Oblig I Modelling
Product monitoring during shipping

General

In this compulsory exercise (Oblig I) you will be trained in modelling the behaviour of processes and technology focusing particularly on interaction and communication. We have selected a case of relevance for both cyber-security and societal risk that should be easy to grasp without prior domain knowledge. In a later compulsory exercise (Oblig III) you will be asked to conduct a security risk assessment of the same case.

The description is underspecified, and there are many ways to answer the questions. This is intentional and reflects how things are in practise. You are free to make assumptions as long as they are stated explicitly by you in your oblig-solution.

The solution in the form of a single pdf-document should be sent to kst@sintef.no by midnight September 12.

Case

The case involves a factory (the client) that produces chemicals, which are sold to other factories across Europe (the customers) for further processing into end-user products. The chemicals are stored in large containers and transported by trucks. Some of these chemicals are affected by external factors – such as temperature, humidity, vibrations, *etc*. – and might spoil by the time they are received by the customer. The client wants us to address three challenges related to this spoiling of the chemicals after it is produced, both in short-term storage at the factory, and during transport:

1. If a customer receives a shipment of multiple containers and finds one of them to be spoilt, more often than not, the whole shipment is sent back to the client even though the chemical in the other containers might still be of good quality.
2. As the client produces different chemicals in the same factory, it usually takes some time to re-configure the equipment for a given chemical. This, in turn, causes a delay at the customers side when new chemicals have to be produced because of spoilage.
3. To minimize the risk of waste chemicals, the client employs specialized containers, trucks and procedures for storage and transport. It is likely that some of these are excessive in some cases – e.g. in cold weather, short shipping distances – and to reduce the cost and environmental impact, the client wants to only apply these measures when strictly necessary.

To help with these challenges, we propose a system of data-gathering sensors and infrastructure to monitor the chemicals from production all the way to the customer. As the chemical comes out of the production plant and is put into a container, a sensor-unit is dropped into the container. The specific ID of the sensor-unit, the tag of the container, the produced chemical and parameters from the production equipment is logged in a central database. While the containers wait for the transport trucks, they are stored in a short-term storage facility at the client factory. A gateway will be installed in this facility that monitors the external factors in the storage-space and communicates directly with the sensor-units inside the containers, to relay the logged information to the central database. When containers are loaded onto trucks, a mobile gateway is also put onto the truck, which monitors

external factors and relays sensor data through the cellular network to the central database, while the chemicals are shipped to the customers. When the customer receives the chemicals, the mobile gateway is taken off the truck and the sensor-units out of the containers, which is then sent back to the client factory for re-use or recycling.

By combining the logged data from a specific sensor-unit, the corresponding parameters from the production plant, and the monitored external factors from the short-term storage and transport truck, the likelihood of spoiled chemicals will be estimated for every single container. The client will have access to the data at any given time. In addition, other actors will get access to the data in certain situations to address the afore mentioned challenges:

A. When a shipment of chemicals arrives at a customer's facility, the customer will get access to the status – good or bad – of the chemicals in each individual container that is delivered, either locally through the mobile gateway, or through the central database. This allows the customer to only return spoiled chemicals and keep the still good containers.
B. By continuously estimating the likelihood of spoiled chemicals in each container, the system will be able to automatically notify the client if the chemicals have gone bad. That way, the client can make sure they don't ship chemicals that have spoiled in the short-term storage, and it also allows more time to plan for re-production – both for the client and the customer – if it is spoiled during transport.
C. During transport, the driver of the truck and the transport company will have access to and be notified of the state of the containers on the truck. This enables them to carry out expensive procedures and counter-measures to prevent the chemicals from spoiling, only when strictly necessary.

Question I

a) Make a class-diagram describing the case relevant concepts. The class-diagram should at least represent factory, customer, short-term storage, container, sensor-unit, sensor, gateway, truck, chemical, shipment.
b) Argue the goodness of the class-diagram with respect to slide 25 (Lecture I) and the law of proximity (slide 32, Lecture I).

Question II

As we have highlighted during the lectures, although sequence diagrams originate from the telecom they can be employed much more broadly. Make a sequence diagram with lifelines for at least factory, truck, truck-driver, sensor-unit, mobile gateway and customer. It should describe traces of relevance for A, B and C of the text above. Use the ref-construct to split the specification into several diagrams.

Question III

Make a detailing of the sensor-unit lifeline to clarify the internal behaviour of the sensor-unit. It should consist of a controller and individual sensors for temperature, humidity, vibrations, etc. All internal and external communication in the sensor-unit should be via the controller.

Question IV

a) Make a state-machine representing the controller lifeline.
b) Argue that the state-machine for the controller is consistent with the controller lifeline in the sequence diagram.

Question V

Discuss the robustness of the state-machine for the controller. Update the state-machine to deal with identified weaknesses.