



xSeriCon

Safety experts & risk consultants

PROCESS MANAGEMENT SYLLABUS

PRACTICE QUESTIONS FOR FUNCTIONAL SAFETY EXAMINATIONS

By
Dr. Peter Clarke, CFSE
Managing Director
xSeriCon

1st Edition
April 2021

Contents

1. INTRODUCTION	3
2. ABBREVIATIONS	4
3. THE SAFETY REQUIREMENTS SPECIFICATION.....	6
3.1. Multiple choice questions.....	6
3.2. Short answer questions	8
3.3. Long answer questions	9
3.4. Answers to multiple choice questions	10
3.5 Answers to short answer questions	13
3.6 Answers to long answer questions	16
4. PRELIMINARY SIS DESIGN	21
4.1 Multiple choice questions.....	21
4.3 Long answer questions	25
4.4 Answers to multiple choice questions	26
4.5 Answers to short answer questions	30
4.6 Answers to long answer questions	34
5. DETAILED SIS DESIGN	39
5.1 Multiple choice questions.....	39
5.2 Short answer questions	40
5.3 Long answer questions	40
5.4 Answers to multiple choice questions	41
5.5 Answers to short answer questions	42
5.6 Answers to long answer questions	43

This book is published by xSeriCon Limited, Hong Kong. Copyright © 2021 xSeriCon Limited.
All rights reserved. ISBN: 978-988-75729-0-9. www.xsericon.world

This is revision 1.02.

1. INTRODUCTION

This document contains study questions to test your knowledge and understanding of functional safety (FS). The questions are suitable for preparing for FS exams such as TÜV FS and exida's CFSP/CFSE, as well as for demonstrating FS competency. The questions are generally more challenging than those in other publications, on the basis that they are designed to demonstrate understanding in depth, rather than superficial formulaic knowledge.

The focus is on FS for process systems, specifically FS management, risk analysis, overall SIS specification and design, and confirmation activities such as verification and validation. Questions are based on the requirements of the international standard IEC 61511:2016 along with typical industry practice.

Topics covered

In this edition, the topics covered are:

- The Safety Requirements Specification (concentrating mainly on hardware requirements; software requirements are not the main focus here)
- Preliminary SIS design (up to the point where SIL verification can be executed; however, the questions do not cover SIL verification itself)
- Detailed SIS design

Please contact xSeriCon if you require practice questions on other functional safety topics.

Question organization and types

The questions are arranged according to topic, and are separated into question types within each topic:

- Multiple choice: where only one answer is correct, or one answer is the best answer among those presented
- Short answer: A few words or 1-2 sentences is expected.
- Long answer: An extended response of several sentences, potentially including tables and/or diagrams, is expected.

Questions are of generally increasing difficulty within each section. Answers, with detailed explanations and references to the IEC 61511:2016 standard, are presented after the questions in each section.

The expected answers are predominantly descriptive, rather than mathematical. This is intentionally done to reflect the typical balance of question content in the CFSP/CFSE examination, where candidates are often surprised by the relatively small number of questions requiring calculation.

About the author

Dr. Peter Clarke CFSE is a Functional Safety consultant, trainer and author with more than 20 years' experience in the chemical industry. After 5 years with exida, Dr. Clarke launched xSeriCon in 2015, serving the chemical industry in Asia Pacific, Europe and the Middle East.

3.4. Answers to multiple choice questions

3.4.1. 3.1.1. The SRS must be prepared for every project where a SIS is implemented.

- A True, the SRS is always required.
- B Only for greenfield projects. Updates to legacy systems do not require an SRS.
- C Only if the SIS contains a SIF at SIL 3 or 4.
- D False. The SRS is optional.

The correct answer is A.

The SRS is a compulsory requirement for every project that implements a SIS, if the SIS is required to comply with IEC 61508/61511.

3.4.2. 3.1.2. A typical double block and bleed arrangement comprises two shutdown valves in series, with a small bleed valve to vent the piping between the valves. What success criterion (“voting”) should be specified for this configuration in the SRS?

- A 1 out of 2 for the two block valves. The bleed valve can be ignored.
- B 1 out of 3.
- C 2 out of 2 for the two block valves. The bleed valve can be ignored.
- D 3 out of 3.

