UML for Embedded Systems

Exam FALL 2013

Modeling an Automotive System: "Messages lead to safety reaction"

Ludovic Apvrille

ludovic.apvrille@telecom-paristech.fr

http://soc.eurecom.fr/UMLEmb/

During an exam, you are not supposed to talk with someone else, by any means (including mobile phones, chat, etc.). Access to Internet is not allowed during the exam, apart the website of the UMLEmb course. During the exam, you may consult your own UML/SysML models made in the scope of the labs, but no other models. Electronic devices are not allowed at all, apart from your computer ;-).
A grade is provided for each question. 1 bonus point is given for the redaction part.

1 Objective

The system to model is an automotive application named "Messages lead to safety reaction". The specification of the system has been written by Continental, Bosch, Fraunhofer ISI and BMW in the scope of the EVITA European Project[1]. Your objective is to model the **software part of the automotive system** involved in the "Messages lead to safety reaction" system.

You have exactly 3 hours to model this system, and answer to various questions: the time is very short. This means that you have to take modeling assumptions. **Keep your diagrams simple and readable**, in particular the analysis diagrams.

Your grade takes into account your report and your models. At the end of the exam, **reports** (in pdf format) and **models** (in TTool format) **must be sent to me by email**. Also, the r**eport must be printed** and **given to Alexia Cepero right after the end of the exam session**. The report should contain explanations concerning your models, as well as relevant screen captures of models (e.g., interesting simulation traces, formal verification results).

2 System specification

2.1 Acronyms

Car2X	Car to "something" communication
CSC	Chassis Safety Controller
CU	Communication Unit
DSRC	Digital Short Range Communication
OBU	On Board Unit
PTC	Power Train Controller
RSU	Road Side Unit

[1] That document is public and should be available on the website of the project: `http://evita-project.org/deliverables.html`

