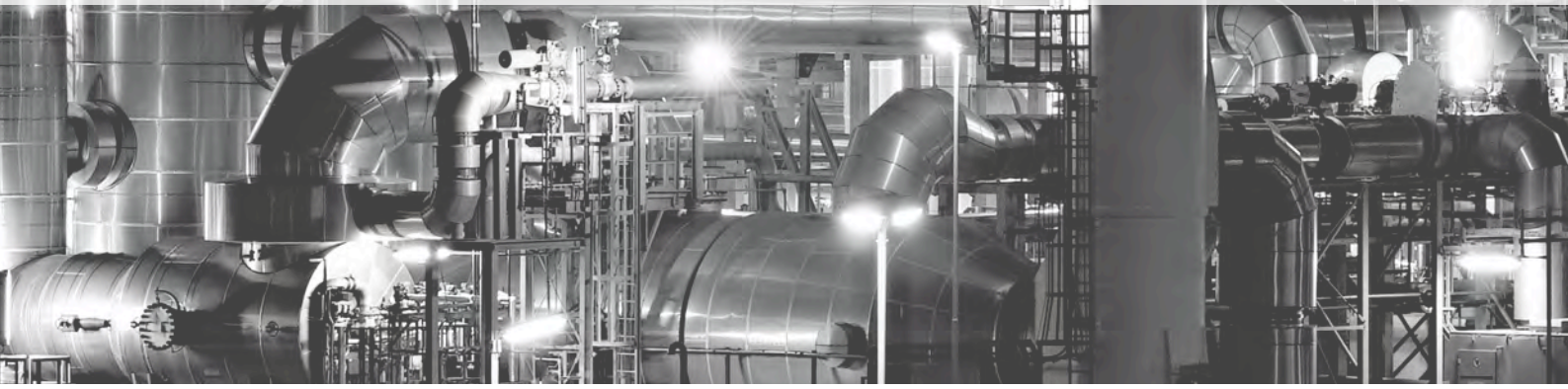
FUNCTIONAL SAFETY VOCATIONAL TRAINING

Functional Safety Engineer (TÜV Rheinland) Safety Instrumented System

rev. 2022-00



COURSE PREPARATION

- General information
- Training Agenda
- Eligibility Requirements info
- SIL manual excerpt
- Sample Questions
- Trainer info & facts

Within the TÜV Functional Safety Program:

TÜVRheinland®
Precisely Right.

The purpose of this document is to help YOU preparing for the Functional Safety Engineer (TÜV Rheinland) SIS training.

- **General information**
  FirstofallcongratulationthatYOUdecidedtojointheflagshiptrainingFSEngineerSIS of TÜV Rheinland. Background in both IEC61511 and IEC61508 would be ideal. Nevertheless it is common that people do not have that and still manage to get thru the course and pass the exam. We have foreseen in this manual an excerpt of the SIL manual of GM International for your to read and understand chapter 7 (IEC61511) and chapter 8 (SRS). My advise is, foresee 4 days during the training of ONLY training and study/review time. Do not spend your evenings catching up with your normal work/tasks. You will need every minute to review your home work and material and get ready for your exam on the morning of the last day.

- **Training Agenda**

- **Eligibility requirments (ER) info**
  Theeligibilityrequirmentformisaseparatefile/formthatshouldhavereceivedfromthe course organising party. Included in this manual here is a filled example (4 pages) that shows you exactly what YOU will NEED to fill in carefully - correct and complete!
  The ER document file can be filled in electronically and together with the supporting file/ documents (university degree OR employer statement letter) should be saved in 1 PDF file with as filename your EXACT name spelling as your require on the certificate.
  Alternatively a quality hard copy of a by hand filled in and legibly ER document can be scanned and returned by email. In case or no electronic document or scan possible, then a hard copy needs to be presented on the first training day at the class to the teacher

- **SIL manual excerpt**
  TheSILManual-SafetyInstrumentedSystemsiscurrently(Jan2018)inthe1streprint -4th edition and will be provided either as ebook or hardcopy during the training course. For those having a copy already, I would not recommed to read the complete book (277 pages) BEFORE the course. But as a minimum, we recommend to read Chapter 7 - IEC 61511 Ed 2.0: Functional safety - Safety Instrumented Systems for process industry sector and Chapter 8 IEC61511 Ed. 2.0 - SIS Safety Requirement Specification (SRS). Both chapters are included here in this manual and will be a good foundation for the training course, but again is not a mandatory requirement.

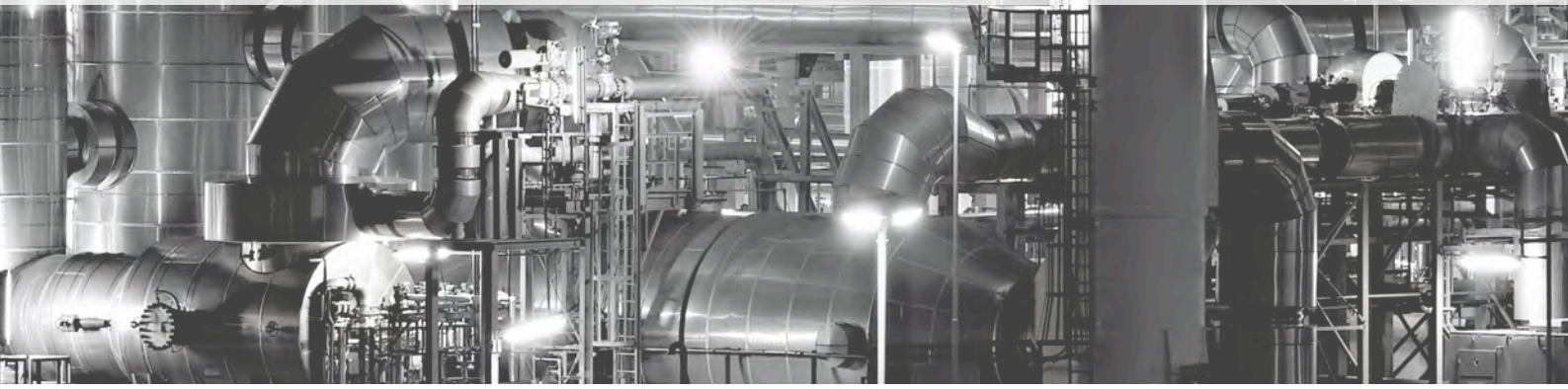
- **Sample questions**
  The sample questions are purely to give YOU an idea of a multiple choice questions and answers. Those 15 questions originated out of a pool of questions that were available begin 2000 made by a group of engineers who started the foundation of competency review programs today on the market. Those Q&A do not reflect the quality of the exam questions of this training course.

- **Trainer info & facts**
  Tino Vande Capelle - Functional Safety Senior Expert & Trainer (TÜV Rheinland, #109/05, SIS) resume from LinkedIn - Feedback from previous participants and Training FACTS 2019

FUNCTIONAL SAFETY VOCATIONAL TRAINING

Functional Safety Engineer (TÜV Rheinland) Safety Instrumented System

rev. 2022-00



TRAINING AGENDA

Within the TÜV Functional Safety Program:

TÜVRheinland®
Precisely Right.