The most likely correct answer is A.

This answer would match the most likely definition of the process safe state (no flow of process gas to the downstream equipment); success or failure of the bleed valve is irrelevant. However, this assumes the valves do not require tight shutoff (TSO) to achieve the process safe state. If TSO is required, then there is an alternative way to achieve the safe state: (a) Close the upstream valve without achieving TSO, AND open the bleed valve to vent the leakage away from the process; or (b) close the downstream valve with TSO. This could be indicated as 1oo[2oo2 OR 1oo1]. In practice, however, this solution is not usually considered when modelling such a system.

3.4.3. 3.1.3. A complete SRS must be prepared as a single document for each project.

- A True, a single document is required.
- B The SRS can be divided into 2 documents: hardware and software.
- C The SRS is required, but the standard imposes no restrictions on the way it is structured.
- D False. The SRS is not a strict requirement.

The correct answer is C.

While IEC 61511:2016 does impose requirements on documentation (see part 1, clause 19), it does not restrict the way information is divided among documents.

3.4.4. 3.1.4. The SRS must specify, for every SIF, how manual trip shall be implemented.

- A True. Manual trip must be specified for each SIF.

- B** Each SIF must either specify how manual trip is implemented or indicate that no manual trip is required.
- C** The SRS only needs to state whether manual trip is required or not. It does not need to specify the means of manual trip.
- D** False. This does not need to be mentioned at all in the SRS.

The correct answer is B.

See IEC 61511:2016, part 1, clause 11.2.8.

3.4.5. **3.1.5.** The SRS must specify, for every SIF, whether auto-reset is required.

- A** True. This must be specified for each SIF.
- B** Only need to specify this for SIFs where auto-reset is required. If it's not required, there's no need to mention it.
- C** False. This does not need to be mentioned at all in the SRS.
- D** Auto-reset is not allowed for any SIFs.

The correct answer is B.

IEC 61511:2016, part 1, clause 11.2.7 indicates that auto-reset should be the exception rather than the rule, and must be specified for SIFs that require it.

3.4.6. **3.1.6.** The SRS must specify the manufacturer and model of each item of hardware in the SIS.

- A** True. It is a full definition of the SIS.
- B** Only for the logic solver, not for sensors and final elements.
- C** False. It is not compulsory to specify this in the SRS.

The correct answer is C.

However, if not specified in the SRS, hardware needs to be specified in another document such as an equipment list, as it is needed input to the SIL verification.

3.4.7. **3.1.7.** The SRS must include all functions implemented in the SIS, even if the SIL target is less than 1.

- A** True.
- B** Functions with $SIL < 1$ need to be included, except for vendor package functions.
- C** False. Functions with $SIL < 1$ do not need to be included in the SRS.

The correct answer is C.

3.4.8. **3.1.8.** A distillation column normally operates at 2 barg and its design pressure is 5 barg. The most appropriate set point for a high pressure trip at the top of the column is:

- A** 1 barg.
- B** 2.5 barg.
- C** 4.5 barg.
- D** None of the above. It would be better to detect high pressure scenarios by high temperature.

The correct answer is C.

1 barg (answer A) is below the normal operating pressure, so not suitable for a high pressure trip. 2.5 barg (answer B) is too close to the normal operating pressure, and this could lead to spurious trip due to normal process fluctuations, especially during startup. Answer D is incorrect because, in distillation columns, pressure normally rises faster than temperature in an upset condition.

3.4.9. **3.1.9.** In order to provide traceability, it is sufficient to indicate the source of data in the SRS by:

- A** Providing a reference to the project's master document list.
- B** Providing a reference to the project's Functional Safety Management Plan.
- C** Providing a list of safety-related reference documents such as the HAZOP report.
- D** Providing an indicator (such as a reference number) on each item of data, indicating the exact source of data.

The correct answer is D.

Traceability is useful only if it provides a specific indication of where each item of data originated.

3.4.10 **3.1.10.** Which of the following documents is typically required as input to the SRS?

