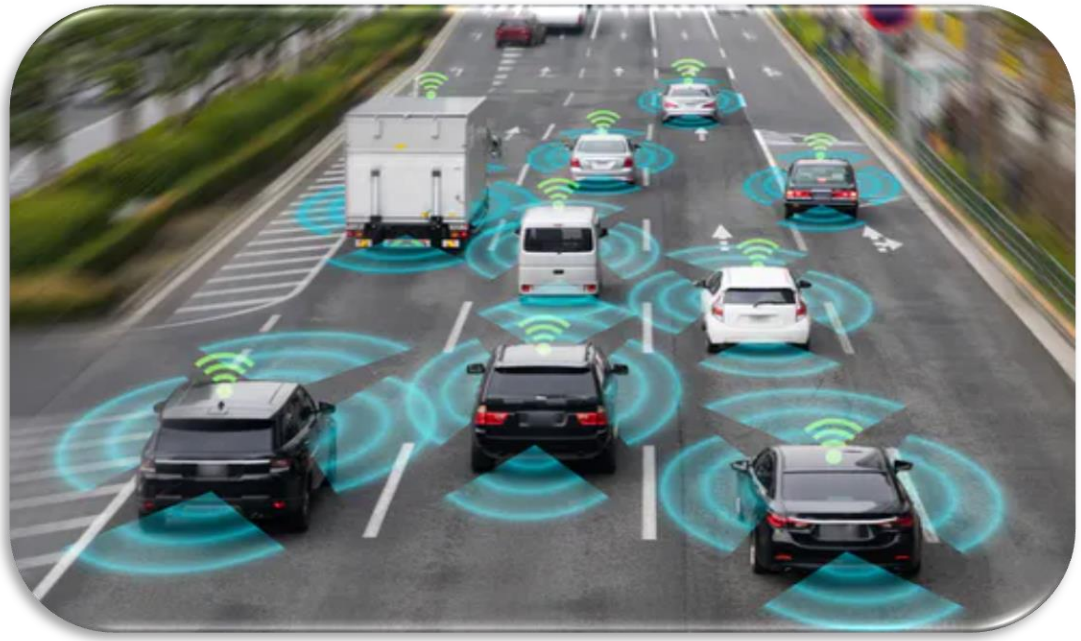
01

CONTEXT

Introduction

INTRODUCTION

- Rapid development of autonomous vehicles
- Complex system evolving in an unpredictable environment
- Comply to strict standards and norms (AUTOSAR, ISO26262)



BUG CONSEQUENCES

- A failure can cause severe accidents
- High cost (Brand, Recall, Bug's correction,…)
- **Essential to ensure the quality of the requirements**

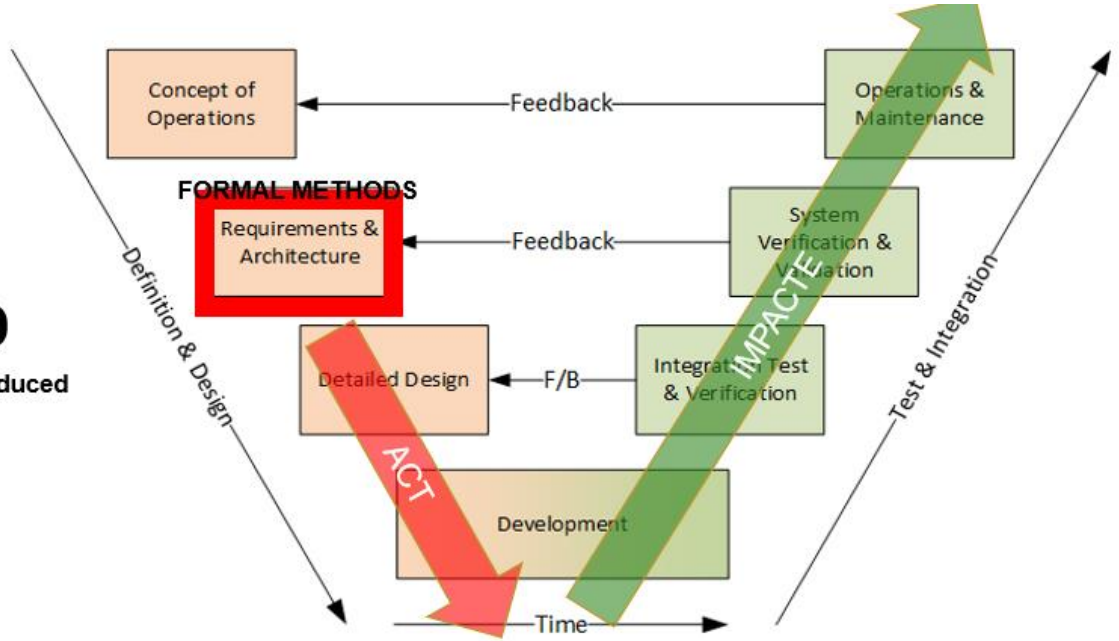
Critical System = *deal with scenarios that may lead to* ***loss of life****, serious personal injury, or damage to the natural environment*

REDUCE BUGS

- **Early Validation**
- Rigorous Model-Based approach
- Using formal methods
- Goal:
  - Improve SW quality
  - Reduce time to market
  - Reduce costs

64%

of bugs are introduced



The V-Model: Systems development lifecycle

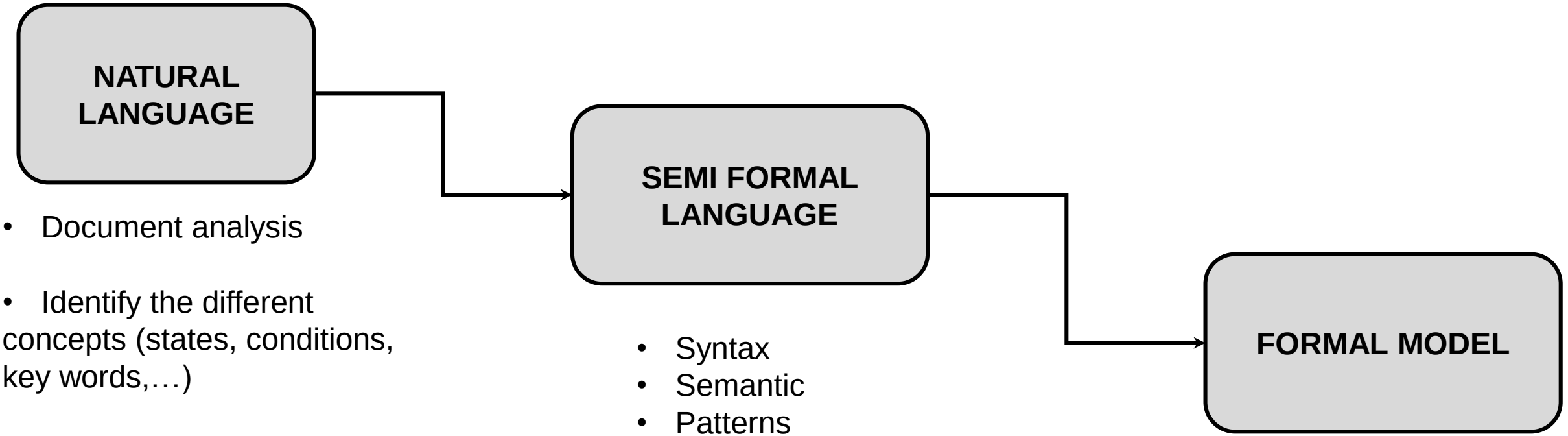
Source :
Software engineering environments: concepts and technology
Robert N. Charette

02

APPROACH

The use of formal specification and formal verification to prove the reliability of the studied systems

