Instructions for the Risk Analysis

SMS, and MH

September 19, 2013

1 Motivation

In this experiment you will perform a risk analysis of a **Train Door System** (see in appendix A). The knowledge and experience gained by doing this experiment will help you to perform risk analysis for your projects (section 8.2.4 in the Red book) that is mandatory.

2 Risk Analysis

Risk analysis is an iterative process and it consists of the following four steps:

1. Planning
2. Risk identification
3. Determine the risk probability (likelihood level)
4. Determine the risk consequence (severity level)

The method used here is perspective-based risk analysis. It is different from traditional risk analysis because it supports the analysts to view and analyze the system from different perspectives. For example, one analyst may analyze the system from the point of view of the designer, another from the point of view of the developer, and another from the point of view of the user/client of the system.

For the perspective-based risk analysis of the **Train Door System**, the following three perspectives will be used:

- System Engineer (SE)
- Tester (T)
- Train Staff Member (TS)

Note: It is possible that several of the identified risks from the different perspectives can be the same.

2.1 Step 1

The planning step contains the following tasks:

i. Forming groups (three members in each group)

ii. Careful reading of the system description (see in appendix A)

iii. Selection of different perspectives for the risk analysis

iv. Selection of the moderator of the risk analysis team

v. Selection of the person responsible for writing that will merge and write the common risk list

Note: One person can perform both the moderator and the writing tasks.

In step 1, after forming the groups you will read the system description (see in appendix A) carefully to understand how it works and which components of the system are critical. Then, each member of the risk analysis team will choose one perspective for the experiment (i.e., system engineer, tester or train staff member). After this, you will decide among the group members who will be the moderator and who will perform the writing task.

2.2 Step 2

Step 2 of the risk analysis consists of the risk identification activity that determines a list of possible risks. Risk identification is an iterative activity that is normally carried out by brainstorming. For the risk identification step the risk analysts attempt to find a list of possible risks by answering the following question:

- What could happen or what can go wrong?

In step 2 you have to perform the following tasks:

i. Find your own individual list of possible risks according to your perspective, i.e., system engineer, tester and train staff member.

ii. Compare and merge your individually identified risks with others and make a common risk list.

Example: Figure 1 shows the structural and functional diagram of an example system (insulin pump).

For the example system the following three perspectives were used during the risk analysis: the system engineer, the tester, and the patient.

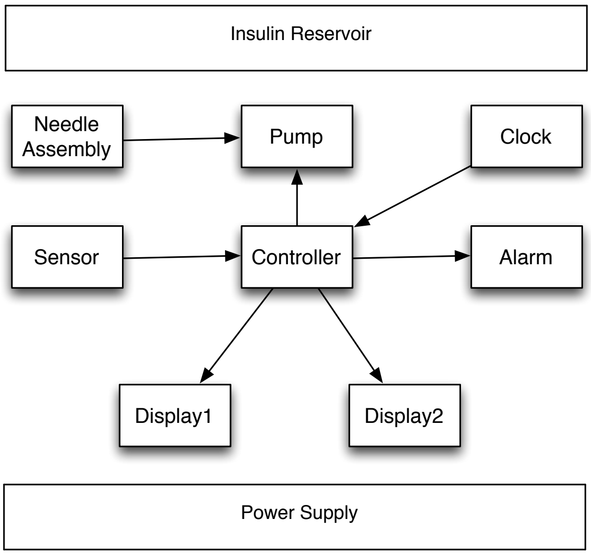


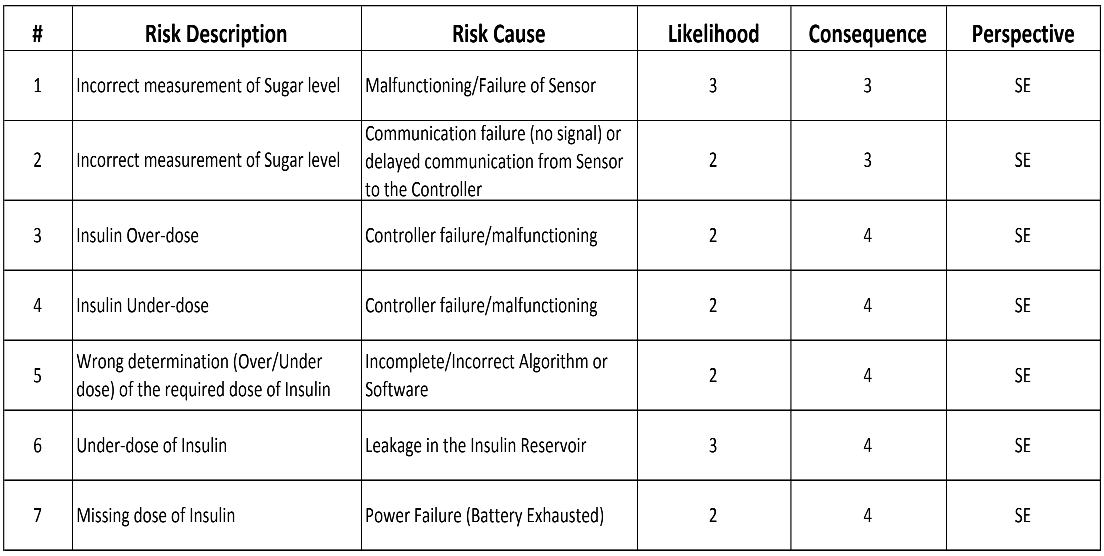
Figure 1: Example System: Insulin Pump

As an example, shown in Table 1, the perspective-based risk analysis has been carried out from a *System engineer's perspective* and identified some of the potential risks for the example system.