- A** SIL assessment (SIL classification) report.
- B** Factory Acceptance Test (FAT) report.
- C** Management of Change procedure.
- D** SIS validation report.

The correct answer is A.

The other answers may be generated after the SRS is already completed (answers B and D) and do not provide information required for the SRS.

3.4.11. **3.1.11.** Suppose we have a sensor which, according to the Cause & Effect Diagram, closes 5 valves. Which final elements should be included in the SRS?

- A** Only the sensor needs to be included.
- B** All 5 valves in a 1-out-of-5 configuration.
- C** All 5 valves in a 5-out-of-5 configuration.
- D** Only those valves whose closure is necessary to achieve the designated process safe state.

The correct answer is D.

Non-critical final elements are not part of the SIF, and therefore need not be included in the SRS.

3.4.12. **3.1.12.** Suppose we have a Plant Shutdown (PSD) SIF which triggers a Unit Shutdown (USD) trip. For the PSD SIF, what final elements should be shown in

the SRS?

- A** Only the PSD's final elements shown in the Cause & Effect Diagram. The USD can be ignored.
- B** Only the USD's final elements shown in the Cause & Effect Diagram. The PSD can be ignored.
- C** All the final elements of both the PSD and the USD.
- D** Only the final elements of the PSD and USD that are necessary to achieve the designated process safe state.

The correct answer is D.

The SRS should mention all final elements necessary to achieve the safe state, no matter whether they are designated PSD or USD in the Cause & Effect Diagram.

3.5 Answers to short answer questions

- 3.5.1.** **3.2.1.** The combustion chamber for a particular fired heater has a design pressure of 0.1 barg. The normal operating pressure is 0.01 barg.
- (a)** Suggest an appropriate setpoint for an overpressure trip in the combustion chamber.
 - (b)** Is there a better alternative for detecting typical combustion chamber overpressure scenarios? If so, suggest an alternative. State your reasoning.

Answer

(a) A possible set point would be in the range 0.05 to 0.07 barg – outside the normal operating range, but leaving time for the SIF to act before the overpressure occurs.
(b) However, it would be better to detect the demand scenarios by some other method. This is because the narrow operating window between normal pressure and overpressure may be hard to detect and act on automatically, without causing frequent spurious trips. The SIS designer should refer back to the HAZOP report to find out the actual root causes of high combustion chamber pressure, such as flue gas damper out of position or fuel gas high pressure.

- 3.5.2.** **3.2.2.** The SRS must specify the safe state to be achieved. Suppose a SIF is provided to prevent overpressure of a gas-containing vessel D-100 by opening a blowdown valve BDV-1002 to flare. Give an example of a “safe state” definition for this case.

Answer

The safe state should be defined in terms of the process condition (not the condition of the SIF final elements). Therefore, a suitable safe state definition is “No exceedance of design pressure of D-100”. However, examiners may accept an answer such as “BDV-1002 achieves >90% opening within xx seconds”, as this is (unfortunately) a typical industry safe state definition.

- 3.5.3.** **3.2.3.** For each of the following items of information, state whether it is necessary to be included in the SRS. (Simply answer Yes or No to each)
- (a)** Whether a trip alarm is raised when the SIFs activate

- (b) The Safe Failure Fraction (SFF) of each component
- (c) Fireproofing or other survivability requirements for each component
- (d) The brand and model of the logic solver

Answer

(a) No, (b) no, (c) yes, (d) no. IEC 61511:2016 clause 10.3.2 details the requirements for the hardware SRS.

- 3.5.4. 3.2.4.** Draw a Cause & Effect Diagram that sufficiently depicts the following SIF: On low low pressure from PIT-1234A/B/C (2 out of 3), close shutdown valves XV-47 and XV-48 (1 out of 2 success criterion) and open bleed valve XV-49, all actions to be completed within 10 seconds.

Answer

The following is a possible answer. The final element success criterion (1oo2) is typically not shown in the Cause & Effect Diagram.

CAUSES				EFFECTS		
Sensor	High or low	Voting	Response time (end to end)	XV-47	XV-48	XV-49
PIT-1234A	Low	2oo3	<10 s	Close	Close	Open
PIT-1234B	Low					
PIT-1234C	Low					

- 3.5.5. 3.2.5.** The SRS is required to identify “sources of demand” for each SIF. Give 2 typical examples of “sources of demand”.