THE APPROACH

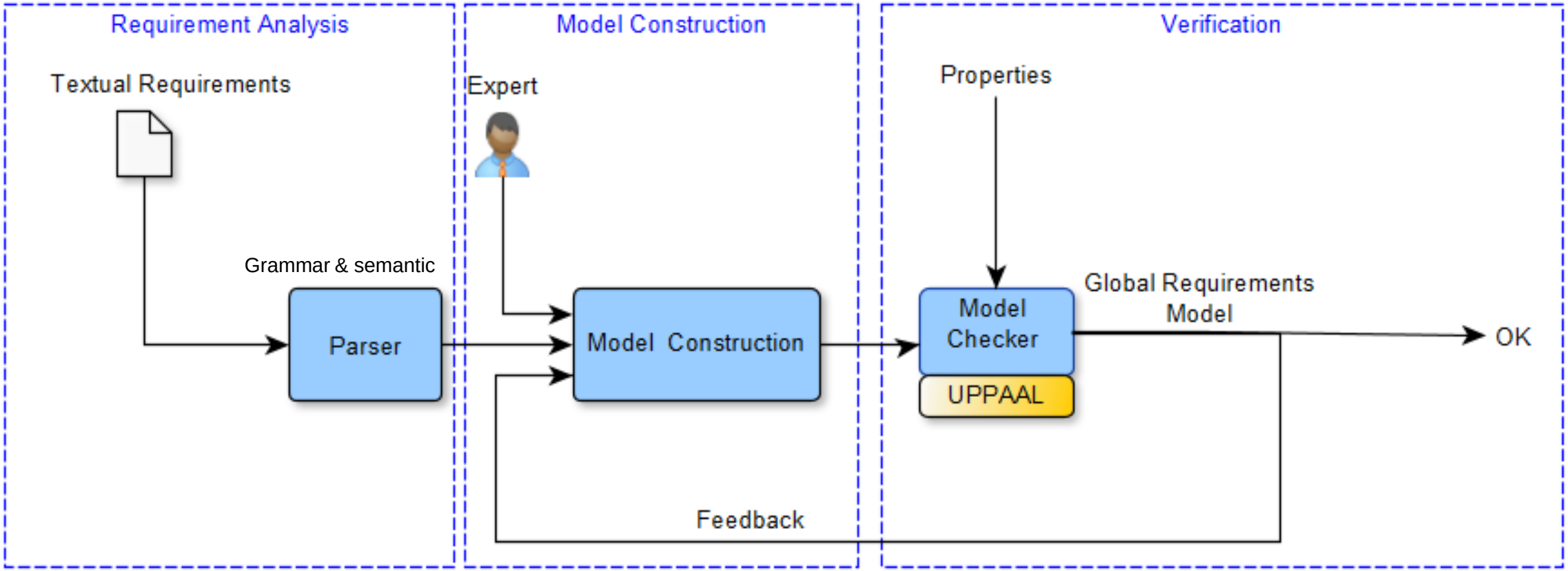


- Document analysis
- Identify the different concepts (states, conditions, key words,…)

- Syntax
- Semantic
- Patterns

- Automata
- Model checking
- Properties verification

OUR FRAMEWORK



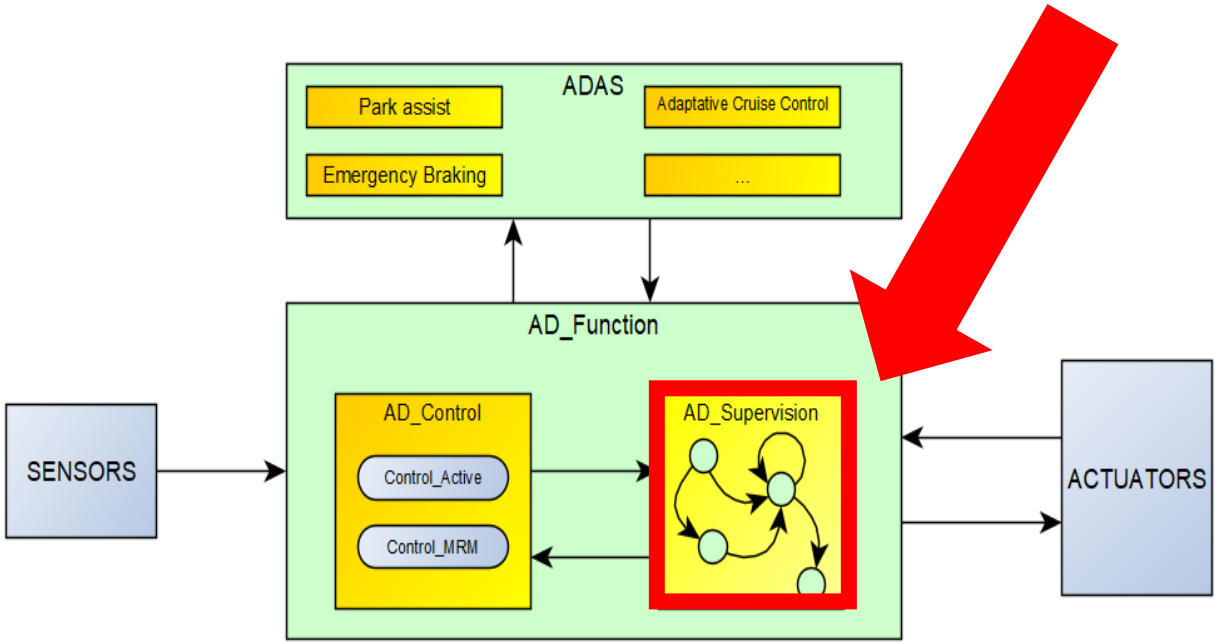
03

MODEL CONSTRUCTION

The different steps to transform informal requirement into a formal model (state machine) for formal verification applid to AD (Autonomous driving supervision)

CASE STUDY

THE AUTONOMOUS DRIVING (AD) FUNCTION SPECIFIES A SELF DRIVING CAR

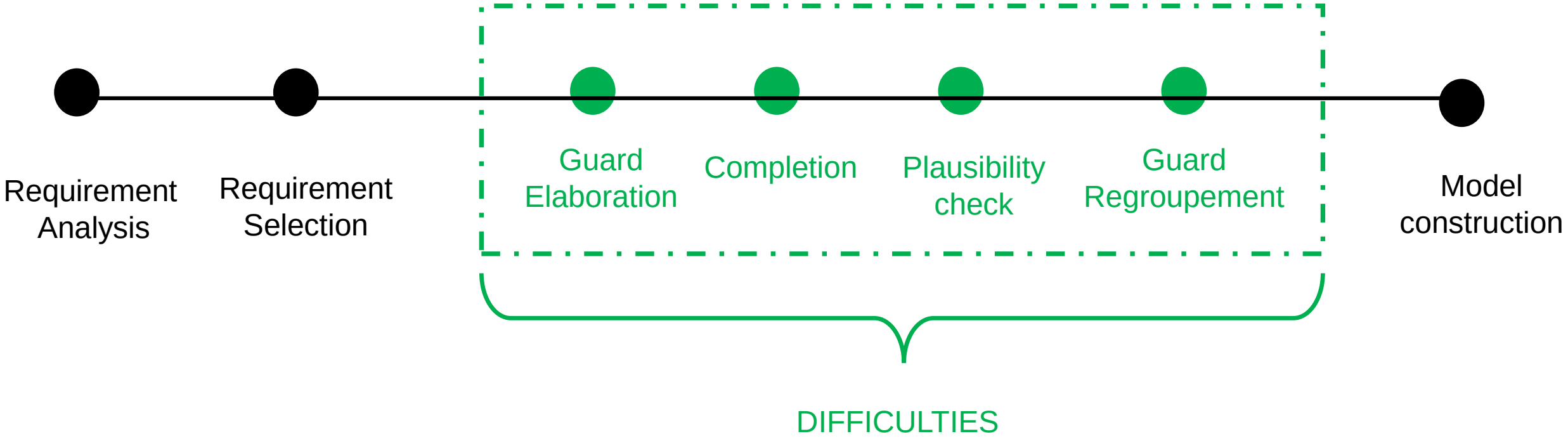


Control function specifies the Autonomous driving function behavior

Surpervision function gives or takes back the **control** from AD_Control

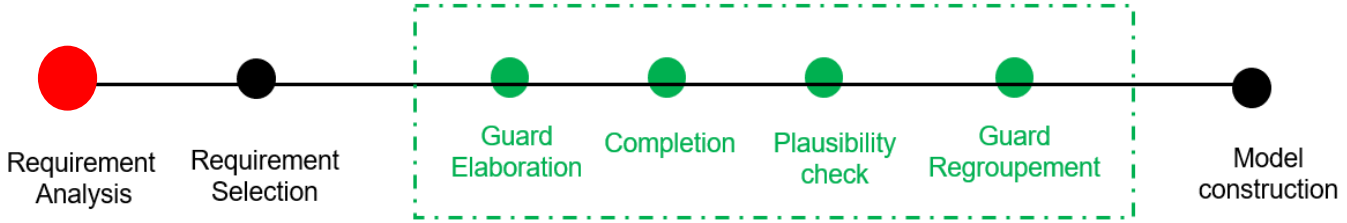
STEPS

The model construction follows different steps:



Some steps are recursive

REQUIREMENTS ANALYSIS



"The lateral jerk requested by the AD-function shall be limited to a threshold" (**FR1**)

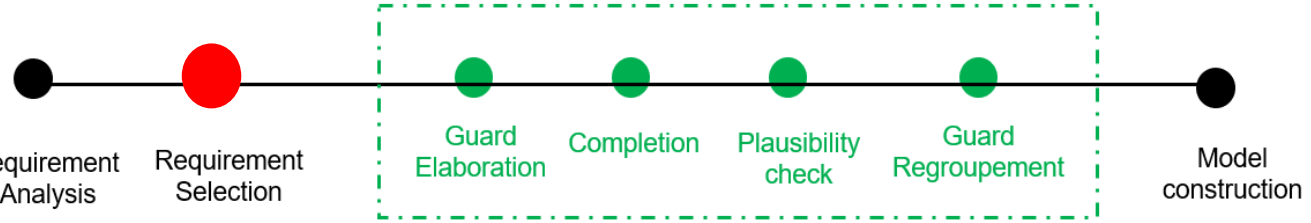
"AD-function shall be available at dawn and dusk" (**FR2**)

"AD-function shall be available on verified road sections" (**FR3**)

"IF AD-function is not available and vehicle is in Germany or in France then AD-function shall be available" (**FR4**)

Function's name | State's name | Condition | Key words

REQUIREMENT SELECTION



"The lateral jerk requested by the AD-function shall be limited to a threshold" (**FR1**)

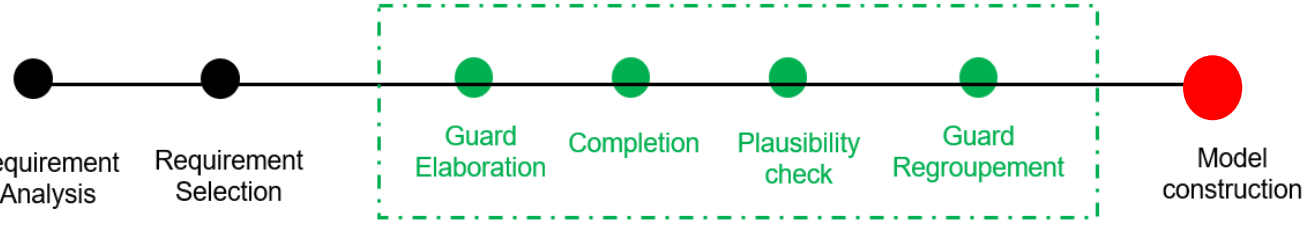
"AD-function shall be available at dawn and dusk" (**FR2**)

"AD-function shall be available on verified road sections" (**FR3**)

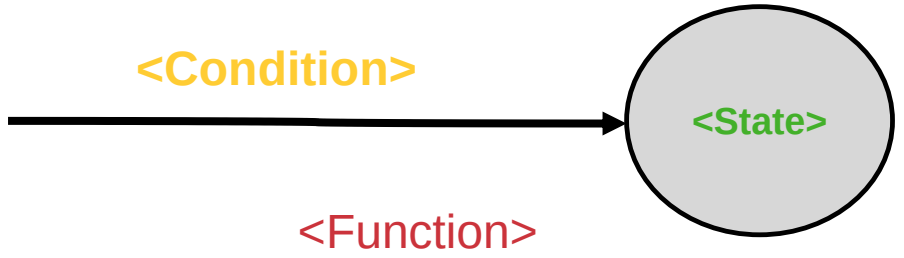
"IF AD-function is not available and vehicle is in Germany or in France then AD-function shall be available" (**FR4**)

Function's name | State's name | Condition | Key words

MODEL CONSTRUCTION



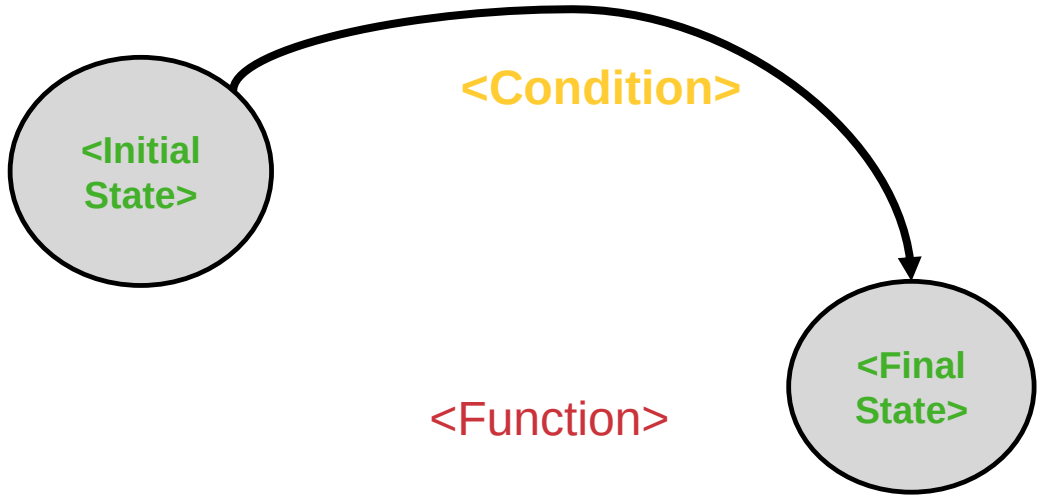
<Function> **SHALL BE** **< State>** **<Condition>**



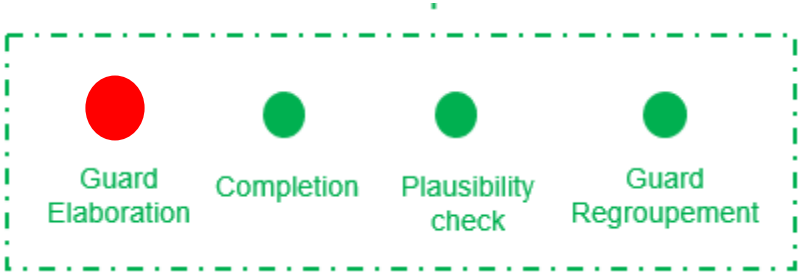
IF <Function> is in **<Initial State>**

AND **<Condition>**

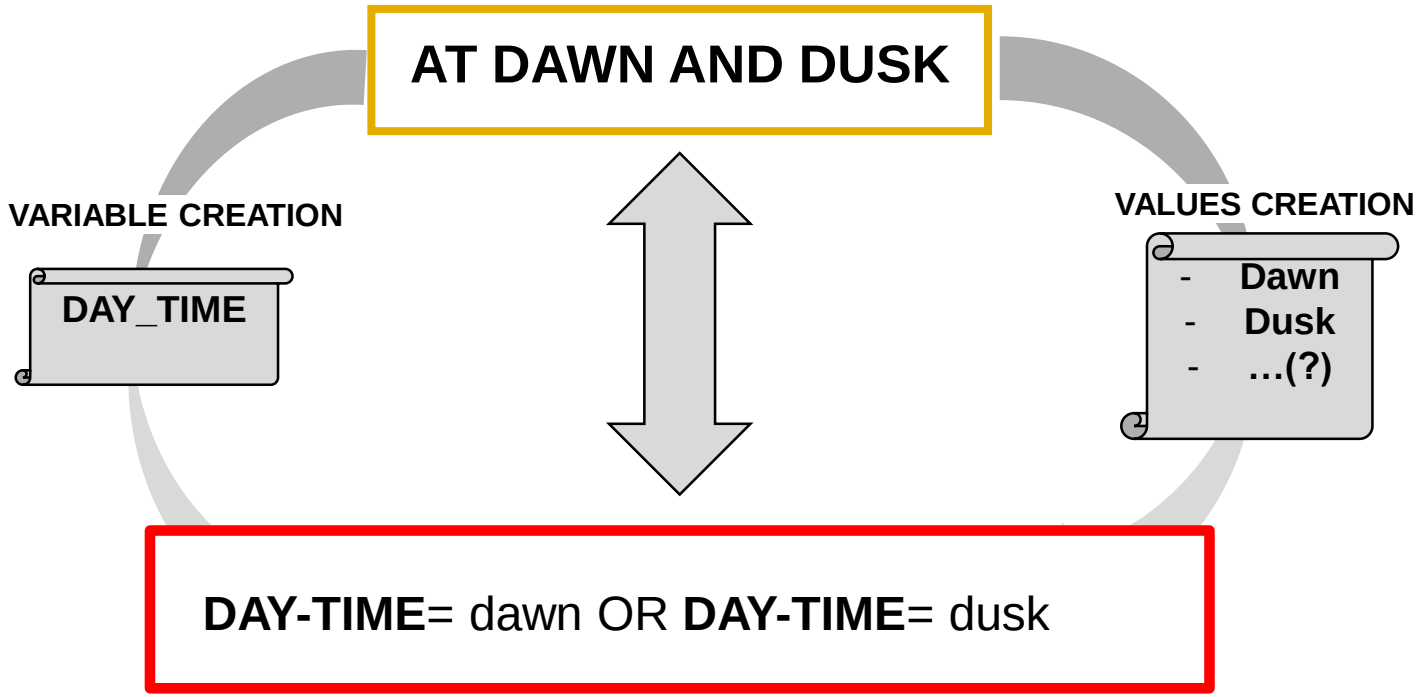
THEN <Function> **SHALL BE** **<Final State>**