Course duration: 3 consecutive days + 1/2 day exam

DAY 01

- **Introduction to Functional Safety**
  - Modern history of disasters
  - What is safety?
  - Legal status IEC61511
  - Overview of legal requirements
  - Layers of protection
  - Safety Instrumented System
  - Safety Integrity Level
  - Problems with safety systems
  - Safety system failures
  - What is Functional Safety?
  - Functional Safety Standards
- **Management of Functional Safety**
  - Lifecycle concept 61508/61511
  - Functional Safety Management
  - Competency
  - Risk evaluation and management
  - Safety Planning
  - Implementation and monitoring
  - Functional Safety Assessment
  - Functional Safety Audit
  - SIS configuration management
- **Planning the Safety System**
  - Safety lifecycle structure/planning
  - FS management system
  - Verification & Validation plan
  - Safety Requirement Specification
- **Verification & Application Program**
  - Verification planning
  - Verification testing
  - Application program verification

DAY 02

- **Process Hazard & Risk Assessment**
  - Hazard & Risk definition
  - Tolerable risk and ALARP
  - Risk management
  - Hazard Identification Techniques, FMEA, FTA, HAZOP
  - Hazard Analysis Techniques, ETA, dispersion modeling, bowtie
  - Hazard Analysis Techniques ETA
  - Risk Reduction Techniques, risk matrix, risk graph,
  - Security Risk Assessment, digital mapping, Security Levels, Security Assurance Levels, Foundational Requirements
- **Allocation Safety Function to layers**
  - Layer Of Protection Analysis LOPA
  - Typical IPL characteristics
  - LOPA working example
  - LOPA pros and cons
  - LOPA CCPS books references
  - SIF operating modes and Safety Integrity Requirements
- **Safety Requirement Specifications**
  - SRS general requirements
  - SIF description requirements
  - MTTR-MRT, etc
  - Application Program SRS

DAY 03

- **SIS Design and Engineering, AP development**
  - General requirements H/W
  - Safety Manual as per IEC61508
  - Hardware concepts
  - IEC61511 SIF - mode of operation
  - Safety - vs Process - HFT
  - Diagnostics - vs Proof - test
  - IEC61508 Safe Failure Fraction
  - Architectural constraints Route 2H - Route 1H
  - Selection of devices/field devices
  - Maintenance and testing requirements
  - Quantification of Random Failures
  - Three barriers to clear to claim SIL

  - General requirements AP
  - Application Program (AP) design
  - V-model lifecycle documentation
  - AP implementation
  - AP verification and testing
  - AP methodology and tools

- **Installation, Commissioning and Validation**
  - Installation plan and documentation
  - Activities, procedures and techniques
  - Validation FAT - SAT

- **Operation and Maintenance**
  - Planning operation/maintenance
  - Procedures operation/maintenance
  - Bypass - MOS
  - Proof test procedure for every SIF
  - Training for operators/maintenance personnel

- **Modification**
  - Modification objectives
  - Input needed
  - Change vs Modification
  - Before you start modification
  - During modification
  - After modification
  - FSA before you begin

- **Decommissioning**
  - Procedures, analysis and authorisation
  - SIF requirements

- **Wrap up**
  - Summary
  - Exam preparation

- **Student exercises**

  With the student exercises, the participants will have the opportunity to put the learned theory into practice

  - Failure classification
  - video Bhopal - FS Management
  - FMEA
  - FTA
  - video BP Texas City - documentary
  - HAZOP
  - HRA techniques evaluation
  - SIL selection exercise
  - Define a SIF description
  - System architectures & HFT
  - Design SIF's using SFF & HFT
  - video Williams Olefins - documentary

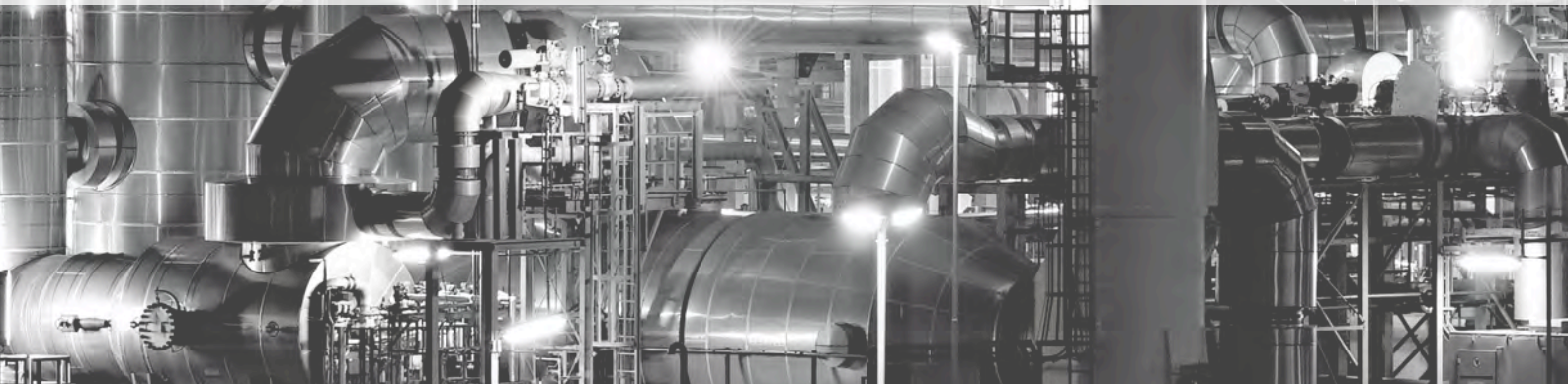
  - Morning sessions - homework question review (only day 01 & 02)
  - Questions & Answers

This page is intentionally left blank

FUNCTIONAL SAFETY VOCATIONAL TRAINING

Functional Safety Engineer (TÜV Rheinland) Safety Instrumented System

rev. 2022-00



ELIGIBILITY REQUIREMENTS

Within the TÜV Functional Safety Program:

TÜVRheinland®
Precisely Right.

TÜV Rheinland Functional Safety Training Program

READ ME FIRST

PLEASE check every YELLOW/RED box below, DO NOT forget to fill, sign, date etc as advised below
INCOMPLETE FORM = NO EXAM!

USE the EMPTY 'editable' form YOU received + SAVE the form/file with filename = your EXACT NAME as you want on YOUR certificate and return BEFORE the course start, alternatively BRING a papercopy to the class on the FIRST day

Name of participant:	First Name - Family Name (exact name spelling as YOU want to have it on YOUR certificate !)
Training Date:	This will be filled in by TinoVC
Training Location:	
Exam Date:	
Trainer:	**Mr. Tino Vande Capelle (#ID 109/05)**

1. Functional Safety Experience:

Please give proof of 3 years of business experience in Functional Safety.

Position/Title	Company Name	Location
Your position or Title	The company name	Location / Country of the company
Start date: start month / year	Description of duties: Summarise your experiences to FIT this box. PLEASE MAKE SURE the word 'SAFETY' is in your text, Process automation / industrial automation / Process safety related experience etc. DO NOT attach a CV/resume to this file. When you fill in this PDF electronically, make SURE ALL fit in this box, or form WILL be REJECTED	
End date: end month / year. Please fill 'current job' when you still hold this position		
Total # months: Number of months from start to end/current date!		

Functional Safety or Security relevant experience (continued)

Position/Title	Company Name	Location
Start date:		
End date:		
Total # months:		

REPEAT IF NECESSARY,
WE NEED MINIMUM OF 36 MONTHS
(3 YEARS) EXPERIENCE EVIDENCE

Position/Title	Company Name	Location
Start date:		
End date:		
Total # months:		

REPEAT IF NECESSARY,
WE NEED MINIMUM OF 36 MONTHS
(3 YEARS) EXPERIENCE EVIDENCE

Position/Title	Company Name	Location
Start date:		
End date:		
Total # months:		

REPEAT IF NECESSARY,
WE NEED MINIMUM OF 36 MONTHS
(3 YEARS) EXPERIENCE EVIDENCE

Total numbers of **YEARS** **(NOT months !!)** example: **3+** is the minimum we need to see!

Total number of years of relevant business experience in Functional Safety	.... years	A minimum of 3 years of experience in the field of Functional Safety is required

WITNESS

2. University degree (minimum Bachelor's) in relevant field:

University Name:	- When you have a UNIVERSITY degree, then YOU need to fill in **EVERY** field of this table **AND** YOU need to attach a COPY of your degree/diploma (preferably attached as PDF, alternatively a paper copy can be brought to the first day of class) - When attached check the box below! - Language accepted are Dutch/French/German/Italian/English. **ANY** other language diploma need to have a certified official translation in English
City:	
Country:	
Technical Field:	
Degree Title:	
Date:	
Copy of Degree/Diploma attached:	☑ Yes ☐ No WITNESS

3. Reference Letter:

Only applicable for persons who do not have an engineering degree.

