CFSP Process Applications

Section 1: Multiple Choice

Candidate Exam Number (No Name):

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

1 **:** Which of the following does not affect PFDavg?

    A. Lambda D.

    B. Proof test interval.

    C. Proof test coverage.

    D. SFF

2 **:** An cyclic process runs through a complete cycle every week. A hazardous event expected to place a demand on the safety function one time per cycle. A Type A single channel (1oo1) SIF has been designed with external automatic diagnostics (not part of safety function) that also runs every week. The following data is provided for the entire SIF:
Lambda DD = 0.002 failures per year,
Lambda DU = 0.0004 failures per year,
Lambda SD = 0.006 failures per year,
Lambda SU = 0.003 failures per year.
The safety functions is fully proof tested every six months.
To what SIL does this design qualify?

    A. Does not meet any SIL

    B. SIL1

    C. SIL2

    D. SIL3

3 **:** For de-energize-to-trip safety system configurations using identical components in low demand mode, which is the correct ranking of architectures in terms of spurious trip rate:

    A. Lowest 1oo2, 2oo2, 2oo3, 1oo1 Highest

    B. Lowest 1oo1, 2oo2, 2oo3, 1oo2 Highest

    C. Lowest 2oo2, 2oo3, 1oo2, 1oo1 Highest

    D. Lowest 2oo2, 2oo3, 1oo1, 1oo2 Highest

4 : What does it mean for a system to have a fault tolerance of 2:

A. Never fail dangerous after 1 random failure

B. Never fail dangerous after 1 systematic failure

C. Never fail dangerous after 2 random failures

D. Never have 2 random failures

5 : What is the best definition of risk?

A. Consequence x Likelihood

B. Likelihood x Frequency

C. Consequence x Vulnerability

D. Occupancy x Vulnerability

6 : How many systematic hardware failures can a 2oo4 system withstand without losing the ability to perform the safety function?

A. 0

B. 1

C. 2

D. 3

7 : If a system with a wear out time of 5 years in normal service is proof tested every 3 years and replaced every 6 years, what is the average probability of failure on demand in normal service assuming a dangerous failure rate of 0.01 failures per year?

A. 0.03

B. 0.015

C. 0.025

D. 0.083

E. It cannot be properly calculated under these conditions.

8 ： Which of the following is not typically a mitigation layer of protection?

    A. Containment dike or bund

    B. Emergency services

    C. Fire suppression

    D. Alarm with operator intervention

9 ： Where is the best place to find information about a safety system component?

    A. IEC 61508

    B. IEC 61511

    C. The Safety Manual from the supplier

    D. Plant procedure documents

10 ： A "smart" transmitter has a total failure rate of 0.08 failures/year. The percentage of safe failures is 75% and diagnostic coverage of dangerous failures is 20%. Assuming all diagnosed dangerous failures will immediately be converted to a safe process shutdown, what is the average probability of failure on demand if the transmitter is tested four times per year. The Mean Time To Repair is estimated to be 8 hours.

    A. 0.0002

    B. 0.0040

    C. 0.0020

    D. 0.0016

CFSP Process Applications

Section 2: Short Answer

Candidate Exam Number (No Name):

Please write down your exam number in the above provided space. Answer the questions in the space provided. If you need additional space please attach a separate sheet with your exam number on it. Make sure to number each attached sheet and label your answer with the corresponding question number.

IMPORTANT NOTE:
There are more than 20 points of questions in the short answer part of the exam. You are only required to answer questions totaling 20 points. You may choose to answer any combination of questions totaling at least 20 points. Please clearly indicate which questions should and should not be assessed as part of the required 20 points.

1 : How should the response time of a safety function be determined as part of preparing the safety requirements specification?
(2 points)

2 : Name 4 aspects that MUST be true about safety system documentation according to 61511.
(2 points)

3 **:** What are two main differences between continuous (or high demand) and demand (or low demand) mode safe
(4 points)

4 **:** Name three things that must be done before modifying a safety system according to IEC 61511.
(2 points)

CFSP Process Applications

Section 1: Multiple Choice Explained EXAMPLE

Candidate Exam Number (No Name):

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

1 : D. SFF

The SFF or safe failure fraction is a ratio of failure rates and does not affect the average probability of failure on demand (PFDavg). However the SFF can affect the achieved safety integrity level (SIL) through th hardware fault tolerance requirements. Lambda D or the dangerous failure rate directly affects the PFDavg as does the proof test interval and the proof test coverage.

2 : C. SIL 2

The safety function falls into the continuous mode because the demand is so frequent and the diagnostics are very slow. This means
that PFDavg does not apply and the proof test has no impact on safety. In addition
it is not possible to take credit for the automatic diagnostics either. Thus the effective dangerous failure rate is 0.0024 failures per year which converts to 2.7 x 10-7 failure per hour which is between the 10^{-7} and 10^{-6} limits that define SIL 2 for continuous mode operation.