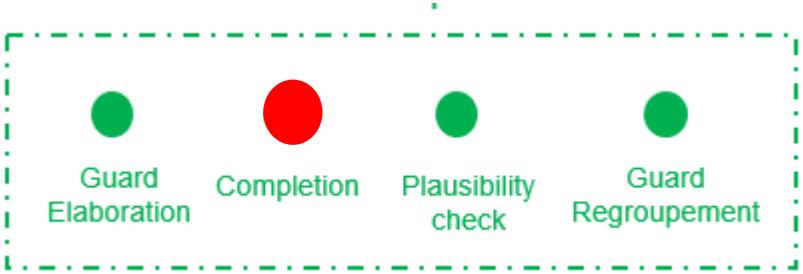
GUARDS ELABORATION



"AD-function shall be available at dawn and dusk" (FR3)

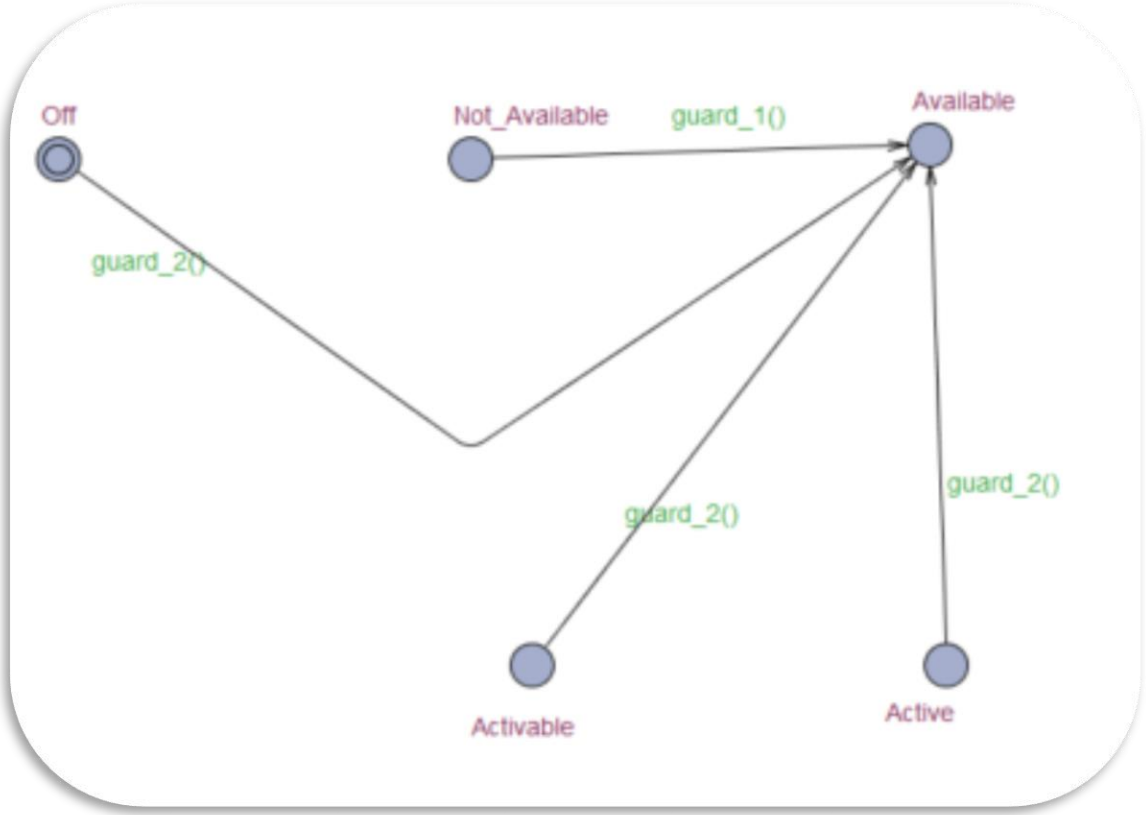


COMPLETION

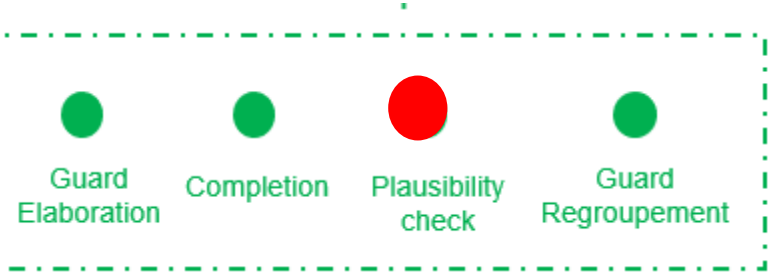


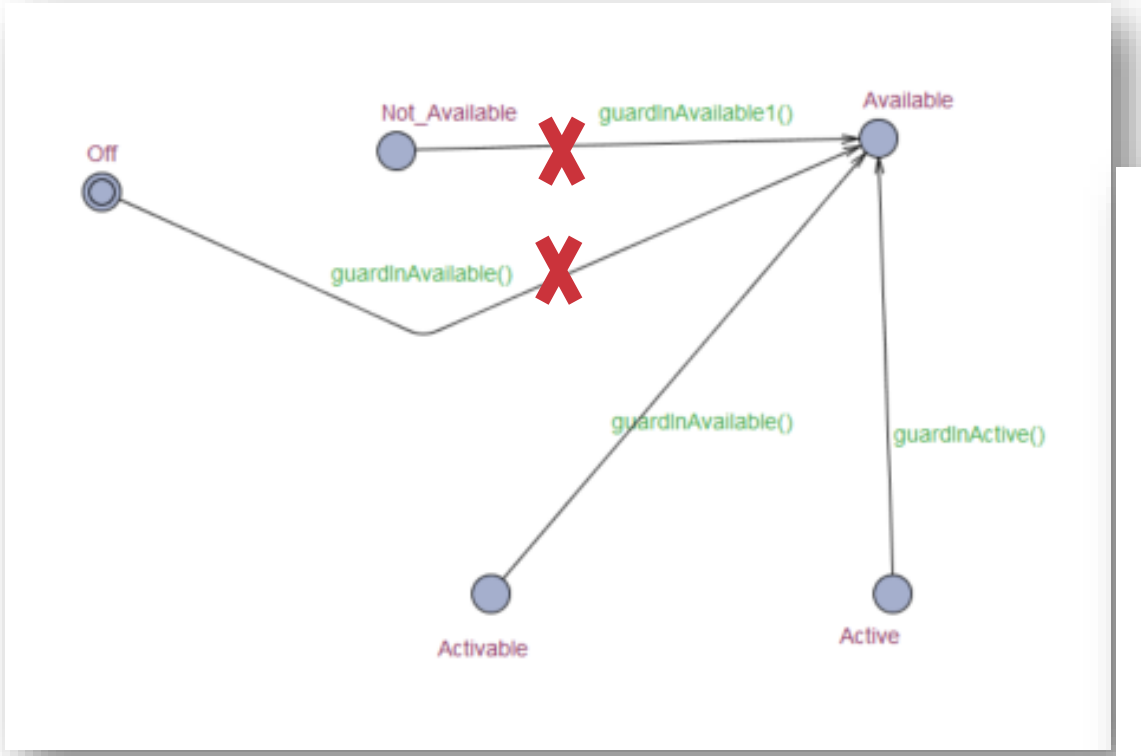
Possible states:
OFF, NOT_AVAILABLE, AVAILABLE, ACTIVABLE, ACTIVE