Company Name:	Alternatively to the university degree, you need a letter from your employer on **a company letter head & signed by your supervisor/manager.** Below some sample of text: *I hereby testify that <name> has the skills and equivalent engineering experiences, as outlined in section 1 of the TUV Rheinland Eligibility Requirements form.* *I therefore have no hesitation in putting <name> forward as a suitable candidate for this program.* *Do not hesitate to contact us if you need further information...*
City:	
Country:	
Technical Field:	
Title / Responsibility:	
Date:	
Signed letter attached:	☑ Yes ☐ No WITNESS

READ and **make YOUR selection** clear with the below **4 check boxes**
This is to be in line with the **GDPR** (General Data Protection Regulations)

4. Personal and Business Data:

This information is provided for the following specific reasons	
1	… to enable TÜV Rheinland Industrie Service GmbH, Automation, Functional Safety & Cyber Security, to contact me regarding my FS Engineer (TÜV Rheinland) certificate,
2	… to enable TÜV Rheinland Industrie Service GmbH, Automation, Functional Safety & Cyber Security, to contact me in the future by email for any issues related to my FS Engineer (TÜV Rheinland) certificate.
I confirm that TÜV Rheinland is a Data Processor in the context of the GDPR, and collects information which entails the following data processing:	
1	Collecting contact details – including business email address.
2	Collecting eligibility information including name, mailing address, employment history, copy of relevant academic history and qualifications or employer letter certifying experience.
3	Recording my name, contact details and examination results.
4	Issuing a certificate including my name and country of my location.
5	Listing my name, country of my location, ID number of certificate and topic of training I attended on the TÜV Rheinland website.
6	Storing of this data.
☑	I give my consent for the collection and processing of my personal data as outlined above.
☐	I **do not** give my consent for the collection and processing of my personal data as outlined above – I understand that this will mean that I will not get my FS Engineer (TÜV Rheinland) certificate.
☑	I understand that I am able to change and/or update contact information by contacting TÜV Rheinland.
☐	I **do not** wish to be contacted by TÜV Rheinland about further information.

Information for
FS Engineer (TÜV Rheinland)
Certificate

Please type or write in block letters

Full Name as you would like it to appear on the FS Engineer (TÜV Rheinland) certificate)	**YOUR EXACT NAME spelling as YOU want to have it on YOUR certificate**
Company	**NOT a MUST!** As the certificate will be on your personal name
E-Mail Address Only business email address	WE NEED 1 (ONLY 1) **VALID email address** to deliver your certificate.
City	**NOT a MUST!** As the website only list your name & country
Country	This **country** name is used on the TUV Rheinland - website next to your name on the list of FS ENGINEERS
Signature	Your Signature (Digital in Adobe Acrobat is acceptable - or - manual)
Date	Don't forget the date of signing this document!

SIGN HERE

Note

WITNESS

I confirm that the above information is correct and accurate to the best of my knowledge.

WITNESS

I understand that inaccurate information could void my **FS Engineer (TÜV Rheinland) certificate** any time in the future.

WITNESS

SIL MANUAL

Functional Safety Engineer
(TÜV Rheinland)
Safety Instrumented Systems

TRAINING PREPARATION MATERIAL

rev. 2022-00

This is a excerpt for FS Eng SIS course preparation only covering:

- chapter 7 - IEC61511:2016
- chapter 8 - Safety Requirement Specifications

gmi technology for safety

FS Eng SIS Edition

SAFETY INSTRUMENTED SYSTEMS

Manual for Plant Engineering and Maintenance

With reference to IEC61508 Ed. 2.0 “Functional safety of electrical/ electronic/programmable electronic safety-related systems” and IEC61511 Ed. 2.0 “Functional safety - Safety instrumented systems for the process industry sector”.

4th Edition - 1st reprint

Authors

Abbamonte Basilio
Software Development and Quality Assurance Manager, GM International.

Glisente Landrini
President and Managing Director, GM International.

Chapters 7 and 8
Tino Vande Capelle
Director Functional Safety Services, GM International.
FS Senior Expert and Trainer (TÜV Rheinland, # 0109/05, SIS).

gmi technology for safety

www.gminternationalsrl.com

ISBN: 978-88-942087-0-2
ISBN-A: 10.978.88942087 / 02
SIAE: 2017000345

Printed in Italy

Introduction

GM International designs, manufactures and sells SIL2 and SIL 3 certified Intrinsically Safe Interfaces for use in Hazardous Locations, Safety Relays and Power Supplies that are intended to prevent accidents before they occur, thus reducing risk and enhancing safety in a very wide variety of applications.

This manual is a practical aid for the analysis, installation and maintenance of safety instrumented systems and associated components and will hopefully serve as a guide for understanding and implementing procedures into practical applications.

It represents an effort to share the results achieved in many years of research and experience in the field, with anyone willing to approach Safety Related Systems.

This manual is not intended for safety reliability specialists, but for the thousands of professionals employed in process industries who work with safety instrumented systems and who are expected to follow the appropriate industry standards.

Aren't the standards alone enough? The answer depends upon the knowledge and experience of the individual and the company.

The growing demand for experts in a critical sector like functional safety, underlies the urgency of a greater awareness and comprehension of all subjects presented herein.

Glisente Landrini
President

Index

ATTENTION

This is a excerpt of the SIL MANUAL - Safety Instrumented Systems, 4th edition for the Functional Safety Engineer (TÜV Rheinland) SIS course preparation and will only cover:

· chapter 7 - IEC 61511 Ed 2.0: Functional safety - Safety Instrumented Systems for process industry sector

· chapter 8 - IEC61511 Ed. 2.0 - SIS Safety Requirement Specification (SRS)

Chapter 7 IEC 61511 Ed 2.0: Functional safety - Safety Instrumented Systems for process industry sector

This chapter presents a general overview of the “IEC 61511 – Functional safety – safety instrumented system (SIS) for the process industry sector - Normative Part 1: Framework, definitions, system, hardware and software requirements”, edition 2.0. This is based on the CDV version (65A/691/CDV - 2014-05-09, CDV=Committee Draft for Vote) of the standard and the author’s interpretation of the changes in relation to edition 1.0.At the time of releasing this chapter the forecasted publication date of IEC61511 Ed. 2.0 – part1 has been postponed to 2016-03. Please note that there may be additional or different changes to the final published version of the IEC 61511 Ed 2.0

7.1 Introduction

This chapter outlines a general overview of the IEC61511 Ed 2.0 and the expected changes to be published forecast 2016-03. (source www.iec.ch, SC 65A Work programme (15), Fcst. Publ. Date – status Sep 2015). It is not the intention to summarize the complete 3 parts of the IEC61511 edition 1.0 or 2.0, nor will this text replace any definition or concept of the IEC61511 Ed. 2.0 standard.

7.2 History

IEC61511 Ed. 1.0 was first released in 2003 and was based on the principles of the ‘umbrella standard’ IEC61508 Ed. 1.0 that was earlier released in 1998. Because of the IEC61508 Ed. 2.0 being revised and released in April 2010 is imminent that the changes will have an immediate effect on the current IEC61511 and its future revision.
It should be emphasized that the IEC61508 is clearly more focusing on the manufacturers building safety equipment/instrumentation & systems, whereas the IEC61511 is mainly used by the end user/plant/project perspectives to realize a SIS in the process industry.
The acceptance and adoptions of IEC61511 varies around the world, but is in many countries (E.g. UK, Norway, Belgium, etc) becoming a well-accepted standard of good practice for safety instrumented systems in the process industry. It's certainly not a legal requirement in itself, but the requirement to implement good practice is a legal requirement.

7.3 General overview of IEC61511 Ed. 2.0

The IEC61511 Ed. 2.0 standard is a ‘performance’ based standard and although many definitions have changed to be more prescriptive and used the word SHALL throughout the standard, it is not just following a prescriptive cookbook with recipes. The standard remains

with two fundamental concepts to its application, the safety lifecycle and safety integrity levels (SIL) to express how well the system is expected to perform. The safety lifecycle is a rational engineering design process with a systematic approach that is helping people outlining a good engineering practice for safety instrumented system design, engineering and maintaining safety. There are technical requirements and non-technical or management requirements in the standard as shown in Figure 81 (ref. IEC61511 Ed. 2.0 part 1).