Answer

Causes of demand are equivalent to the HAZOP causes for cases where SIFs are used as safeguards. Typical examples are:

- Control loop malfunction
- Actuated valve operates inadvertently
- Electric motor (e.g., for pump or compressor) trip
- Loss of feed from upstream source
- Plugging of tubes in a heater
- Misoperation (e.g., operator misoperates a manual valve)

- 3.5.6. 3.2.6.** Apart from proof test interval, what other information regarding proof testing should be documented in the SRS?

Answer

The following should be documented:

- Proof test procedure (can be a reference to a separate document)
- Expected maximum proof test duration (as this is required input for the SIL verification)
- Whether proof testing will be done with the process online or offline
- If the process will be online, what measures will be taken to offset the loss of protection during proof testing

- Whether proof testing of multiple elements (e.g., in a 2oo3 group) will be staggered
- The means of providing overrides for proof testing

3.5.7. **3.2.7.** Give 3 examples of environmental conditions that should be defined for the SIS.

Answer

Referring to IEC 61511:2016 clause 10.3.2 bullet 27: temperature limits, humidity limits, and resistance to: contaminants, loss of grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning.

3.5.8. **3.2.8.** The SRS should document survivability requirements in the event of a major incident. Give 2 examples of the types of incident that may need to be considered.

Answer

Major fires and floods are the most likely incidents that are relevant here.

3.5.9. **3.2.9.** Why does the SRS have to include a maximum spurious trip rate for each SIF? Give at least 2 reasons why spurious trip is an important consideration in the safety performance of a SIF.

Answer

While spurious trip does not directly create a safety issue (as it places the relevant part of the process in a safe state, by definition), it can lead to other issues such as:

- Increased demand on other SIFs (when one SIF trips, it may place a demand on another SIF), which may exceed the assumed demand rate on the other SIFs
- Increased stresses on process equipment, potentially leading to an increased probability of equipment failure
- Environmental impact (trips may lead to blowdown and/or flaring)
- Repeated spurious trips may tempt operators to override safety functions in order to meet production targets.

3.5.10. **3.2.10.** If a qualitative method (such as Risk Graph) is used to determine the SIL target, how can the target Risk Reduction Factor (or PFDavg/PFH) be defined in the SRS? Explain your reasoning.

Answer

The concern here is that quantitative SIL determination methods such as LOPA provide both a SIL and a failure measure (RRF, PFDavg or PFH) target, qualitative methods such as Risk Graph only provide a SIL target. However, it is possible to derive a failure measure target from qualitative methods, as follows.

The Risk Graph normally defines a range of frequencies for each likelihood category (usually labelled W0, W1, W2 etc.), for example W1 may be designated “0.1 to 1.0 times per year”. The upper end of this frequency range should be selected, and multiplied by the probability of failure of all valid independent layers of protection that occur before the SIF, e.g., an independent control loop or alarm with operator response. The resulting value is a plausible upper limit for the expected actual demand rate of the SIF. Dividing this by the tolerable frequency yields the target RRF. If the

tolerable frequency is not known, it can be back-calculated from the Risk Graph by taking a case where (e.g.) SIL 1 is specified, assume conservatively $RRF = 10$ (or a mid-range value such as $RRF = 30$) for such a SIF, estimate the expected SIF demand rate for such a case, and thereby deduce the effective tolerable frequency. (Better still, refer to the documented calibration basis for the Risk Graph; however, this is rarely available in practice.)

- 3.5.11.** **3.2.11.** Suggest a reason why the software SRS is typically prepared separately from the hardware SRS.

Answer

There are 2 main reasons:

- According to IEC 61511:2016 part 1, clause 10.3.3, the software SRS is developed using the hardware SRS as a source of information. Therefore, the hardware SRS has to be developed first.
- The two SRSs are usually developed by different teams. In practice, the software SRS is often prepared by the SIS system integrator, not the main engineering contractor.

- 3.5.12.** **3.2.12.** Give 3 examples of information that should be included in the software SRS.