AD-function shall be available **IF** DAY-TIME = dawn OR DAY-TIME = dusk



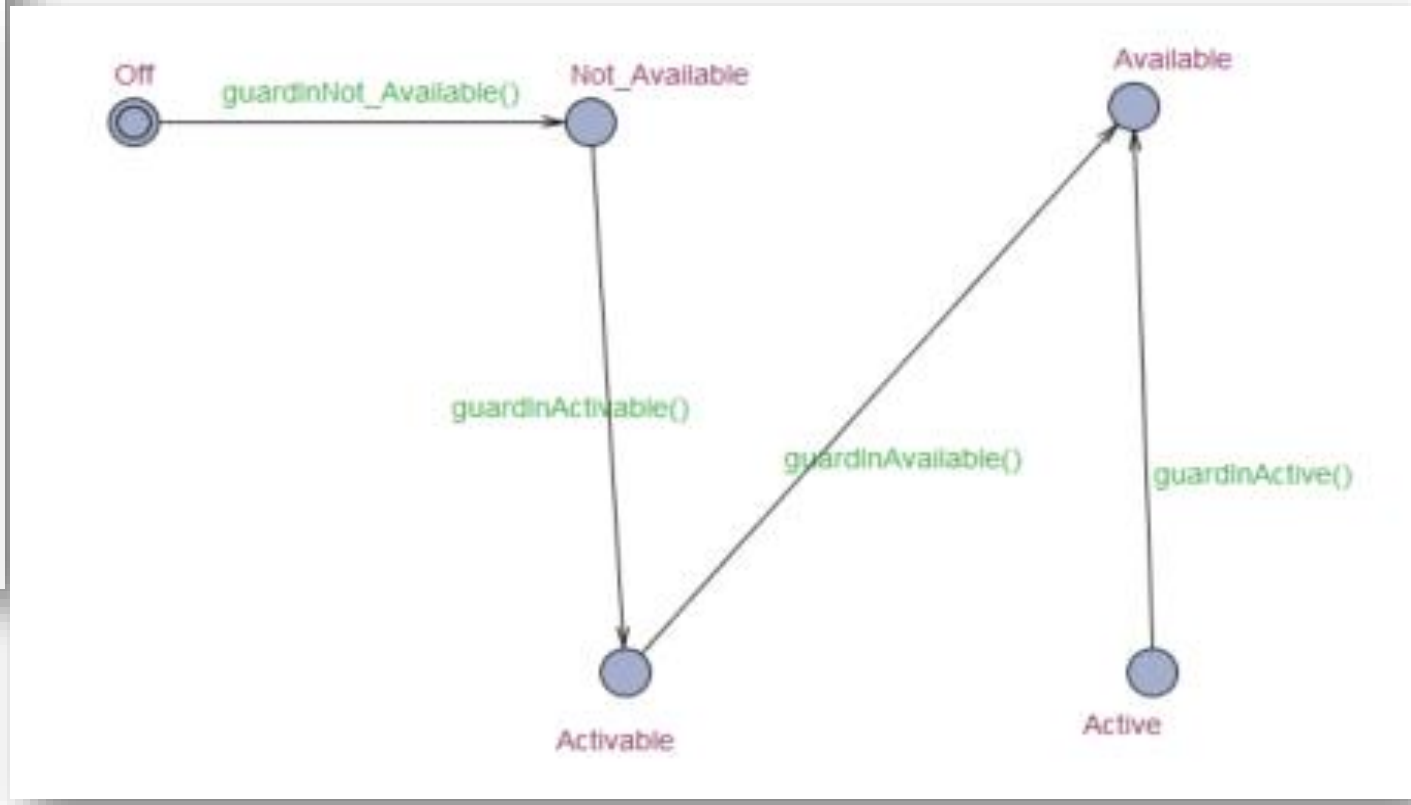
PLAUSIBILTY CHECK



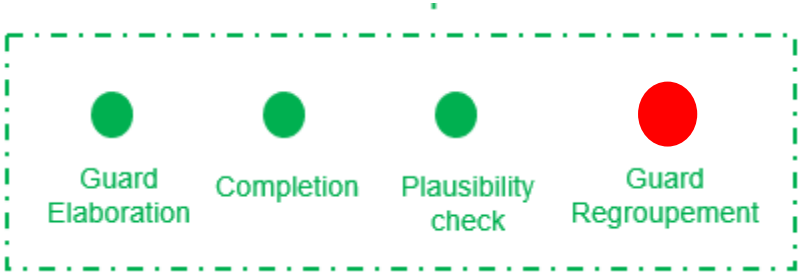


CORRECTION

Using the Plausibilty Table

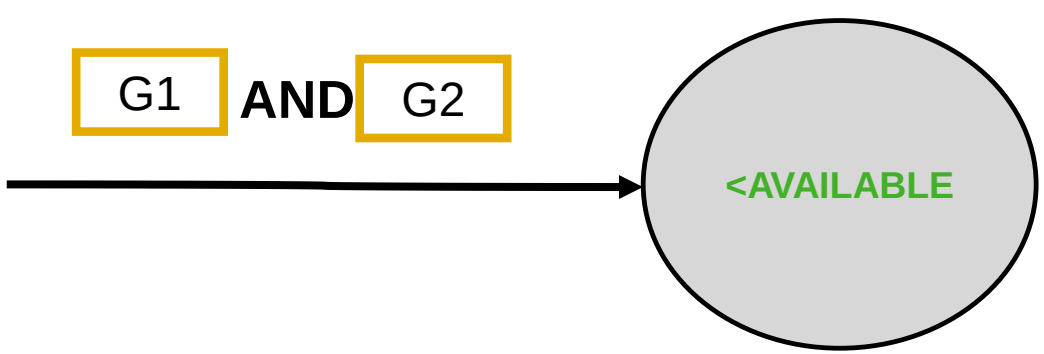


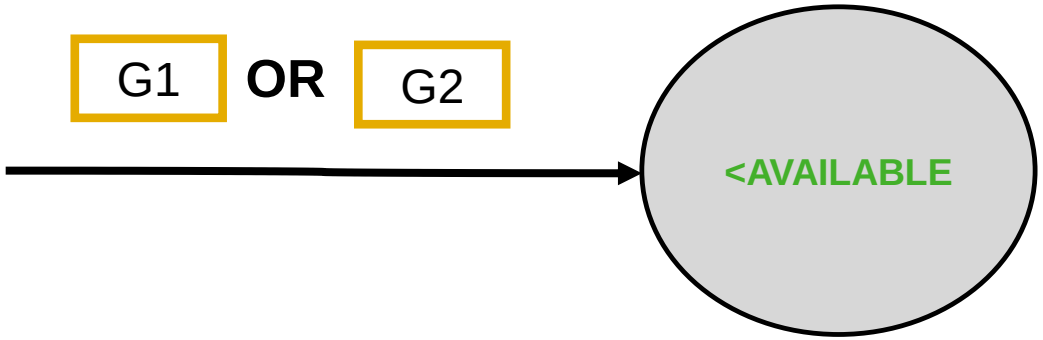
GUARDS REGROUPEMENT



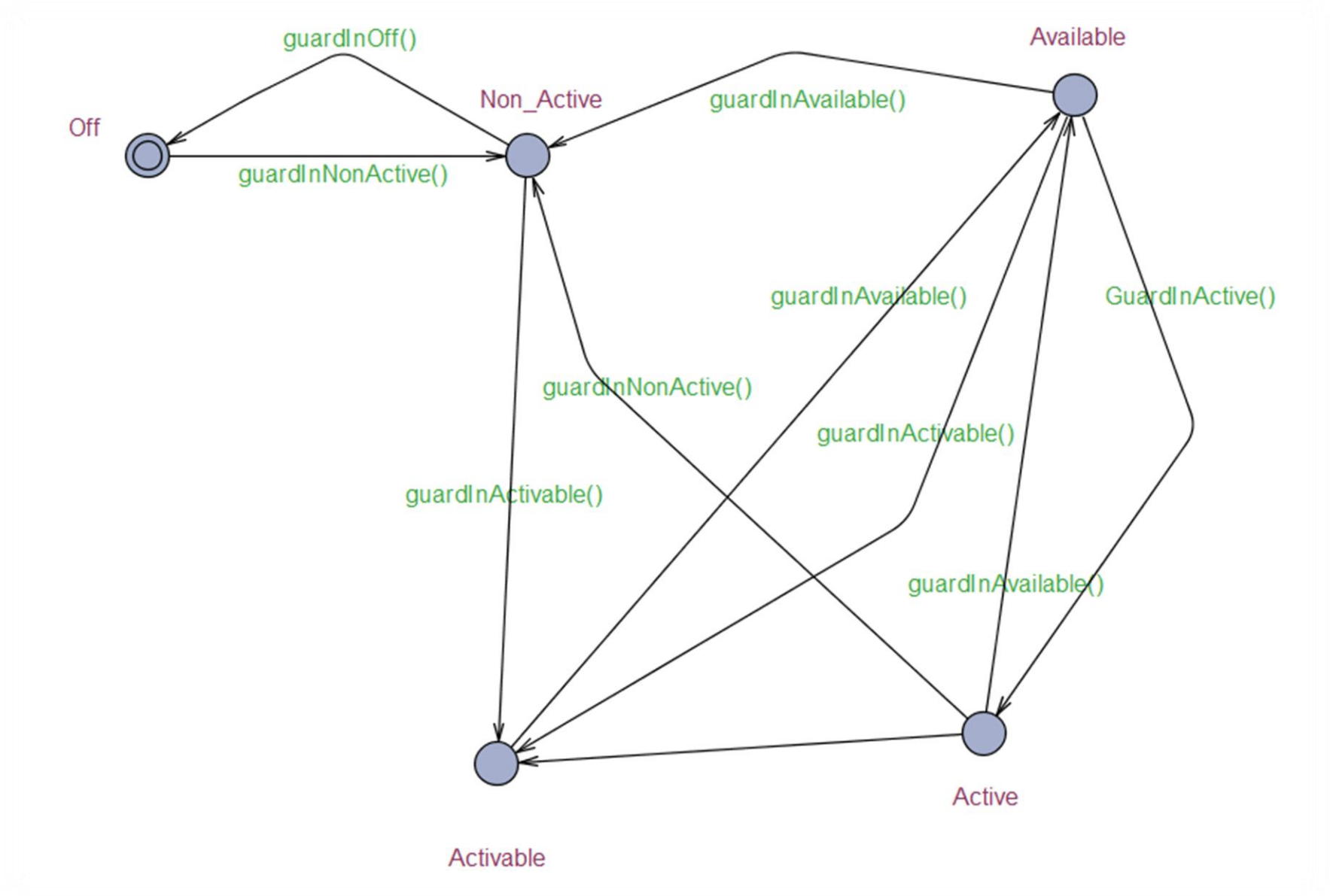
"AD-function **shall be** available IF DAY-TIME = dawn OR DAY-TIME=dusk" — G1

"AD-function **shall be** available IF ROAD-SECTION=ok" — G2