3 : D. Lowest 2oo2, 2oo3, 1oo1, 1oo2 Highest

The 2oo2 architecture requires both elements to signal a trip out of only two units present so it has the lowest spurious trip rate. The 2oo3 architecture also requires two elements to signal a trip but there are more units present so this is more likely. Both the 1oo1 and 1oo2 only require a single element to signal a trip which gives them a higher spurious trip rate. Of the 1oo1 and 1oo2, the 1oo2 has more units present so it has the highest spurious trip rate.

4 : C. Never fail dangerous after 2 random failures

The definition of fault tolerance applies to the systems ability to operate even with random failures present. It does not mean that the system will never fail. It also does not mean that it is immune to systematic failures that are capable of causing highly redundant systems to fail regardless of their fault tolerance.

5 : A. Consequence x Likelihood

The correct definition of risk includes both the size of the harm and how often it is expected to occur.

6 : A. 0

Systematic failures are different from random ones and redundant architecture alone does not prevent them from causing a safety function to fail. For example, the single systematic error of specifying the wrong pressure rating of a safety valve in a redundant system can cause all of the valves to fail dangerously in high pressure service and thus prevent the safety function from operating.

7 : E. It cannot be properly calculated under these conditions.

Since the system will be in service without replacement for longer than its useful life, the dangerous failure rate does not apply and the PFDavg cannot be calculated. It is also important to note that the 3 year proof test will also not address the wear out problem.

8 : D. Alarm with operator intervention

Alarm and operator intervention is the only one of these layers of protection that is more typically capable of entirely preventing the harmful accident rather than just making it smaller.

9 : C. The Safety Manual from the supplier

Although IEC 61508 and 61511 provide valuable information about safety lifecycle requirements, they do not contain details about specific safety system components. Similarly, the plant procedures are also not likely to contain the component information although they may refer to the component safety manual provided by the supplier.

10 : C. 0.0020

Taking the total failure rate times (1 - % safe failures) gives the total dangerous failure rate of 0.02 failures per year. Then taking this value times (1 - % diagnostic coverage) gives a dangerous undetected failure rate of 0.016 failures per year. Then applying the lambda x Time / 2 equation for PFDavg gives 0.0020 as the answer.

Section 2: Short Answers Explained

Candidate Exam Number (No Name):

   Please write down your exam number in the above provided space. Answer the questions in the space provided. If you need additional space please attach a separate sheet with your exam number on it. Make sure to number each attached sheet and label your answer with the corresponding question number.

   IMPORTANT NOTE:
   There are more than 20 points of questions in the short answer part of the exam. You are only required to answer questions totaling 20 points. You may choose to answer any combination of questions totaling at least 20 points. Please clearly indicate which questions should and should not be assessed as part of the required 20 points.

1 : How should the response time of a safety function be determined as part of preparing the safety requirements specification?
   (2 points)

   The response time is the sum of the sensing element's scan time, the execution time of the logic, and the actuation time for the final element. When determining the response time, you must first consider the process safety time or the time for the process to move from the safety function trip point to the harmful accident. The SIF response time must be considerably faster than this to prevent the accident. One accepted rule of thumb is that the response time should generally be less than one half of the safety time. This helps ensure that even if the hazardous condition presents itself at the end of a scan cycle, the SIF will still have enough time to react.

2 : Name 4 aspects that MUST be true about safety system documentation according to 61511.
   (2 points)

   IEC 61511-1 section 19.2 mentions several such as:
   It shall be available.
   It shall have unique identities.
   It shall have designations indicating the type of information.
   It shall be traceable to the requirements of the standard.
   It shall have a revision index.
   It shall be revised, amended, reviewed and approved (these 4 are each different).

   Note that the question asks which items MUST be true so answers of "easy to understand" and other "SHOULD" items will only be given partial credit..

3 : What are two main differences between continuous (or high demand) and demand (or low demand) mode safe
(4 points)

Although 61508 (61508-4 Clause 3.5.12-13) and 61511 (61511-1 Clause 3.2.43.1-2) have slightly different definitions, there are a number of acceptable practical differences and they can be referenced to the standards as part of the answer. One difference is that the demand rate is too high for proof testing to be helpful in continuous mode operation while proof testing is an important part of demand mode operation. Another difference is that most dangerous undetected failures of the safety system will lead directly to a harmful accident with continuous mode operation while there are other means (such as the BPCS) of preventing the accident with demand mode systems. Another difference is that SIL is defined by average probability of failure on demand for demand mode while SIL is defined as probability of dangerous failure per hour for continuous mode.

4 : Name three things that must be done before modifying a safety system according to IEC 61511.
(2 points)

IEC 61511-1 section 17.2 mentions several such as:
Procedures for authorizing and controlling changes shall be in place
These procedures shall include a clear method of identifying and requesting the work to be done and the hazards which may be affected.
An impact analysis shall be carried out on the effect the modification will have on functional safety
Modification activity shall not begin without proper authorization.