Software Safety Exercise 1

Dennis J. Frailey

Select a scenario below and identify up to three ways in which software might contribute to a safety hazard. In each case, identify

- the hazard and how software might create that hazard
- a mishap that might cause a safety problem.

Present your findings to the rest of the class.

Scenarios:

Virus research lab.

In this laboratory, scientists study various viruses to determine which ones might cause harm to humans or animals. They have many computer-controlled machines that perform such functions as spinning test tubes around, measuring and analyzing biological samples, controlling machines that open and close containers of various substances, some of which may contain viruses, and adding materials to existing viruses to induce the generation of modified viruses. They also maintain a data base of experimental data and other research results.

Virus testing lab.

This is the laboratory where test samples are sent for analysis. There are computer-controlled systems for opening test samples, transferring them to test equipment, and disposing of used test samples. The test equipment is also computer-controlled. Finally, they generate test result reports using computer software.

Electronic thermometer.

This device is used to take the temperature of people entering a facility. The intent is to deny them entry if they have a fever, which might indicate that they have a viral infection. It is also used in homes to determine if someone has a fever or in medical offices and hospitals to determine the patient’s temperature. The device consists of a tiny computer connected to a sensor and a panel where the temperature is displayed.

Treatment planning software.

This software assists the medical practitioner who is treating a patient by supplying patient data and other information used to assess the proper treatment. Some of that information may be fed into a medical treatment device, intended to help treat the patient. The software also assists the medical practitioner by performing various analyses of the data.

Medical diagnostic device.

Many diagnostic devices use so**f**tware to help diagnose a patient's condition. For example, a machine called a tri-axial accelerometer that is attached to a digital camera that and is used to examine the patient. The software controls the operation of the device and analyzes the data collected by the device, producing results on a screen for the technician to view and also producing a written report.

Medical treatment device.

Many modern medical devices contain embedded computers and software to control their function. Some of these devices, such as x-ray machines or machines that control dosage of medications, must be carefully controlled to assure proper treatment and avoid patient harm. Most such machines also have software to guard against operator errors, such as accidentally specifying too high a dose of medication.

Equipment leak tester.

This device is used in factories that manufacture personal protective equipment (masks, gowns, shields, etc.) to assure that they are functioning properly and do not have leaks or tears. The device typically attempts to blow air through the device to detect leaks. It positions the equipment in various ways and runs a variety of tests.

Mathematical model.

This software model simulates the future consequences of various actions that have been proposed to reduce the spread of a disease. Based on historical records and what is known about the disease, the model predicts how many people are likely to be infected, how many deaths can be anticipated, where and how quickly the infections will occur, etc. The model is relied on by experts, government officials, and practitioners.

Patient database.

This software maintains records of patients who have contracted a particular disease as well as additional information, such as the results of various treatment options. Experts and practitioners rely on the accuracy of this data.

Manufacturing process control.

This software controls the manufacturing process for various medical equipment. Its purpose is to make sure the equipment is manufactured correctly. It controls such functions as the speed of the manufacturing process (assembly line), the proper functioning of the various machines used to manufacture the product, and detection and response to situations where something goes wrong.