FORMAL MODEL

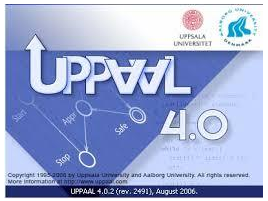


04

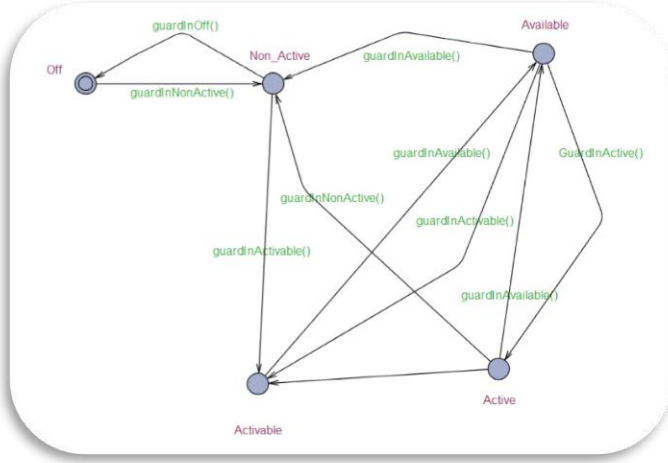
VERIFICATION

The use of a model checker (UPPAAL) to verify the generated model using properties and simulation

FORMAL VERIFICATION

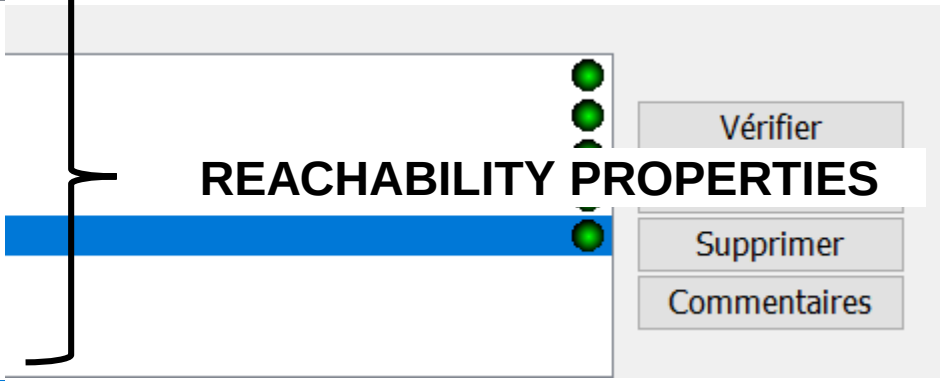


Use automatic model checker UPPAAL ***http://www.uppaal.org/***



Aperçu

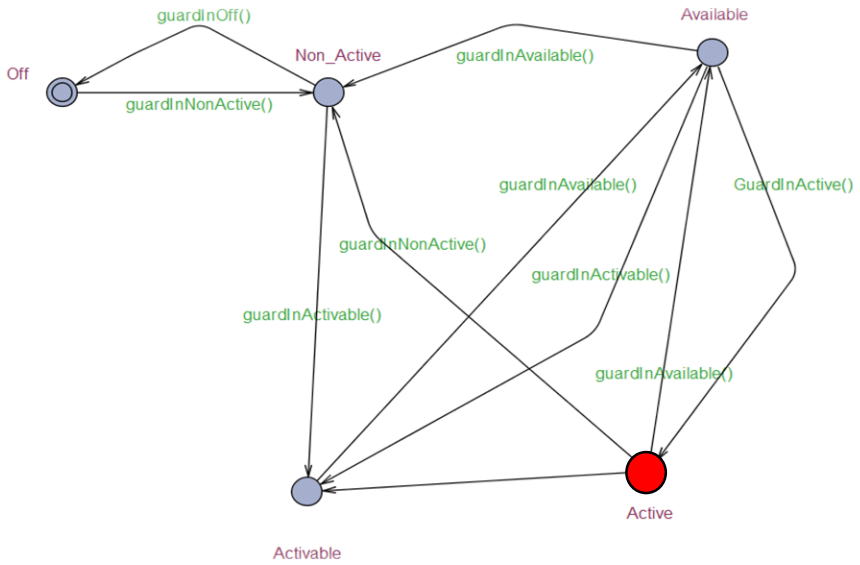
```
E<> AD_function.activatable
E<> AD_function.available
E<> AD_function.n_acti
E<> AD_function.active
A[] not deadlock
```

