ASSIGNMENT 1B. SAFETY-SECURITY MODELLING USING EVENT B

Introduction: a brief overview of how control systems work

Figure 1 shows a generic structure of a networked control system. The system has cyclic behavior and should not terminate (unless it is forced to shut down.) At each cycle, the sensor measures the monitored physical parameter (temperature, pressure, flow, speed etc) and sends the measurement to the controlling program (called controller). Based on the obtained measurement, the controller assign a certain state to the actuator (a motor, switch, valve etc) and sends its command to it over the network. The actuator changes its state according to the obtained command and affects the state of the physical process controlled by the system. The automated control discipline studies how to implement the controlling functions (usually by using differential calculus). In DD2460, we abstract away from these details and create a simple abstract model of a control system described below. The control loop executed indefinitely unless the controller detects some failure and decides to shut down the system. Then the controller puts the actuator in a safe state and stops sending the control commands to it.

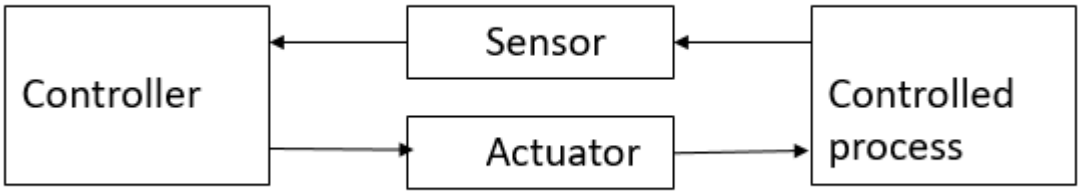

Figure 1. Generic control system

System description

Given a steam boiler – a large tank, which produces steam for an industrial process by boiling the water supplied into it. The pressure inside of the steam boiler should be between 50 and 60 bars but should never exceed 65 bars (then there is a danger of explosion). The pressure is maintained by switching the heater (it heats water, which boils and gets transformed into the steam).

A sensor measures pressure inside of a boiler and sends its measurements as a payload of a packet over a network to the controller. The controller analyses the sensors readings and assign the heater one of the following values: high if pressure is between 50 and 55, low if pressure is between 56 and 60 and off if the pressure is above 61 bars.

In the first part of the assignment, we do not consider security aspect and focus on safety.

Your task:

OBJECTIVE 1. Create requirements document *0,5 points THIS OBJECTIVE IS OBLIGATORY*

> FOR ALL GRADES: CREATE A REQUIREMENTS DOCUMENT that states your assumptions, requirements and explains how they are modelled and verified in the specification. Introduce labels to describe the assumptions and requirements and use Rodin generated labels to explain their representation on the model. Add a brief summary of what all variables and events

represent in the model. The work on the requirements document should proceed in parallel with the modelling process.

OBJECTIVE 2. Ensuring safety 0,5 points

a) Create an abstract Event-B specification which contains:

- Event modelling behaviour of the sensor by non-deterministic assignment to pressure (Natural number)and time stamp (Natural number)
- Events modelling behaviour of the controller, i.e., analysing sensor value and assignment to the variable modelling the state of the heater.
- The abstract specification might have arbitrary order of events execution and weak invariant, i.e., only types of the variables. The controller has direct access to the time stamp and pressure reading, i.e., we abstract away from the communication between the sensor and the controller

b) Refine the abstract specification as follows:

- Introduce the required order of event, i.e., sensor then controller in the infinite loop
- Make the specification of the sensor more deterministic: if the heater is low the pressure might remain the same or decrease by some amount not larger than 2 bars; the heater is high the pressure might remain the same or increase by some amount not larger than 3 bars. If the heater off the pressure should decrease by max 2 bars.
- Define safety invariant and demonstrate that it holds (all proof obligations should be discharged)

OBJECTIVE 3. Detecting sensor failures or security attacks *2 points*

a) Add a simple model of time progress. Define local sensor time and controller time. Lets time be a natural number and initially it is zero. Time of one cycle execution is some constant TMAX, which is greater than 5 units of time. Modify the event modelling the behaviour of the sensor in such a way, that it produces not only pressure measurement but also time stamp. The time stamp is the value that corresponds to the local sensor time plus some delta, which is non-deterministically chosen between 1 and TMAX. The local time of the sensor becomes equal to the time stamp as well. Add events that describe the following behaviour of the controller: the local time is updated similarly to the sensor. When the controller receives a packet from the sensor it compares its local time and the time stamp and assigns to its local clock the value which is the maximum of these two clocks (i.e., the maximum of controller's and sensors' local times.). Add an invariant that shows relationship between these two clocks.

b) Detecting sensor failure or replay attack

Assume that the sensor might fail. In this case, it fails to produce fresh values of timestamp and pressure. The same effect has a replay attack – the attacker tries to insert the packet that has old value of pressure measurement and old time stamp. (As a result, the controller would believe that the pressure is below critical and keep the heater working). Modify the event representing the behaviour of the controller to detect it and execute safe shut down. Model the following: when the controller receives the packet with the old time stamp, it sets the actuator in OFF and shuts down the system.

c). Preventing man in the middle attack.

(You should have achieved points a and b of this objective)

An attacker might try to insert a packet with the value of the payload being modified in such a way that the controller makes unsafe decision based on the obtained measurement. To prevent it, the controller should (at least) check that the obtained packet was sent by a sensor with a legitimate address. Your task is to define the subset of legitimate addresses for the sensors, model generation of a packet to be sent to the controller either by sensor or by the attacker and modify behaviour of the controller so that it recognises invalid address, switches OFF heater and shuts down the system.

OBJECTIVE 4. Introducing simple role-based access control (RBAC) 2 points

You should have achieved OBJECTIVES 2 and 3 to work on OBJECTIVE 4.

The computer running the controlling software has a simple user interface, which allows the authorised person to monitor the behaviour of the boiler and in some cases override the controller' commands. The boiler can run in three modes: AUTOMATED, MONITORED and SUPERVISED. In the AUTOMATED mode, the system executes control loop specified by achieving OBJECTIVES 2 and 3. In the MONITORED mode, each packet generated by the sensor is displayed on the monitor and the operator or supervisor can switch off the heater. In the SUPERVISED mode, the packets are displayed on the monitor and the supervisor (not the controller or the operator) changes the state of the heater.

There are two user types (roles): operator and supervisor. The operator or supervisor can change the mode from AUTOMATED to MONITORED and from MONITORED to AUTOMATED. While the system is in the MONITORED mode the operator or supervisor can switch off the heater.

The supervisor can switch the modes from AUTOMATED to either MONITORED or SUPERVISED and from MONITORED or SUPERVISED back to AUTOMATED.

You need to model the following: registering a new user and assignment it one of the roles. Modelling behaviour of the user according to the user's role, i.e., changing modes, seeing sensor's readings, or sending commands to the actuator. Analyse your invariant. Can safety be maintained? Try to identify and add missing requirements.

Some suggestions for the types of system parameters:

Pressure measured by sensor: natural numbers
Packets sent between the sensor and controller have the following fields:
sender address, timestamp (when the measurement was made), payload (the measurement of pressure)
The addresses of the network elements can be defined using carrier set
Timestamp is natural number
Payload (pressure) is a natural number

GRADING.
To pass (E) you have to achieve at least OBJECTIVES 1 (requirements document) and OBJECTIVE 2 (modelling safety). The objectives have some interdependencies, so it is not advisable to randomly choose the objectives to achieve.