Answer

Refer to IEC 61511:2016 part 1, clause 10.3.5 for a list. Some simple examples of information requirements are:

- All implemented SIFs with their SIL target
- Which process operating modes are applicable for the SIFs
- Action to be taken on bad process variable
- Functions enabling proof testing
- Functions enabling diagnostics in field equipment
- Application program self-monitoring requirements
- Details of communication interfaces

3.6 Answers to long answer questions

- 3.6.1** **3.3.1.** The SRS should include a description of the functional relationship between sensors and final elements for each SIF. Suppose we have a SIF including the following field hardware:
- 3 pressure transmitters (PT-1234A/B/C) in a 2-out-of-3 configuration, trip on high pressure
 - 2 groups of final elements with 1-out-of-2 success criterion:
 - Group 1: Shutdown of the electric motor of a pump (P-100)
 - Group 2: Closure of an air-operated shutdown ball valve (XV-241).

Show 2 different methods for depicting the functional relationship within this SIF. Also include at least 2 additional interposing elements that would typically be included in such a SIF.

Answer

There are 3 typical ways to depict the functional relationship:

- Textual description
- Cause and Effect Diagram
- Logic Diagram

The following additional elements are typically included:

- Intrinsically safe (IS) barriers on input and/or output sides
- Interposing relay in the signal from the logic solver to the pump's motor control circuit (MCC)
- Solenoid-operated valve and actuator on the ball valve

Text description:

Sensors	PT-1234A/B/C, each with IS barrier
Sensor voting	2oo3
High or low trip	High
Final element group 1	Low signal to P-100 MCC, trip input via interposing relay
Final element group 2	Low signal to solenoid valve of XV-241 (ball valve with quarter turn actuator, single acting, close to trip) via IS barrier
Final element success criterion	1oo2 groups

Cause and Effect Diagram:

CAUSES				EFFECTS	
Sensor	High or low	Voting	Interposing components	P-100 MCC trip signal (low to trip) via interposing relay	Solenoid valve of XV-241 (with quarter turn actuator, single acting, close to trip)
PT-1234A	High	2oo3	IS barrier	Low	De-energise
PT-1234B	High				
PT-1234C	High				

(Final element success criterion: 1oo2 groups)

Logic Diagram:

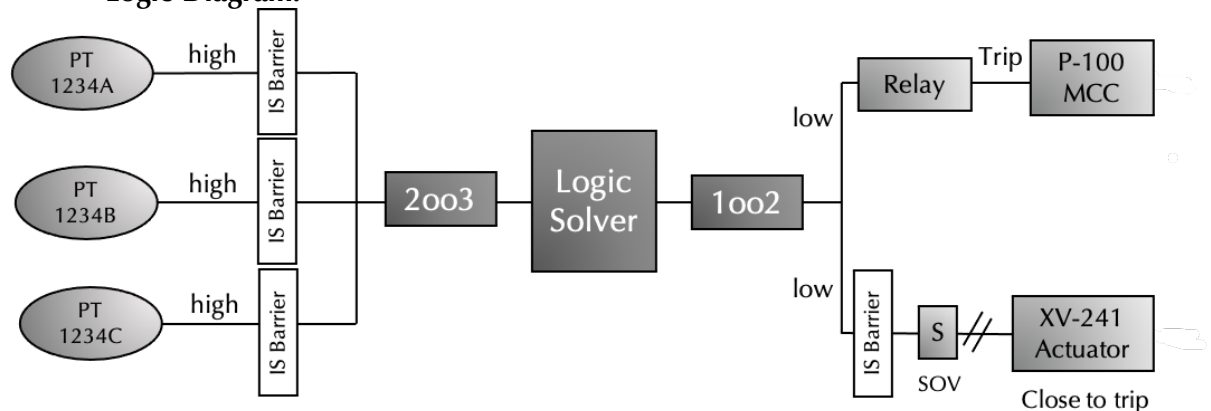


Figure 1: Logic diagram for this configuration

3.6.2. **3.3.2.** After developing the SRS, the SIS must be designed in accordance with the requirements in the SRS. According to the standards, how should the design