CFSE
GOVERNANCE BOARD

Certified Functional Safety Expert
Process Applications

Section 1: Multiple Choice Sample

16

Candidate Name:

Please write down your name in the above provided space. Only one answer is correct. Please circle only the best possible answer.

1: Before performing a Process Hazard Analysis, such as a HAZOP, the participants in the study will need to have all of the following safety information, except:

A. A block flow diagram or simplified process flow diagram.

B. SIS internal wiring diagrams

C. Area electrical classification

D. Design codes and standards employed

2: All of the following are advantages of using programmable electronic systems in safety applications, except:

A. Capability for self-diagnostics

B. Capability for performing complex calculations

C. Inherent safe (de-energized) failure of electronic components performing output switching.

D. Ease of making changes to system logic

3: Which of the following statements about the documentation required for functional safety planning are true:

1. Safety planning documentation can be included as a section in the quality plan entitled “safety plan”

2. Safety Planning can be documented in a series of documents that may include other company procedures or working practices, such as corporate standards

3. Safety planning must be documented in a separate document entitled “safety plan”.

A. 1 and 2 are true, 3 is false

B. 1 and 3 are true, 2 is false

C. 1 is true, 2 and 3 are false

D. 1, 2, and 3 are true

Section 2: Case Study and Short Answer Sample

Candidate Name:

Please provide your name in the above provide space. Answer your choice of at least 50 points worth of questions in the space provided. If you need additional space please attach a seperate sheet. Make sure to number each attached sheet and label your answer with the corresponding question number.

1: The IEC 61511 standard lists goals for safety planning. List three of the five goals of safety planning. (2 points)

2 : Please refer to the Figures on the following page.
A specialty chemical company has developed a batch process to produce a new polymer. The process creates a solution of polymer and cyclohexane that is withdrawn from the bottom of the pressurized, water cooling jacketed, continuously stirred tank reactor. The vessel is charged by filling it with 250 kg. of cyclohexane and manually dumping 125 kg. or 5 bags of reactant A into the vessel. After the vessel is charged and closed, the stirring mechansim is started and the vessel's jacket is flooded with cooling water. After the stirring and cooling have been established a small, metered rate of 0.5 kg/min of reactant B is continuously added to the solution. Reactants A and B combine to form the desired product. Each batch operates for three weeks, and 5 batches are operated per year.

The reaction A and B is nearly instantaneous and highly exothermic. Safe operation of this process requires that cooling water continuously be flowing through the jacket. Hazard analysis determined that loss of cooling water could cause a "runaway" reaction and physical explosion of the vessel. The plant's safety division performed a quantitative consequence analysis of the physical explosion of this vessel. The analysis determined that the explosion would result in the following consequence:

- Probable Loss of Life: 5.64 fatalities
- Probable Injuries: 13.24 injuries

The following layers of protection were identified as a safeguard against explosion of the vessel due to runaway reaction.

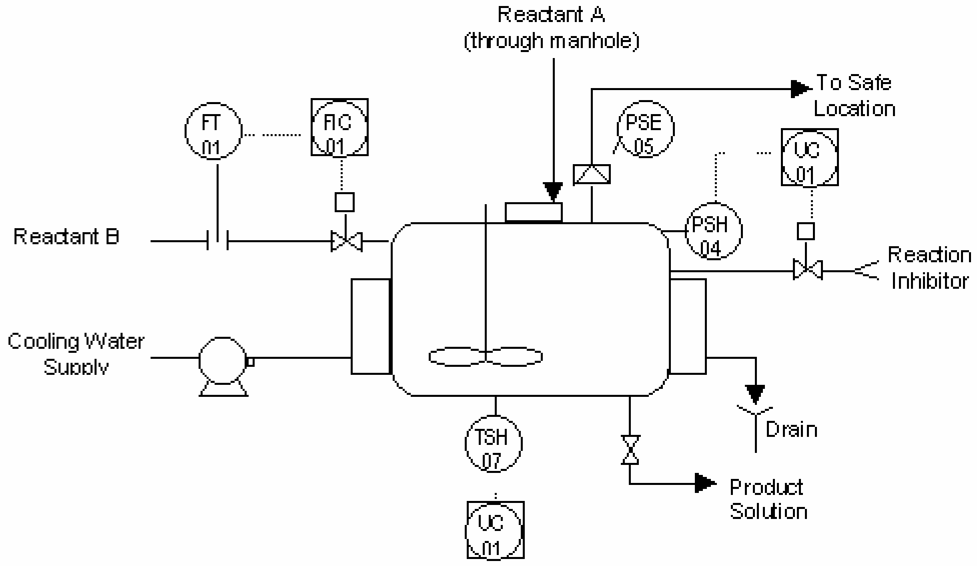
- A rupture disk set to relieve the pressure well below the design pressure of the vessel
- Operator intervention to high vessel temperature, high vessel pressure, and low cooling water flow alarms

A safety instrumented system that injects a reaction-inhibiting chemical if the vessel temperature or pressure exceeds predetermined conditions was recommended in the process hazards analysis.

THIS QUESTION CONTINUES ON THE NEXT PAGE

A process engineer determined the following frequencies and failure probabilities after reviewing the history of the plant.

- Cooling Water Pump Fails: 1/75 /year
- Rupture Disk PFD: 0.0956
- Operator Response to Cooling Water Loss pfd: 0.1



The plant uses the following table to determine tolerable frequency of an unwanted event, based on its consequence.