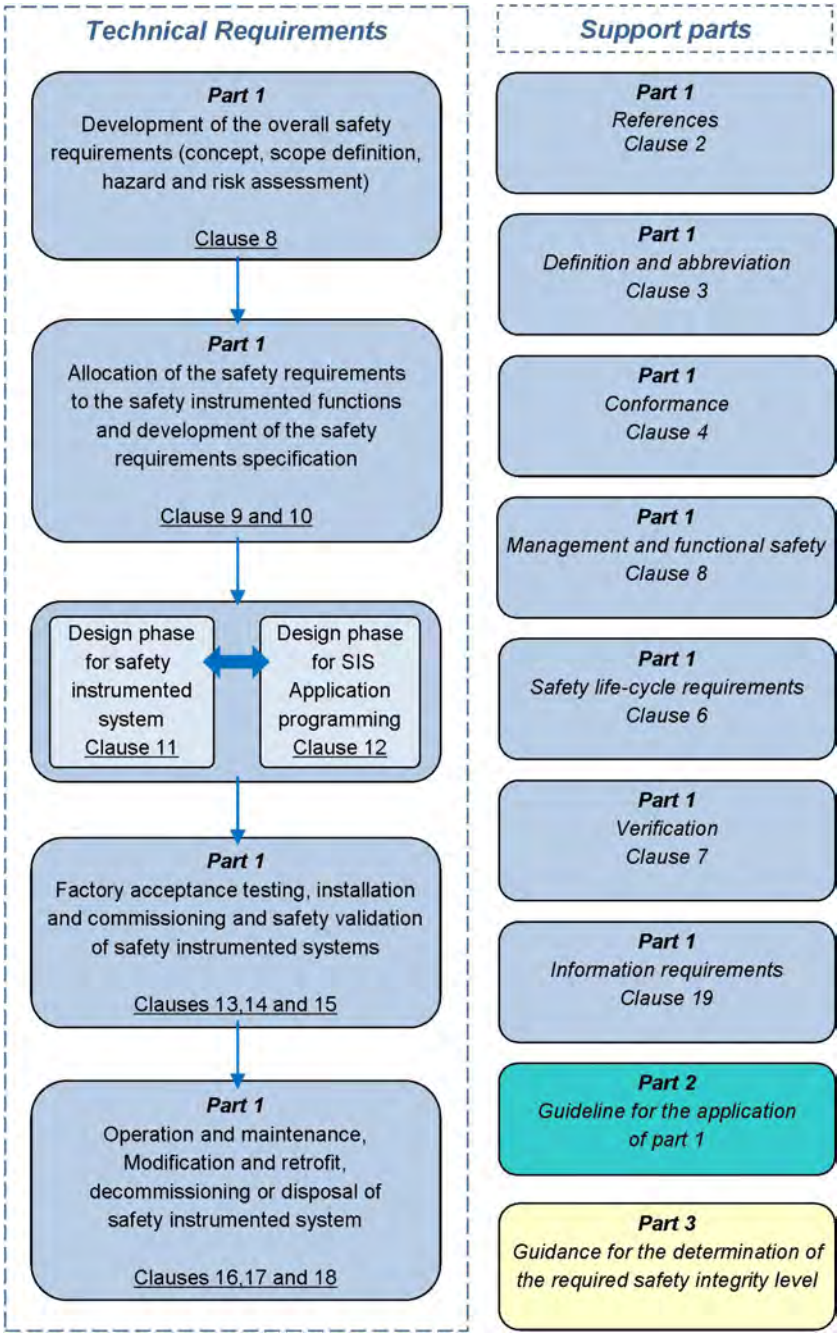


Figure 81, Overall framework of this standard

There are still three parts in edition 2.0, similar concepts as in IEC61511 Ed. 1.0:

Part 1 is NORMATIVE and contains: Framework, definitions, system, hardware and software requirements (publication date 2016-03).
Part 1 outlines the requirements for compliance from clause 5 through 19. There is Project planning, management, documentation, and requirements for competence, as well as the technical requirements for achieving safety throughout the safety lifecycle are defined.

Part 2 is INFORMATIVE and contains: Guidelines for the application of IEC61511-1 (Forecasted publication date 2016-03, status Feb 2016).
Part 2 provides guidance on how to read and understand the clauses of Part 1.

Part 3 is INFORMATIVE and contains: Guidance for determination of the required safety integrity levels (Forecasted publication date 2016-03, status Feb 2016).
Part 3 gives general guidance for risk and safety integrity levels.
Annex A covers the ALARP principle (As Low As Reasonably Practicable),
Annex B through I covers both quantitative and qualitative approaches to SIL selection using event tree analysis, safety layer matrix method, risk graph, LOPA (Layer Of Protection Analysis), risk matrix.
Annex J is new in Ed. 2.0 handling Multiple safety systems describing systemic dependencies.

In general, the IEC61511 standard:

- Requires that a process hazard and risk analysis is performed
- Requires allocation of safety functions to protection layers
- When the tolerable risk cannot be met, then additional protection layers will need to be specified in the safety requirements specification (SRS) for the safety instrumented system (SIS)
- Specifies requirements for system architecture, hardware configuration, application program and system integration
- Specifies techniques and numerical targets (SIL levels) to measure the performance of the SIS
- Requires Field data to be collected through operational and mechanical integrity program activities to assess actual SIS performance
- Uses a safety life cycle, and defines a list of activities and responsibilities required for functional safety management and compliance
- Defines the requirements for testing and analysis, documenting the performance and the need for FS assessments and audits with competency and independencies to be taken into account.

7.4 IEC61511 Ed. 2.0 - part 1 Overview

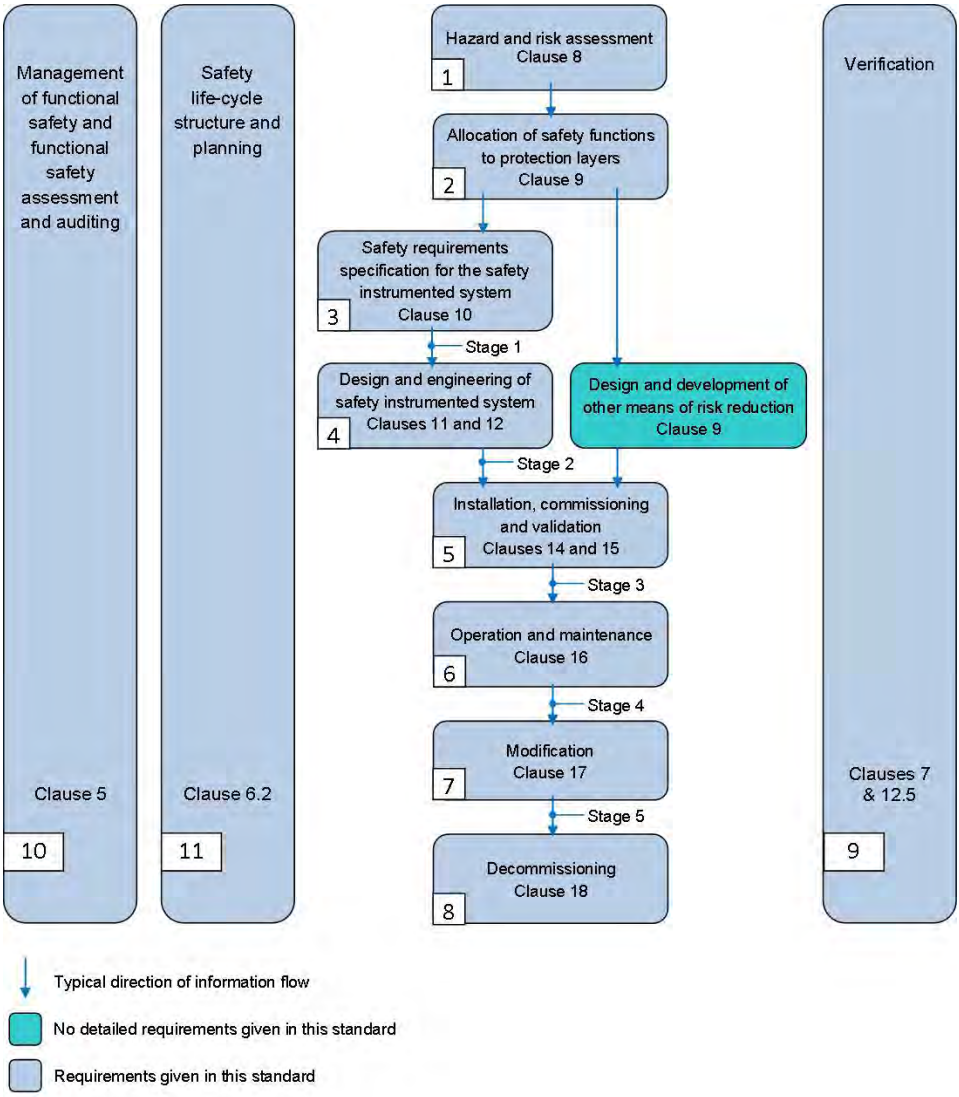
The IEC61511 describes a good engineering practice management system for the end user/ operator/owner on how to specify, design, engineer, verify, assess, install, commission,

