Student no: 940165
Name: Ummi Aishatu Ibrahim
Course: CSCM13 – Critical systems

- **Question 1 (a)**

  This program acts like a boiler where the boiler produces steam after all the correct data has been inputted. Every procedure has its own purpose on how to make this program interactive and finally producing the steam that is necessary after inputting the right data. This program is a safety critical system because it follows and programs safety functions and protocols to state that the program can be dangerous at a certain point. This will be explained further when explain the individual procedures and functions.

  The first procedure is called **Fill_boiler**, this procedure fills in the boiler according to the amount of litre it can take.

  - The procedure first asks the user to enter an integer, once the user enters from 500 to 1000, the boiler will then be filled
  - If the user enters less that 500, the user will not be able to move to the next step unless they include a value from 500 to 1000.
  - If the user goes above maximum amount which is 1000 or critical amount which is 1500, to prevent leakage the user will not be able to forth to the next step.

  The second procedure is called **Accept_Temperature** where it accepts a temperature to boil the water after it has been filled.

  - The procedure first asks the user to enter an integer, once the user enters from 0 to 212, the water will be boiled
  - If the user enters less that 40, the user will not be able to move to the next step unless they include a value from 40 to 212.
  - If the user goes above maximum amount which is 300 or critical amount which is 212, to prevent an extreme accident the user will not be able to forth to the next step.

The next Procedure is called **Reduce_Temperature** which states that the temperature is too high and sets it to 212, which is its maximum critical level that the boiler can accommodate.

- If the temperature is greater than the critical temperature, then the status for the temperature will be **reduced** and it will set it to 212 which is the critical temperature.
- If is lower than it is set to **not_reduced** and it returns the same temperature inputted.

The next Procedure is called **Increase_Temperature** which states that the temperature is too low and sets it to 40, which is its minimum regular temperature that the boiler can accommodate.

- If the temperature is lower than the regular temperature, then the status for the temperature will be **increased** and it will set it to 40 which is the regular temperature.
- If is greater than it is set to **not_Increased** and it returns the same temperature inputted.

The next Procedure is Produce_steam, these procedures the steam when all the necessary criteria has been met. These criteria include:

- When the amount of water is between the regular litre and the maximum amount of water to take and
- When the temperature is not lower than 40 which is the regulate temperature and is not high than the critical temperature which is 212
- Then the program can run, and the boiler can produce the steam.

The next procedure is **Print_status** prints out all the status of the program, which includes the:

- The status of the reduction, whether the temperature was reduced or not
- The status of the Increment, whether the temperature was Increased or not
- The current temperature and the
- The current amount of water in the boiler

The next procedure is **Init** explains how the program acts on null.

function **Status_Reduced_temperature_Print** and function **Status_Increase_temperature_Print** prints out the status when it is either **reduced or increased or not_reduced or not_increased.**

function **heat_safe** and function **Temp_to_boil** explains when the boiler is not too hot and okay to boil temperature.

- **Question 1 (b)**

Using the FMEA hazard analysis, the boundary of the program is to prevent the boiler from getting too hot, prevent it from not boiling at all and prevent it from leaking.

The subsystem of the program is using the procedures **Reduce_Temperature** and **Fill_boiler**. All the procedures that are listed for the subsystem will all affect the program because they have important roles to play when boilers are going to be used.

The first subsystem is **Reduce_Temperature,** when the boiler reaches critical level, the boiler can get too hot and cause damages to the internal components by putting it under stress and cause irreparable damages. Sometimes the boiler can explode leading to a dangerous situation.

Its mission phase: When this happens maintenance repair or regulation of temperature usually solves the case.

The second and final subsystem is **Fill_boiler,** when the water in the boiler is too low and the boiler does not go off, this can cause dry fire accident. And when the water is too much for the boiler this can cause the boiler to leak and if not noticed, this can cause the boiler to leak the hot water and cause an accident on the individual that goes to switch it off.

Its mission phase: When this happens maintenance repair of the boiler and safety system is to be considered. In every boiler, there is a safety system that switches off the boiler when it dry. It is always advisable to check if this is not damaged and working.

Both the subsystems are single-point failures because it can affect the whole system when it is not considered.

The FMEA worksheet consist of

Date: 7/12/2021		Analyst: Ummi Aishatu Ibrahim		
Failure effects locally	Failure propagation next level	Single-point Failure	Risk failure class	Control recommendation
No reduction of temperature when	The boiler might explode or result to further inner	YES	4C	When this happens maintenance

it reaches maximum level	damages to the inner component parts			repair or regulation of temperature usually solves the case.
No filling in the boiler to accommodate it and not turning it off after it dries up.	The boiler can dry off and cause a cause a dry fire accident	YES	4C	When this happens maintenance repair of the boiler and safety system is to be considered. In every boiler, there is a safety system that switches off the boiler when it dry. It is always advisable to check if this is not damaged and working.