Event Type	Tolerable Event Frequency
Fatalities Unlikely	1.0×10^{-3}
Fatality Likely	1.0×10^{-4}
Multiple Fatalities Likely	1.0×10^{-6}

1. Create a LOPA diagram that describes the situation defined above.
2. Quantify the LOPA to obtain the frequency at which the unwanted explosion is expected to occur.
3. Based on the company's tolerable risk guidelines, select the safety integrity level for the inhibitor injection SIS.
(16 Points)

Section 1: Multiple Choice Sample Answers

1: Before performing a Process Hazard Analysis, such as a HAZOP, the participants in the study will need to have all of the following safety information, except:

B. SIS internal wiring diagrams

2: All of the following are advantages of using programmable electronic systems in safety applications, except:

C. Inherent safe (de-energized) failure of electronic components performing output switching.

Explanation: A programmable electronic system provides the user with a great amount of flexibility and computational power. The components used for switching are however not inherently fail-safe. Switching components, such as transistors, have failure mode percentages of about 50% dangerous failures. The high level of safety that PES can achieve, even though component failures are not inherently fail-safe, is due to extensive diagnostics and redundancy.

3: Which of the following statements about the documentation required for functional safety planning are true:

1. Safety planning documentation can be included as a section in the quality plan entitled “safety plan”
2. Safety Planning can be documented in a series of documents that may include other company procedures or working practices, such as corporate standards
3. Safety planning must be documented in a separate document entitled “safety plan”.

A. 1 and 2 are true, 3 is false

Section 2: Case Study and Short Answer Sample Answers

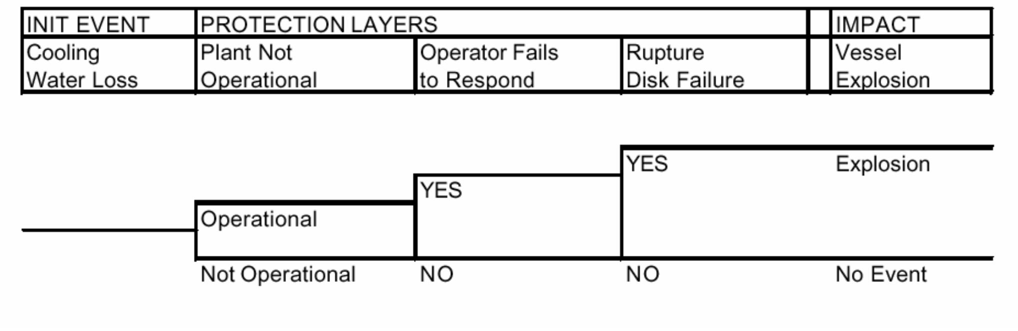
1: The IEC 61511 standard lists goals for safety planning. List three of the five goals of safety planning. (2 points)

According to IEC 61511, safety planning has five goals. They are:
- ensure that the functional safety objectives and the safety integrity level objectives are achieved for all relevant modes of the process
- ensure proper installation and commissioning of the safety instrumented system
- ensure the safety integrity of the safety instrumented functions after installation
- maintain the safety integrity during operation (e.g., proof testing, failure analysis, etc.)
- manage the process hazards during maintenance activities on the safety instrumented system

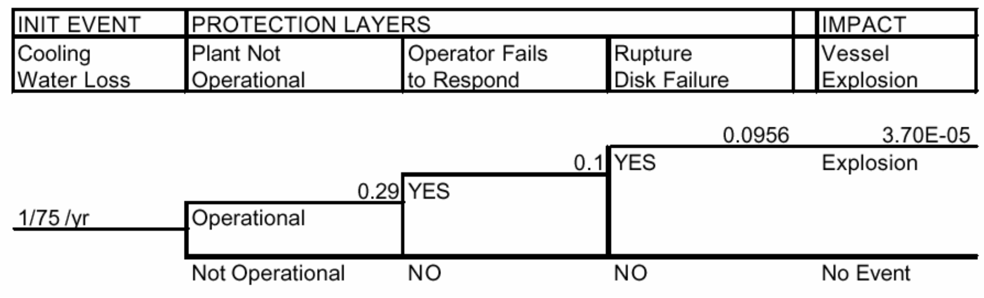
Answer to case study question 2:

1. Create a LOPA diagram that describes the situation defined above.
2. Quantify the LOPA to obtain the frequency at which the unwanted explosion is expected to occur.
3. Based on the company's tolerable risk guidelines, select the safety integrity level for the inhibitor injection SIS.

Part 1. The solution requires development of the Layer of Protection Analysis diagram to describe the situation and quantification of the diagram to determine the frequency of the unwanted accident. The LOPA diagram has four branches with two outcomes. The first stage is the initial event, which is loss of the cooling water. The first branch occurs on whether or not the plant is operational. The second branch represents whether the operator fails to respond or not. The third branch is whether the rupture disk fails. Then finally is the result of explosion.



Part 2: The plant is not continually operational, therefore the time that the plant is not in service will decrease the frequency of the unwanted event. The plant is operational:
5 batches/year * 3 weeks/batch * 7 days/week * 24 hours/day = 2520 operational hours/year or 29% of the year (0.29). Using this value and the data provided, the probability of the event happening is 1/75 /yr. * 0.29 * 0.1 * 0.0956 = 3.7E-5.



Part 3: Because this event has a PLL of 5.64, it is classified as a "Multiple Fatalities Likely". The tolerable frequency is 1.0E-6. Therefore the PFD for the SIS must be 1.0E-6 / 3.7E-5, or 2.7E-2. The Risk Reduction factor of this SIS would then have to be greater than 1 / 2.7E-2, or 37. This means the SIS must be at least a SIL 2.