validate, operate, maintain, document and continuously improve the correct functioning of the SIS. The essential roles, responsibilities and competencies of anyone involved in the life cycle need to be defined, described in procedures and monitored to support the consistent execution of their work needed to achieve functional safety.

In order to prevent human failures, a systematic approach has been defined in the standard by the use of life cycle model. The technical and non-technical requirements are referred to as 'clauses' in the standard, there are in total 19 clauses:

- Clause 01: Scope
- Clause 02: Normative Requirements
- Clause 03: Abbreviations and definitions
- Clause 04: Conformance to this International Standard
- Clause 05: Management of functional safety
- Clause 06: Safety lifecycle requirements
- Clause 07: Verification
- Clause 08: Process hazard and risk assessment
- Clause 09: Allocation of safety functions to protection layers
- Clause 10: SIS safety requirements specification (SRS)
- Clause 11: SIS design and engineering
- Clause 12: SIS application Program Development
- Clause 13: Factory acceptance testing (FAT)
- Clause 14: SIS installation and commissioning
- Clause 15: SIS safety validation
- Clause 16: SIS operations and maintenance
- Clause 17: SIS modification
- Clause 18: SIS decommissioning
- Clause 19: Information and documentation requirements

The lifecycle has 11 phases containing dedicated requirements/information and tasks to be performed which are organized in the above 19 clauses. Many of the requirements in the standard are technical in nature, but the lifecycle approach places equal importance on effective Functional safety management and management activities such as planning, documentation, operation, maintenance and modification for all phases as shown in Figure 82



NOTE 1: Stages 1 through 5 inclusive are defined in 5.2.6.1.3
NOTE 2: All references are to Part 1 unless otherwise noted

Figure 82, SIS safety lifecycle phases and FSA stages

7.4.1 Lifecycle phases overview

Phase 1 (Clause 8, Process hazard and risk assessment)
This is probably the most crucial phase in the lifecycle, because when the team fails to identify the hazard, then there will never be a safety function being required to reduce the potential

risk. Unfortunately, too many times people consider this as a formality and use tools that are not calibrated or trained on, resulting in wrong or failing risk definitions. Risk management contains three main tasks: 1. Identify the hazard, 2. Analyze the hazard & 3. Reduce the risk. A HRA (Hazard and Risk Analysis) team identifies the potential hazards using accepted methods, analyzes the consequences and frequencies, and when the frequency is higher than the tolerable criteria, there will be a need for a risk reduction - safety function achieving a certain SIL band performance or RRF (risk reduction factor).
New in Ed. 2.0 is that there SHALL be a Security risk assessment carried out on the SIS and the associated devices to identify the security vulnerabilities of the SIS, references of guidance are made to ISA TR84.00.09 and IEC62443-2.

Phase 2 (Clause 9, Allocation of safety functions to protection layers)
Once the safety functions are identified, each is assigned to protective layers. There are prevention layers and mitigations layers. The risk reduction allocated to a basic process control system that does not conform to IEC 61511 must be less than 10 and any layer must be independent and separate from the initiating source to avoid common cause, common mode and dependent failures. The safety functions allocated to the safety instrumented system (SIS) are called safety instrumented functions (SIF). The risk reduction is the safety integrity level (SIL) for each SIF or the average frequency of dangerous failure (PFD or PFH) to that SIF. See Table 33 (ref. IEC61511 Ed. 2.0 part 1).

SIL Safety Integrity Level	**PFDavg** Probability of dangerous failure on demand (demand mode of operation)	**PFH** Probability of dangerous failure per hour (high demand or continuous mode)	**RRF** Required Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	≤ 100000 to > 10000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$	≤ 10000 to > 1000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	≤ 1000 to > 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	≤ 100 to > 10

Table 33, Safety integrity requirements: PFDavg and PFH

Phase 3 (Clause 10, SIS safety requirements specification, SRS)
The objective of this phase is to specify the requirements for the SIS including any application programs and the architecture of the SIS. Many consider this document to be the primary document in the lifecycle. However, despite the fact that the IEC61511 Ed. 1.0 was released now for over 10 years, the experiences from international projects still prove that not many people/organization are capable of describing a SIF as summarized in IEC61511-1. (Therefore the detailed list below – reference IEC61511-1, 10.3.1)

The specification of the SIS safety requirements SHALL include:

- SIF description
- List of plant input and output devices
- Common cause failures requirements
- Definition of the safe state
- Assumed sources of demand on the SIF
- Proof test intervals and implementation requirements (e.g. proof test coverage)
- Response time within the process safety time
- Mode of operation (low, high or continuous) and SIL
- SIS process measurements, range and accuracy
- SIF process output actions
- Functional relation between process inputs and outputs
- Requirements for manual shutdown, resetting SIF
- Energize or de-energize to trip for each SIF
- Maximum allowable spurious trip rate
- Requirements for start-up or restarting the SIS
- Interfaces between SIS and any other system
- Application program safety requirements
- Bypass requirements and compensating measures
- Specification of any action necessary to achieve or maintain a safe state of the process in case of a fault detection
- Mean time to repair
- Identification of dangerous combinations of output states
- Environmental conditions likely to be encountered, EMC limits
- Survival requirements for any SIF by a major accidents event

The SIS application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS.
The requirements shall take into account the safety planning requirements and the safety manual of the chosen architecture such as limitations and constraints of the hardware and embedded software. There is of course a close relationship between the SIS hardware and the SIS application program requirements as shown in Figure 83 (ref. IEC61511 Ed. 2.0 part 1).