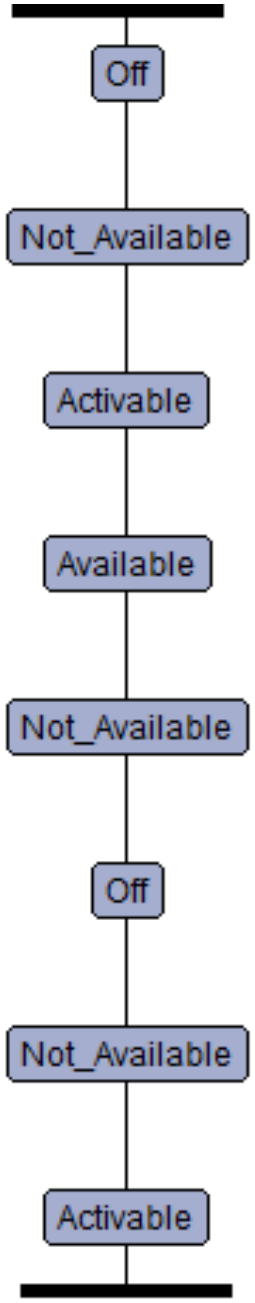


REACHABILITY PROPERTIES

DEADLOCK PROPERTY

SIMULATION & FUNCTIONAL DIAGRAM





- Dynamic behavior
- Visualise the function’s evolution

06

CONCLUSION

Achievements & perspectives

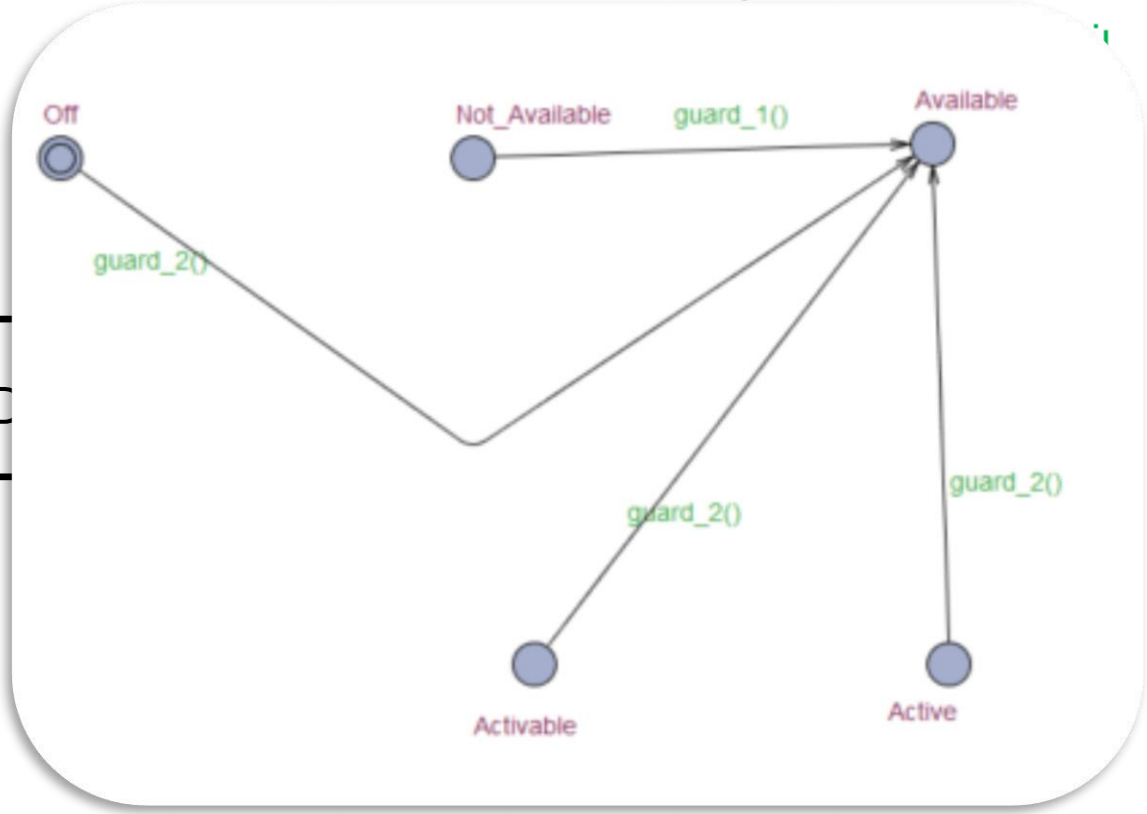
ACHIVEMENTS & PERSPECTIVES

- **Framework**
- **Proof of concept on:**
  - APA (Automatic Park Assist) *https://hal.telecom-paristech.fr/hal-02269614*
  - AD (Autonomous Driving supervion's function)
- **Extend the set of analysed requirements**
  - Time
- **Non functional properties**
- **Validate the whole framework**

THANK YOU

COMPLETION

AD-function shall be available **IF** DAY-TIME = dawn OR D



ASSOCIATED STATE MACHINE

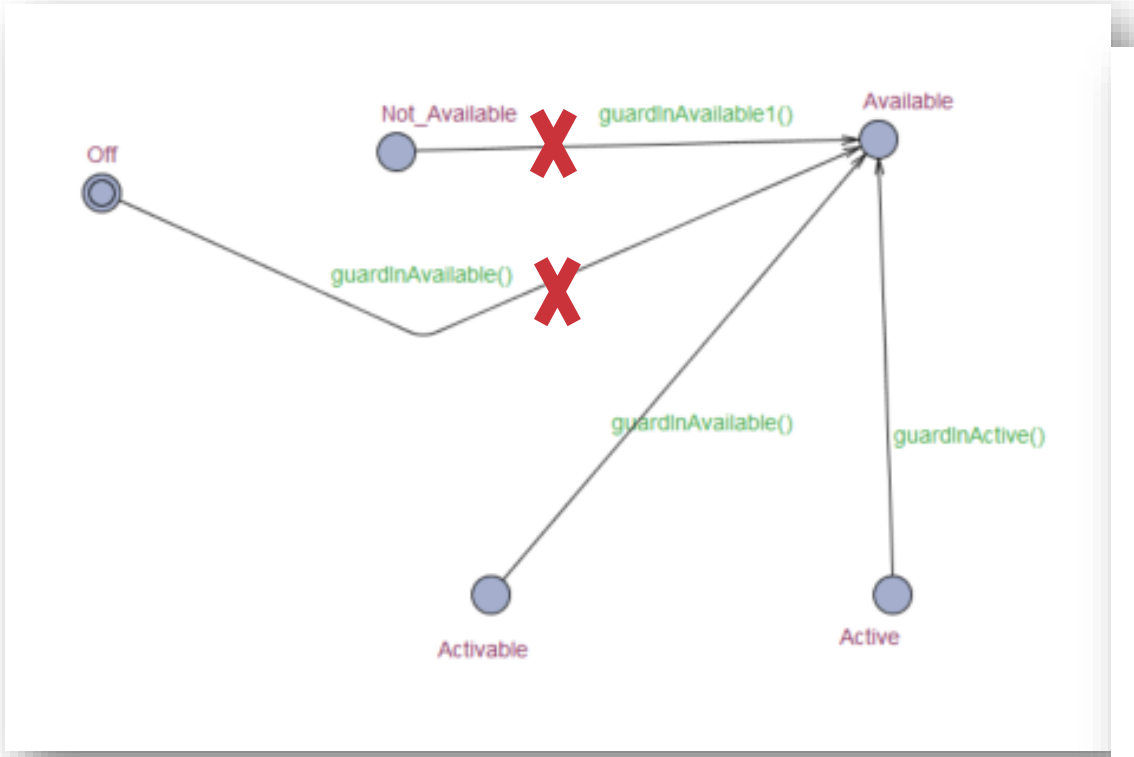
Possible states:
OFF, NOT_AVAILABLE, AVAILABLE, ACTIVABLE, ACTIVE