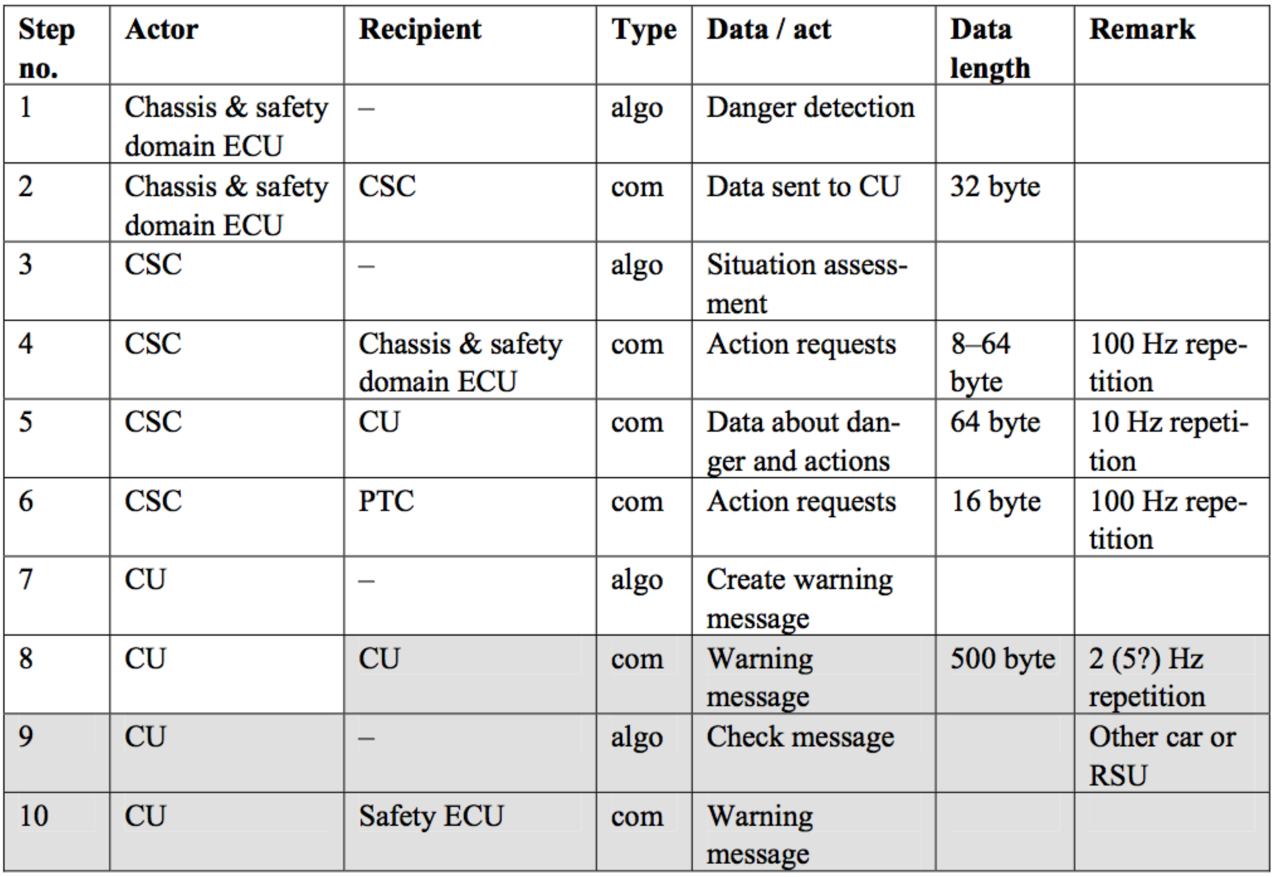
2.2 Description

When a dangerous situation occurs that forces the driver, or the car itself, to perform a manoeuvre, this can endanger other vehicles. In order to warn other vehicles, the car sends out a warning message. Nearby cars that are in danger can then react according to the information provided within the message.

An ECU of the chassis & safety domain detects a danger; this may be the trigger of an air- bag, an obstacle in direction of travel seen by an environmental sensor, or an emergency braking performed by the driver or an automatic system. The Chassis Safety Controller (CSC) gets information about the dangerous situation via the Chassis Domain Bus. The CSC will assess the situation and will take measures to mitigate the danger for the car. The measures will result in commands to actuator ECUs in the chassis & safety domain and additionally commands to the powertrain domain to get a helpful driving power adjustment. In parallel it will also send information to the Communication Unit (CU). This information will contain data about the current vehicle dynamic status and detailed information about the planned actions (deceleration or acceleration, steering, etc.).

The CU will send out a warning message that contains this information via the DSRC interface to nearby vehicles. The emergency message contains longitude, latitude, altitude, speed, acceleration and heading of the car, the time of message generation, the expiry time of the message, an indicator for the reliability of the information, a code that is classifying the car, an id that is identifying the sender of the message, an event code that is classifying the emergency situation and the planed acceleration and heading. All this information is packed in a message frame that adds checksum, information for protocol processing and if necessary security information.

2.3 Scenario



Step no.	Actor	Recipient	Type	Data / act	Data length	Remark
1	Chassis & safety domain ECU	–	algo	Danger detection		
2	Chassis & safety domain ECU	CSC	com	Data sent to CU	32 byte	
3	CSC	–	algo	Situation assessment		
4	CSC	Chassis & safety domain ECU	com	Action requests	8–64 byte	100 Hz repetition
5	CSC	CU	com	Data about danger and actions	64 byte	10 Hz repetition
6	CSC	PTC	com	Action requests	16 byte	100 Hz repetition
7	CU	–	algo	Create warning message		
8	CU	CU	com	Warning message	500 byte	2 (5?) Hz repetition
9	CU	–	algo	Check message		Other car or RSU
10	CU	Safety ECU	com	Warning message		

2.4 Requirements

2.4.1 Functional requirements

- No warning message without a real danger is allowed
- No failure in any single unit may be succeeded by a false message
- No failure of any single communication may be succeeded by a false message
- Any single fault in an ECU has to be detectable
- Information about dangerous events has to be broadcast according to the communication congestion control algorithms
- Information about the dangers have to be broadcast to other cars with highest priority

- Privacy of the broadcast car information has to be guaranteed

2.5 Technical Requirements

- The maximum delay from danger detection to broadcast of the car2X message should be less than 150 ms
- Additional security information on the busses in the chassis and safety & powertrain domains should be less than 15% of the net data

2.6 Security aspects

- Privacy of the broadcast car information has to be guaranteed

3 Assignments

I. Assumptions

1. Your assumptions should be clear. Do list them in the report: that list might evolve according to the models you will make afterwards. [2 points]

II. Requirements

1. Create a requirement diagram. [3 points]

III. Analysis

1. Make a use case diagram. [3 points]
2. Continue the analysis in the form you want: activity diagrams, nominal scenario, error scenarios, . . . : you are free to use the diagrams you want. Of course, the idea here is to show important points of the specification. [3 points]

IV. Design and validation

1. Make a block diagram. Put the emphasis on which blocks are used to model the system to design, and which ones are used either to model the environment, or to prove properties (observers). [3 points]
2. Make state machines, and provide a nominal simulation trace, as well as an error trace. [3 points]

3. Prove that all danger situations result in a safety reaction. From requirements, take a property of your choice, and prove whether it is satisfied (or not!). [3 points]

Good luck, have fun!