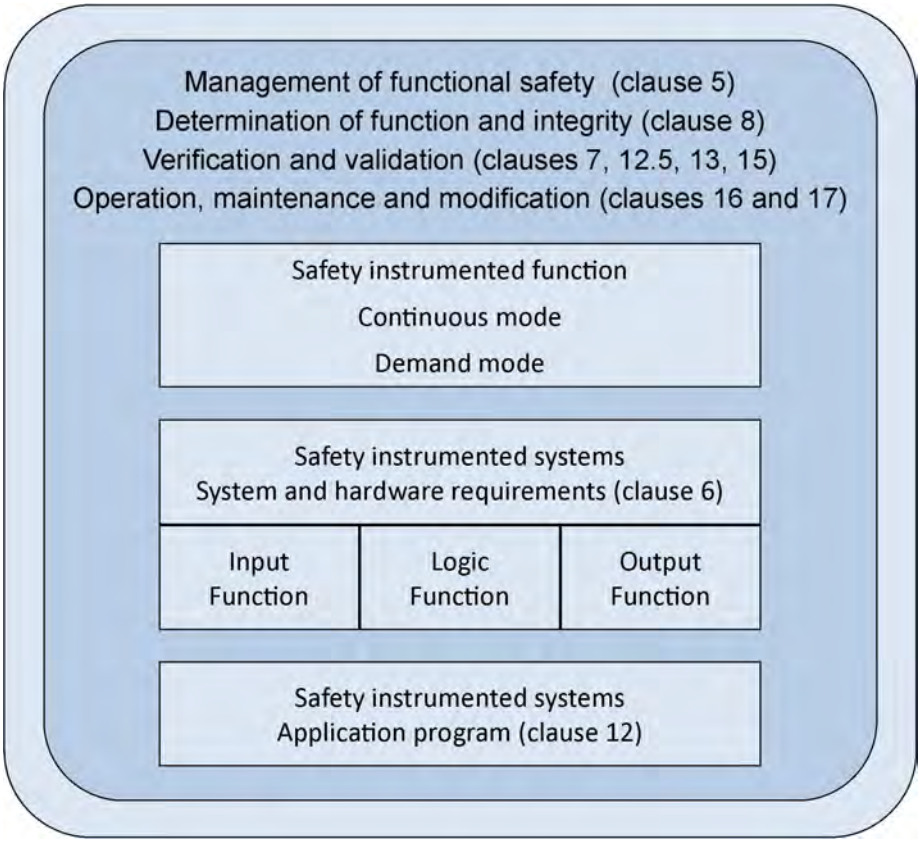


Figure 83, Relationship of system, SIS hardware and SIS application program

The SIS safety life cycle of the application program starts in phase 3 and ends in phase 10 with functional safety assessment. Each phase of the application program safety life cycle (see Figure 84) shall be defined in terms of its elementary activities, objectives, required input information and output results and verification requirements.

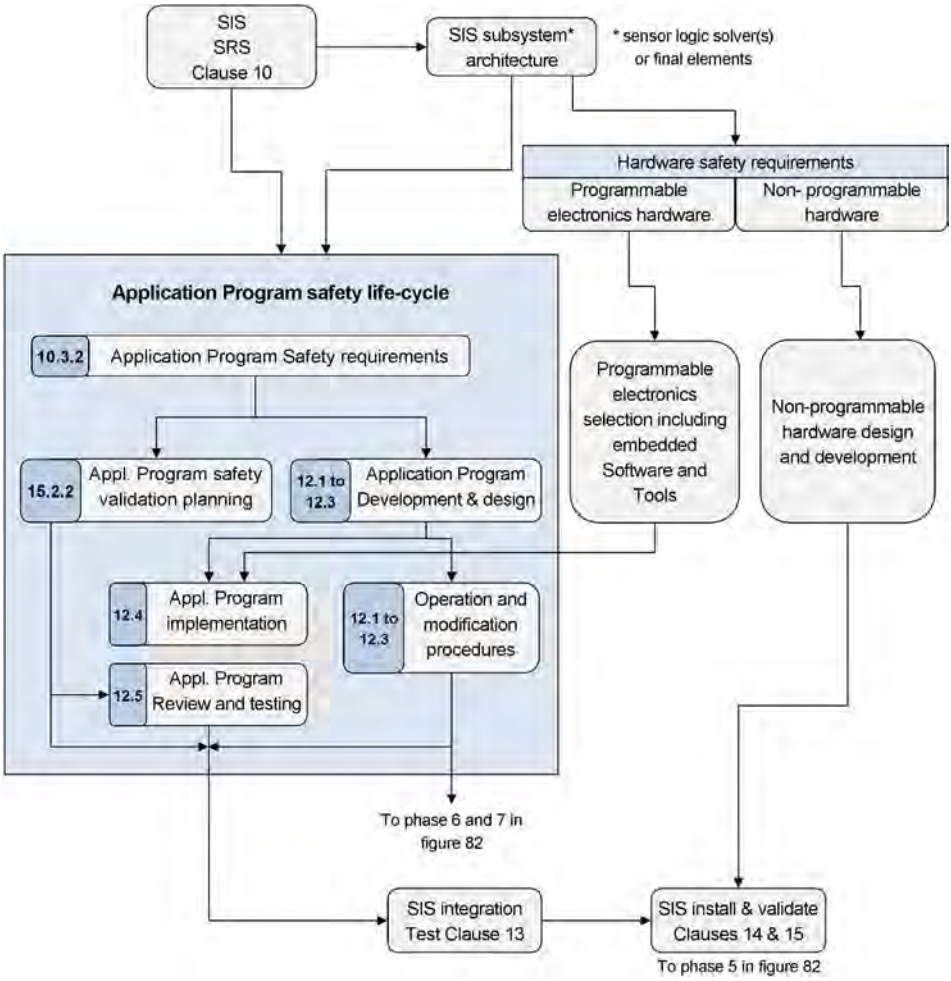


Figure 84, Application program safety life cycle and its relationship to the SIS safety life cycle (ref. IEC61511 Ed. 2.0 part 1)

Phase 4 (Clause 11, SIS design and engineering; Clause 12: SIS application Program Development)

Both clause 11 and 12 provides numerous requirements for the detailed design and engineering of the SIS, both hardware and application software requirements. Some of the important requirements are summarized below:

Clause 11, SIS design and engineering

When the BPCS/DCS (Basic Process Control System/Distributed Control System) is not qualified to the IEC61511, the safety instrumented system SHALL be designed to be SEPARATE

and INDEPENDENT from the BPCS/DCS to the extent that the safety integrity of the SIS is not compromised. Furthermore, the design of the safety instrumented system SHALL provide the necessary resilience against identified security risks.

Most probably the biggest change in Edition 2.0 is the removal of the safe failure fraction (SFF) in relation to the minimum hardware fault tolerance (HFT) requirements SHALL be in accordance to table 6 of the standard as shown in Table 34. However, the minimum required HFT could be reduced if it can be justified and documented that this would result in decreasing the overall process safety.

SIL	Minimum required HFT
1 (Any mode)	0
2 (low demand mode)	0
2 (high demand / continuous mode)	1
3 (Any mode)	1
4 (Any mode)	2

Table 34, Minimum HFT requirements according to SIL

These minimum HFT requirements are derived from route 2H of IEC61508-2. It should be noted that SIS subsystem designs might require more device redundancy than what is stated in Table 34 in order to satisfy process availability requirements (e.g., spurious failure frequency target).
Alternatively route 1H of IEC61508-2 based again on SFF for type A and B subsystems can be applied.

Devices selected for use as part of a SIS with a specified SIL SHALL be in accordance with IEC61508-2 and IEC61508-3, alternatively requirements exist for prior use devices suitable for use in the SIS. The evidence suitability for prior use must be documented and SHALL include things like but not limited to: device performance in similar environment, device dangerous systematic faults are sufficiently low, version of the device, etc. (reference 11.5.3 of IEC61511-1). Guidance on how to qualify field devices and collect data of the device can be found in ISATR84.00.04 and NAMUR recommendation NE130 (“Prior use”-devices for SISs”).
One has to say that prior use compliance on field devices including firmware such as measuring devices / transmitter will remain a challenge as firmware revision of such devices may vary throughout the plant and many end users cannot prove the revision numbers. But even when there is a firmware revision list, functionality differences remain difficult to trace and document.

Safety Manual for all devices used to design a safety instrumented system SHALL cover operation, maintenance, fault detection and constraints associated with the SIS describing the intended configuration and operating environment of that device.

New is the maintenance or testing design requirement for compensating measures to ensure continued safe operation during bypass (repair or testing). The maximum time the SIS is

allowed to be in bypass SHALL be defined.

Quantification of random failure SHALL take into account Proof test effectiveness (coverage), credibility of data used (documented) and data uncertainties. Failure rate date used when quantifying the effect of random failures SHALL be credible, traceable, documented and justified. The lack of reliability data reflective of the operating environment is a recurrent shortcoming of probabilistic calculations. End-users should organize relevant device reliability data collections in accordance with IEC60300-3-2 or ISO14224 to improve the implementation of the IEC61511 standard.

Clause 12, SIS application Program Development

Requirements for application software of IEC61511 edition 1.0 have been completely re written under application program development requirements in edition 2.0. The application program of the safety instrumented system SHALL be in accordance to the SRS from phase 3 – clause 10 up to and including SIL3.

