

EC50 - Pre-Instructional Survey

Name: _____ Date: _____

1. Shutdown systems provide protection for what?

2. Do you believe critical safety functions should be combined in the DCS?
What are the pros and cons of such a design?

3. The majority of control and safety system accidents are due to errors in what?
 - a. Incorrect specifications
 - b. Design & implementation
 - c. Installation and commissioning
 - d. Operations & maintenance
 - e. Changes after commissioning

4. Risk is a function of what two things?

5. Are MTTF (mean time to failure) and Life the same?

6. If a safety system logic box is approved or certified for a certain safety level, does that mean the entire as built system meets the safety level? Why?
7. Place a check by the correct answer:
- a. Which of the following logic systems is the safest (the one most likely to respond to a true demand)?
- 1 out of 1
 - 1 out of 2
 - 2 out of 2
 - 2 out of 3
- b. Which of the following provides the best protection against nuisance shutdowns?
- 1 out of 1
 - 1 out of 2
 - 2 out of 2
 - 2 out of 3
- c. Which of the following provides good safety protection and also good protection against nuisance shutdowns?
- 1 out of 1
 - 1 out of 2
 - 2 out of 2
 - 2 out of 3
8. What are usually the most unreliable parts of a shutdown system, and why?
9. Why do safety systems need periodic testing and how often should this be done?

EC50 - Pre Instructional Survey Answer Sheet

1. Shutdown (or safety) systems protect personnel, the environment, capital equipment, production, litigation, and company image.
2. The separation of safety and process control is not necessarily a black and white issue. This will depend upon the level of risk, but standards from many different industries recommend separation of the two systems.

Advantages of combined systems include single source of supply, potentially lower initial cost, and easier integration of operator interfaces.

Disadvantages of combined systems include increased human interaction and potential errors, difficulty in enforcing security and management of change procedures, potential lack of diagnostics and redundancy required for certain applications, and potential difficulty in communications between different systems.

3. The English Health and Safety Executive (HSE) found that 44% of accidents involving control and safety systems were due to incorrect & incomplete specifications. Specifications are made up of two parts; the functional specification (what the system is supposed to do), and the integrity specification (how well it is supposed to do it).
4. Risk is a function of the probability (or likelihood) of an event, and the severity (or consequences) of the event.
5. MTTF and Life are definitely not the same. In fact, they are not related in any way.
6. A product approval is not the same as a system approval. Using a logic box approved, or certified, for a certain safety level in no way implies the entire system meets the requirements.
7.
 - a. 1 out of 2; the safest system, at the expense of more nuisance trips.
 - b. 2 out of 2; the best protection against nuisance trips, at the expense of safety.
 - c. 2 of 3; good performance in both modes.
8. The field devices. Depending upon the application and your experience, this could be either the sensors, the valve, or both. The logic box is usually in a nice, controlled environment (a control room), while the field devices are exposed to the process and environment, which could be corrosive, erosive, and explosive, with extremes of temperature, vibration, EMI/RFI, etc.
9. No system is 100% fail-safe or has 100% perfect diagnostics. Every system needs to be checked for hidden failures which may prevent the system from responding to true demand. The frequency of testing will be a variable depending upon the desired level of protection, the technology used, and the level of redundancy employed.