IF AD-function is in …. **AND** DAY-TIME = dawn OR DAY-TIME = dusk

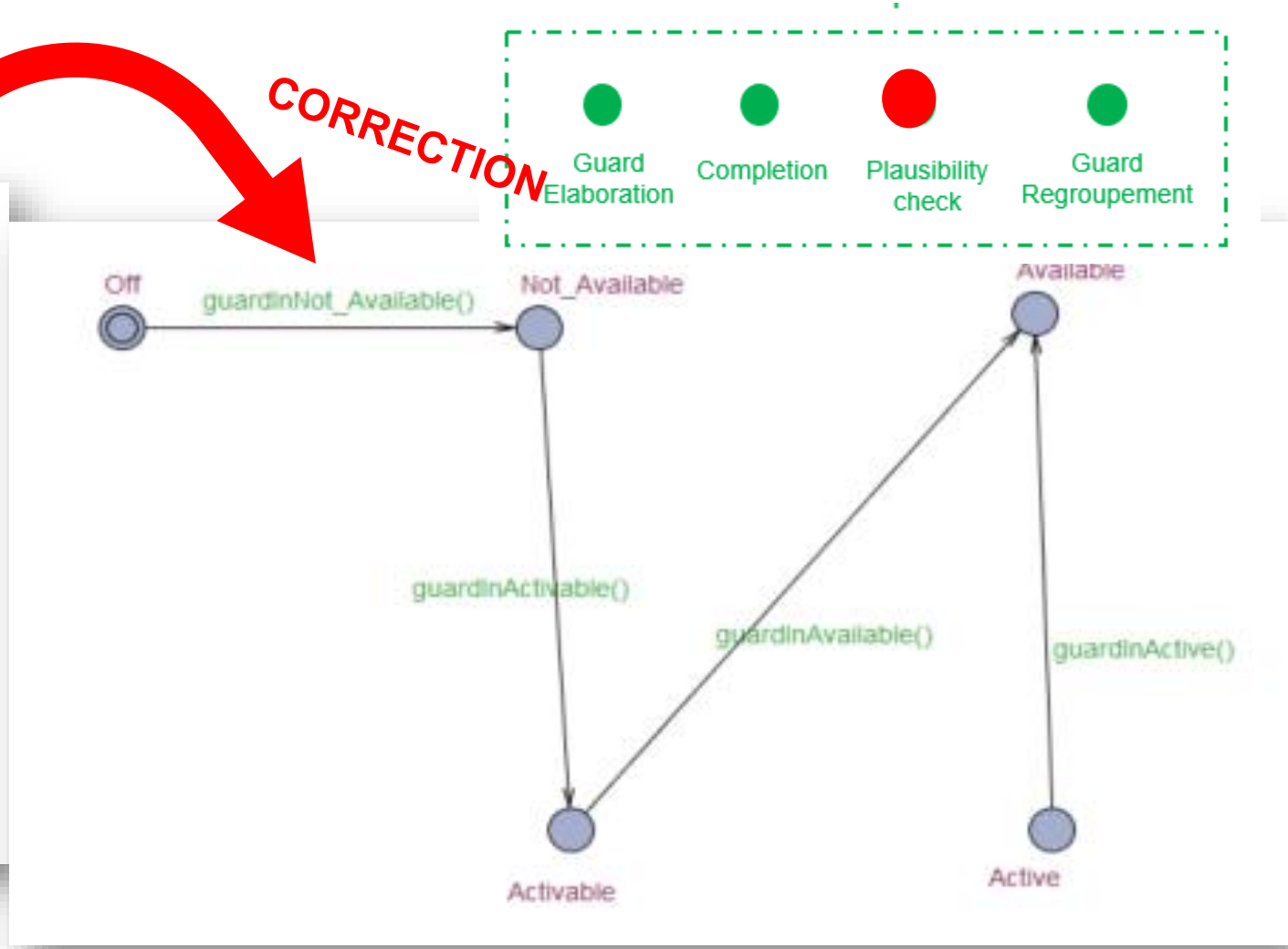
THEN AD-function shall be available

...

PLAUSIBILTY CHECK

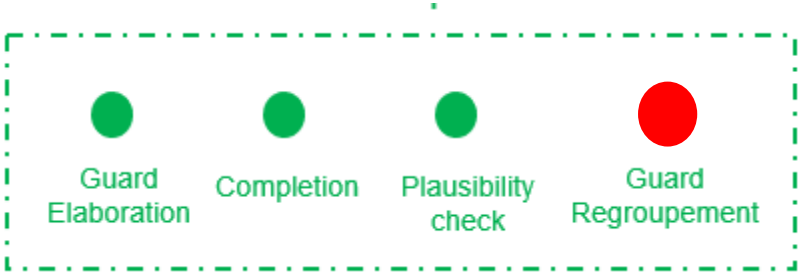


CORRECTION



	Off	Not_Available	Activatable	Available	Active
Off	/	Not_Available	Not_Available	Not_Available	Not_Available
Not_Available	Off	/	Activatable	Activatable	Activatable
Activatable	Off	Not_Available	/	Available	Available
Available	Off	Not_Available	Activatable	/	Active
Active	Off	Not_Available	Activatable	Available	/

GUARDS REGROUPEMENT



⇒"AD-function **shall be** available IF DAY-TIME = dawn OR DAY-TIME=dusk"

=

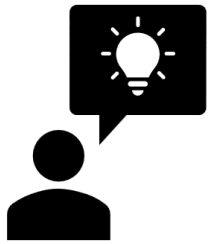
⇒"AD-function **shall be** available IF ROAD-SECTION=ok'

GuardInAvailable= (DAY-TIME=dawn OR DAY-TIME=dusk) **OR // AND** (ROAD-SECTION=ok)

SAFETY

- **Approach**
- **Proof of concept**
- **Finalise step 2 : how it impact on the model**
- **Focus on the patterns**

OBJECTIVE

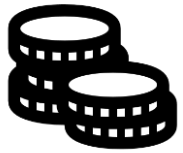


Suggest a methodology for early validation on requirements

- Help engineers in the validation phase
- Improve the product’s quality
- Gain confidence on products
- Reduce bugs and their cost
- Minimize time to market

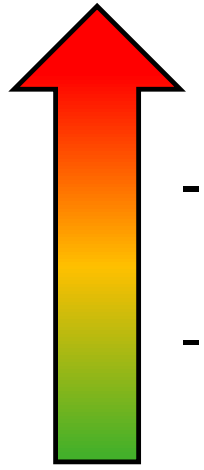
AUTOMOBILE'S EVOLUTION

- **40-60** embedded systems in a classic vehicle
- **80** embedded systems in a premium vehicle



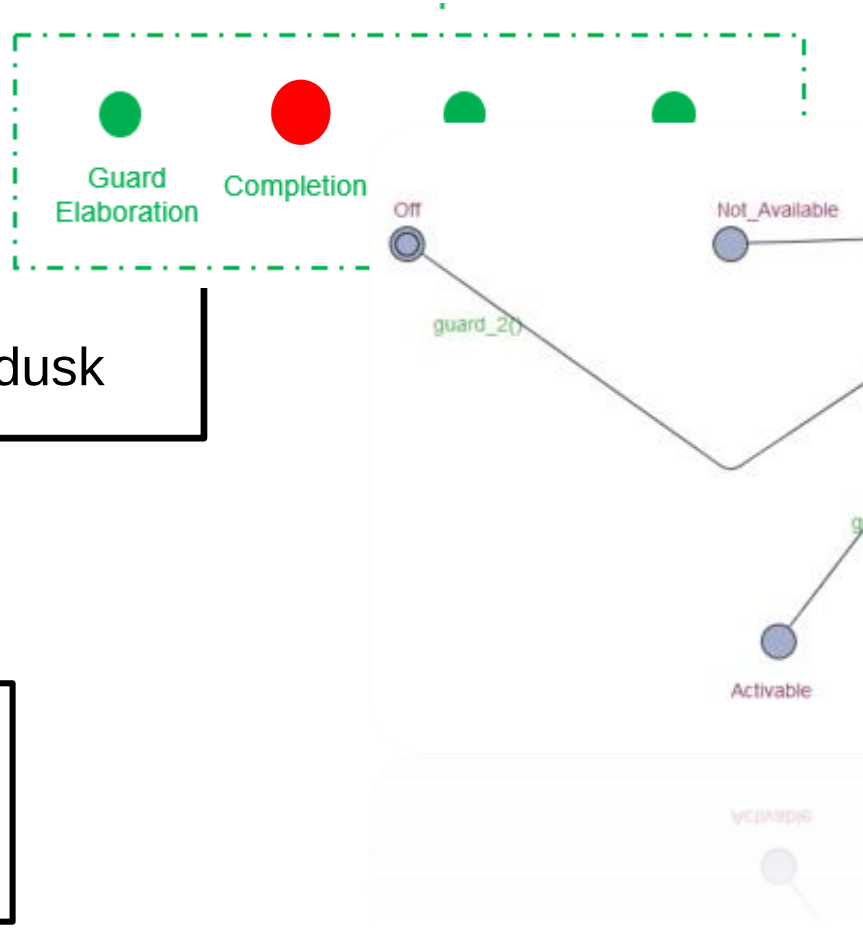
Softwares representes more than 40%
of the vehicle market value

CRITICAL SYSTEM
*Deal with scenarios that may lead to **loss of life**, serious personal injury, or damage to the natural environment*



- **COMPLEXITY**
- **COST**

COMPLETION



AD-function shall be available **IF** DAY-TIME = dawn OR DAY-TIME = dusk

Possible states: OFF, NOT_AVAILABLE, AVAILABLE, ACTIVABLE, ACTIVE

IF AD-function is OFF **AND** DAY-TIME = dawn OR DAY-TIME = dusk

THEN AD-function shall be available

IF AD-function is NOT_AVAILABLE **AND** DAY-TIME = dawn OR DAY-TIME = dusk

THEN AD-function shall be available

ASSOCIATED STATE

...