The application program SHALL allow a functional safety assessment to be carried out. Furthermore, there are new requirements for verification (review and testing) by a competent person NOT involved in the original program development.

Application program development SHALL comply with the constraints in the applicable safety manual(s)

The use of V-model life cycle for the development of an application program starting from the SIS safety requirements to the final testing as SIS safety validation (by FAT or SAT) is highly recommended since it is able to minimize potential systematic failures that can cause malfunction of the program. A similar V-model was available in IEC61511-part 1 Ed. 1.0, but has been revised and moved into IEC61511-part 2 in Ed. 2.0. See Figure 85 below .

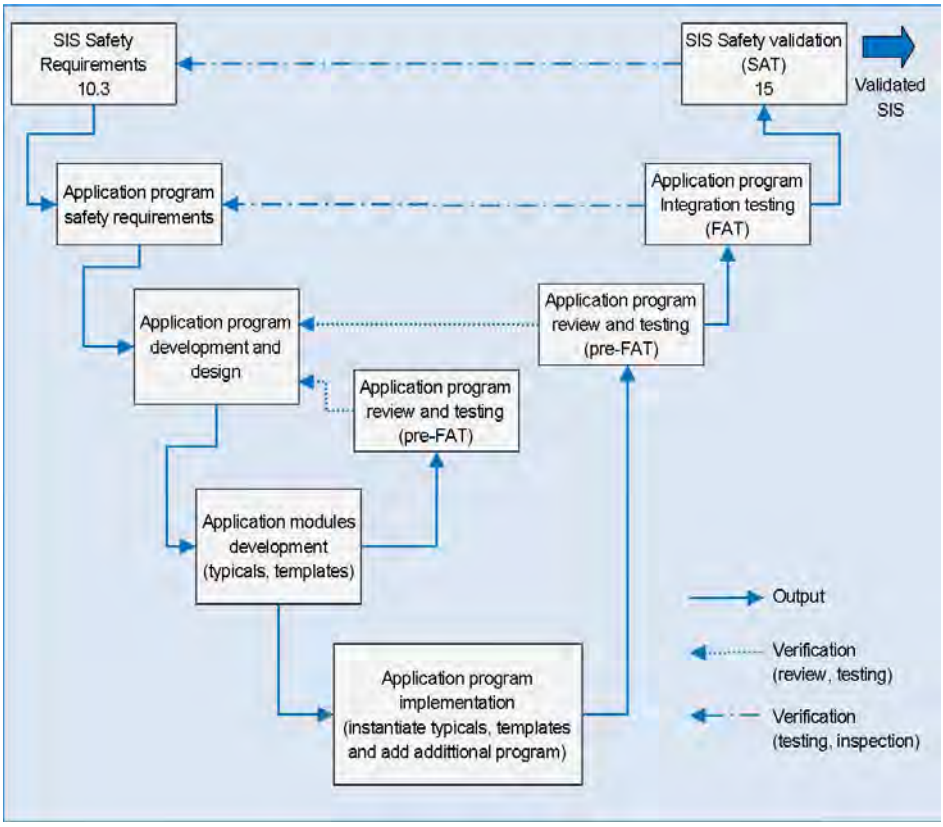


Figure 85, Application program V-Model

Phase 5 (Clause 14, SIS installation and commissioning; Clause 15, safety validation)

Note:
Clause 13, describing Factory Acceptance Testing (FAT) was in IEC61511 – part 1, edition 1.0 the only 'INFORMATIVE' clause inside part 1 as all other clauses were 'NORMATIVE'. Although edition 2.0 made this clause 13 now also NORMATIVE as the rest of the clauses in the part 1 of the standard, it is not referred to in the figure 2 - SIS safety lifecycle phases and FSA stages. This special note is purely based on the author personal opinion for the moment that this FAT clause 13 could be listed under phase 5 of the SIS life cycle model.

The objective of a factory acceptance test (FAT) is to test the devices including the application program of the SIS to ensure that the requirements defined in the SRS are met. The need for a FAT SHALL be specified during the safety planning and has a list of prescriptive requirements in the standard. The FAT requires also competent test personnel and preferably the people who will operate the process since this will give them some early training on the operation of their SIS.

Clause 14: SIS installation and commissioning

The installation of the SIS should be done as per design and installation plan. Any deviation should be properly reviewed with the project team to ensure all of the design requirements are still satisfied. Many vendors provide checklists or installation recommendations to help the end user minimizing potential installation failures.
Once the SIS has been properly installed, it should be fully commissioned and validation activities should be initiated.

Installation and commissioning planning SHALL define all activities required including:

- Procedures, measures and techniques to be used
- When and how this work will be done
- Responsibilities of persons, departments and organization involved in this activity

All must be recorded and documented.

Clause 15: SIS safety validation

Validation is to demonstrate that the SIS achieves the requirements as described in the SRS and needs to be completed prior to placing the SIS into operation. A full validation could be referred to as Site Acceptance Test (SAT), whereas a partial validation at the manufacture's site or system integrator could be referred to as FAT.

Validation planning of the SIS SHALL be carried out throughout the SIS lifecycle and SHALL define all activities and equipment required for validation. The standard describes a list of requirements to fulfil, wherein the need for levels of independencies of people, department and organization involved are required.

Validation planning of the application program as an integrated test SHALL fulfil a list of requirements from the standard and be documented.

After the SIS validation and before the hazards are introduced in the process, the following activities SHALL be carried out:

- All bypass functions shall be returned to their normal position
- All process isolation valves shall be set in the correct position according the start-up requirements and procedures
- All test material shall be removed
- All commissioning overrides and force permissives shall be removed

Phase 6 (Clause 16, Operation and Maintenance)

The objective of this phase is:

- To ensure that the required SIL of each SIF is maintained during operation & maintenance
- To operate and maintain the SIS so that the designed functional safety is maintained at all times.

Operation and maintenance planning SHALL be carried out with a document that describes routine and abnormal activities, proof testing, preventive maintenance, maintenance after failure, techniques to be used for operation and maintenance, verification of adherence to operations and maintenance procedures, when these operations and maintenance activities shall take place and the persons, departments and organizations responsible for these activities.

Procedure SHALL be made available, additional requirements in edition 2.0 are for proof testing efficiency and consistency, for data collections, for compensating measures during bypass (repair & testing). Particular focus is on the procedure for proof testing and inspection and the documentation records of those activities, which are absolutely necessary for functional safety assessments or audits.

Operator and maintenance personnel SHALL be trained to sustain full functional performance of the SIS both hardware and software to meet the target SIL of the SIF.

Phase 7 (Clause 17, Modification)

This clause objective is:

- To ensure that modifications of any SIS are properly planned, reviewed, approved and documented before making the change.
- Guarantee that the functional safety and required safety integrity of the SIS are maintained despite the changes being made to that SIS

Prior to carrying out any modification to a SIS, a procedure for authorizing and controlling SHALL be in place, containing things like, but not limited to:

- Impact analysis of the required modification
- Safety planning for the modification, re-verification, and re-documentation

New in edition 2.0 is that modification activity SHALL not begin until a functional safety assessment (FSA) is completed, the following information SHALL be available:

- Detailed description of the modification
- The reason for the change
- Identified hazards and safety instrumented system potentially affected
- Impact analysis of the modification
- The approval required before the modification starts
- Re test details and records
- Appropriate configuration history & log book

All modifications SHALL be performed by competent, qualified and trained personnel.

Phase 8 (Clause 18, Decommissioning)

This clause's requirements are similar to ones of clause 17 (modifications):
Procedure, analysis and authorization.
To ensure that the required SIF(s) remain operational during decommissioning activities.
A typical example would be during an upgrade of a SIS, parts or all SIF(s) may be decommissioned when upgrade is required.
Same as with the modification, also here decommissioning activities SHALL not begin without proper documentation and authorization.

Phase 9 (Clause 7, verification; Clause 12.5 requirement for application program verification (review and testing))

Clause 7

The objective of this clause is to demonstrate by review, analysis and/or testing that the required outputs of that activity or phase fulfil the defined requirements for the appropriate phases (Figure 2). Verification SHALL be planned and documented so it can be later used for the functional safety assessment, see Figure 86 below.