Similarly, the risk analysis can be performed from other perspectives to identify more risks.

Note: The risk list in Table 1 is not complete. It is an example to give some basic idea about the risk identification step.

Table 1: Identified Risks with their Likelihood and Impact in the Example System (see Section 2.3 and 2.4 for the likelihood and consequence levels)



#	Risk Description	Risk Cause	Likelihood	Consequence	Perspective
1	Incorrect measurement of Sugar level	Malfunctioning/Failure of Sensor	3	3	SE
2	Incorrect measurement of Sugar level	Communication failure (no signal) or delayed communication from Sensor to the Controller	2	3	SE
3	Insulin Over-dose	Controller failure/malfunctioning	2	4	SE
4	Insulin Under-dose	Controller failure/malfunctioning	2	4	SE
5	Wrong determination (Over/Under dose) of the required dose of Insulin	Incomplete/Incorrect Algorithm or Software	2	4	SE
6	Under-dose of Insulin	Leakage in the Insulin Reservoir	3	4	SE
7	Missing dose of Insulin	Power Failure (Battery Exhausted)	2	4	SE

2.3 Step 3

In step 3 you have to determine the likelihood of occurrence of all identified risks in step 1 by using following qualitative descriptors:

1. **Highly unlikely:** The event might occur in the exceptional circumstances. It could happen, but probably will not
2. **Unlikely:** There is a slight possibility that the event may occur at some time
3. **Possible:** The event might occur at some time
4. **Likely:** There is a strong possibility that the event will occur
5. **Very likely:** The event is expected to occur in most circumstances

Example: Table 1 also shows the expected likelihood of occurrence for the identified risks.

2.4 Step 4

In step 4 you have to estimate the consequences (severity level) of all identified risks in step 1 by using following qualitative descriptors:

1. **Insignificant:** Discomfort or only minor personal injury; First Aid needed but no days lost
2. **Minor:** Minor injury; Medical treatment and some days lost
3. **Moderate:** Injury; Possible hospitalization and numerous days lost
4. **Major:** Single death or long-term illness or multiple serious injuries
5. **Catastrophic:** Fatality(ies) or permanent disability or ill-health

Example: Table 1 also shows the expected severity levels for the identified risks.
Note: The above mentioned descriptors are for user health and safety.

Appendix A Train Door System

The system chosen for this experiment is a simple automated train door control system. It is an embedded socio-technical safety-critical system and it has all the components that exist in the complex/large safety-critical systems (e.g., an aircraft, nuclear power plant etc.).

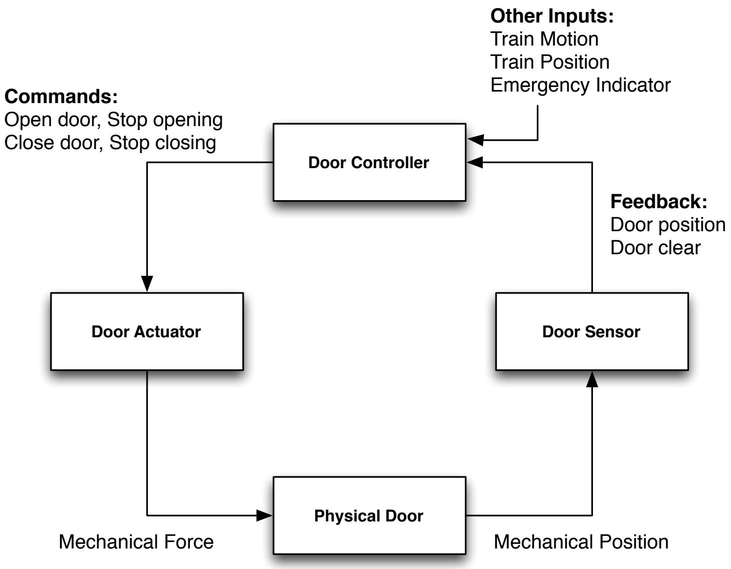


Figure 2: Structural and Functional diagram of a Train Door System

Figure 2 shows a control structure diagram of an automated train door system. It has four main components, shown in Figure 2, the door sensor, door controller, door actuator and the physical door.

Door sensor: It sends a signal/feedback about the door position and the status of doorway (e.g., doorways is clear or not) to the door controller.

Door controller: It receives input from the door sensor about the door position and doorway. It receives some other inputs from the external sensors about the motion and the position of the train. It also gets an indication about an emergency in train from an external sensor. After receiving inputs, the controller performs some computation and then it issues door open/close commands as shown in the Figure 2.

Door actuator: It receives commands from the controller and it applies mechanical force on the physical door. Here, the actuator is an electric actuator that converts electrical energy to mechanical force/energy.

Physical door: There is a physical door in the system that is closed/opened by the force applied by the door actuator.

Other inputs: The controller receives three other inputs from the external sensors as shown in Figure 2.

i. The first input, train motion, gives information about movement of train, i.e., moving or stationary.

ii. The second input, train position, gives information about the position of train, i.e., on the way or at station platform.

iii. The third input, emergency indicator, gives a signal to the controller about any kind of emergency in the train. After receiving this input, the controller should send open door command to the actuator.

Note: Please consider risks related to the *Other Input* signals without their source systems. The source systems of the other inputs are not part of this risk analysis.