Oblig III Security Risk Assessment of product monitoring during shipping

General

In this compulsory exercise (Oblig III) you will be trained in security risk assessment of the same case you have already modelled as part of Oblig-I.

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 November 5. You may work in groups of maximum three students or you may work alone. Hence, one solution may have up to three names. There should be no collaboration or copying between different groups. Hence, each group should solve the exercise independently.

You should use the new CORAS-tool: https://coras-explorer.firebaseapp.com/try-it

With respect to likelihood reasoning, use the rules for frequencies presented in the lectures. (In the CORAS book there are also rules for probability reasoning. They should not be used.)

It is a very good idea to start by reading Chapter 3 of the CORAS book.

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.

Security Concern

The chemicals that are transported are highly toxic and may also under special circumstances explode with devastating consequences. A government authority has assessed the already ongoing storage and transportation practice, but the introduction of the new technology for data-gathering and monitoring, as well potential measures that may be undertaken during transportation, requires a new risk assessment to be carried out from scratch.

In the following we address some of the aspects that such a risk assessment may involve.

Question I

Identify at least seven assets of relevance. The party in question is the **government authority**. Minimum two assets should be indirect and minimum three assets should be direct.

Two of the direct assets should be "public safety" and "accountability".

Make a CORAS asset diagram that correctly relate them.

For detailed advice, see Section 7.2.2 in the CORAS book.

Question II

Make a good ordinal scale for measuring harm (consequence) to the asset "public safety".

Question III

Make a good quantitative scale for measuring harm (consequence) to the asset "accountability".

Question IV

You should also make consequence scales for the other direct assets you have identified, as well as a quantitative scale for likelihood based on frequencies. They should all be good ☺

Question V

Make relevant threat diagrams with respect to the direct assets. The diagrams should all together capture at least seven risks. The diagrams should be annotated with consequences and likelihoods in such a way that they are consistent.

Question VI

Present the identified risks in a risk-matrix.

Question VII

Annotate the threat diagrams from Question V with relevant treatments.

Question VIII

Assume the government authority requires the treatments for the three most important risks to be implemented. Use the CORAS before-after style to illustrate the effect of these treatments on the already identified risks. The threat diagrams you have already drawn (Question 5) corresponds to the before situation. You are to "translate" these threat diagrams into threat diagrams expressed in the so-called before-after style reflecting the situation both before and after the implementation of the treatments.

Read Section 6 of
http://www.uio.no/studier/emner/matnat/ifi/INF5150/h11/undervisningsmateriale/2011.FOSAD-preprint.pdf.

Question IX

Any risk treatment will introduce some new risks (possibly with respect to some new assets). Update the threat diagrams from Question VIII to capture at least two new risks.

Question X

Present the risk matrix as it looks after the risk treatment (also considering the results from Question IX).