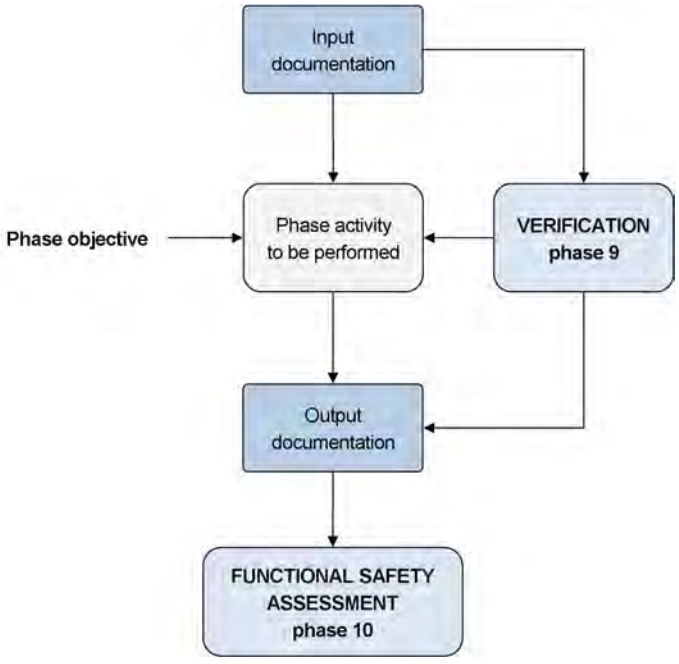


Figure 86, Relation between Verification and Assessment

Basically no matter which phase of the life-cylce you are active/responsible for, every single

phase, before moving to the next phase must be verified. This is one of the key principles of functional safety.

Clatuse 12.5

A competent person not involved in the original development SHALL review the application program including its documentation. The approach used for the review and the review results SHALL be documented

Phase 10 (Clause 5, Management of functional safety)

Besides verification, there is management of functional safety including assessments and audits the remaining keystones to achieve functional safety. Management of functional safety is the 'non-technical' or 'management' requirement from the standard that is unfortunately disliked by many users / engineers because of the documentation requirements and duties.

The objective for functional safety management is to document, monitor and assess requirements for implementing management activities that are necessary to ensure that the functional safety objectives are met by those responsible. Functional safety management SHALL be planned. The plan or procedure may be in conjunction with organization's quality management system. New in edition 2.0 is that 'Everyone' claiming Functional Safety compliance SHALL have a functional safety management system in place.

Besides responsibilities, every person, departments or organizations involved in SIS safety lifecycle activities SHALL be competent to carry out the activities for which they are accountable. New in edition 2.0 is that there SHALL be a procedure in place to manage competence of all those involved in the SIS life cycle + periodic assessment SHALL be carried out documenting the competence of individuals against the activities they are performing and on change of an individual within a role.

Functional safety assessment (FSA) team SHALL include at least 1 senior competent person not involved in the project design team for stages 1-2-3 or not involved in the operation and maintenance of the SIS for stages 4 & 5:

- Stage 1 - After the hazard and risk assessment has been carried out, the required protection layers have been identified and the SRS has been developed.
- Stage 2 - After the SIS has been designed.
- Stage 3 - After the installation, pre-commissioning and final validation of the SIS has been completed and operation and maintenance procedures have been developed. (this is sometimes called Pre-Startup-Safety-Review PSSR)
- Stage 4 - After gaining experience in operating and maintenance.
- Stage 5 - After modification and prior to decommissioning of a SIS.

(These 5 stages are shown in Figure 82).

Besides those stages and new in the edition 2.0 is that functional safety assessments SHALL

be carried out periodically during the operations and maintenance phase (typically one of the longest phases in duration) to ensure that everything is still being carried out according to the assumptions made during design and that the requirements within IEC61511 for safety management and verification are still being met. This assessment is typically called a functional safety audit.

New in edition 2.0 is that functional safety audits SHALL be performed by an independent person not undertaking work on the SIS and procedures SHALL be defined and executed for auditing compliance with the requirements.

Phase 11 (Clause 6.2, Safety lifecycle structure and planning)

A SIS safety lifecycle incorporating the requirements of the IEC61511 SHALL be defined during the safety planning. New in edition 2.0 is that it also addresses the application programming now.

The safety lifecycle requirements including an objective and detailed description of each phase activity, the inputs needed for the phase and the output generated by the phase. Each phase SHALL be verified and documented as per the requirements of the standard.

A graphical explanation of the phases is shown in Figure 82.

7.4.2 The remaining clauses not directly referenced in the lifecycle phases

Clause 1, Scope

Defines the requirements of the specification, design, installation, operation and maintenance of a safety instrumented system (SIS) so that it can be confidently entrusted to achieve or maintain a safe state of the process. The IEC61511 has been developed as an application specific standard for the process sector implementation of the IEC61508. See Figure 87 for a relationship between IEC61511 and IEC61508.

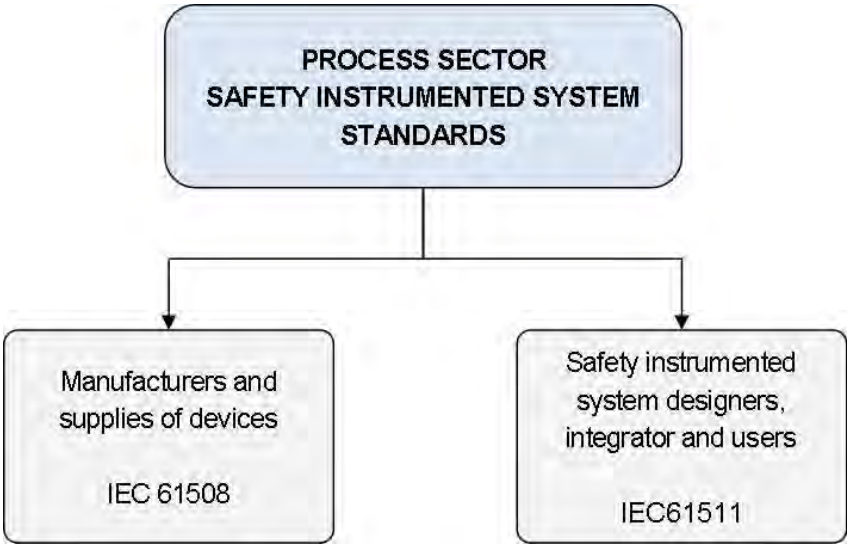


Figure 87, Relationship between IEC61511 and IEC61508

IEC61508 is also often used by safety instrumented designers, integrators and users where directed in IEC61511.

Clause 2, Normative references

The following referenced documents are indispensable for the application of the IEC61511:

- IEC61508 part 2 (hardware) and part 3 (software)
- IEC TS 6100-1-2 Ed. 2.0 (technical specification EMC)
- IEC 62682 Ed.1 (Alarm management in the Process Industry)

Clause 3, Abbreviations and definitions

This clause contains abbreviations and definitions and is quite comprehensive with approximately 20 pages of definitions

Clause 4, Conformance to this International Standard

Declares that compliance with IEC61511 requires demonstration that each of the requirements outlined in clauses 5 through 19 has been satisfied and therefore the clauses objectives have been met.

7.5 Executive summary of the edition 2.0 changes

The new edition 2.0 will be more aligned with the definitions of the IEC61508 and aimed to eliminating some inconsistencies, but one of the biggest changes to the standard is the definition of the word 'should' used in edition 1.0, is becoming in many clauses of the edition 2.0 standard more prescriptive 'shall', meaning that many definitions will gain more strength in the standard and become more restrictive than before.

Below is a summary of the 61511 – 1 edition 2.0 changes, however previous knowledge and competency in the IEC61511 Ed. 1.0 will be necessary to understand the brief descriptions per clause of the standard from part 1

Clause 1: Scope

- 'Application software' is now called 'Application program'
- The 'demand – mode' is now being split into 'Low' and 'High' demand modes to be inline with the IEC61508 Ed. 2.0.

Clause 2: Normative references

- Compatibility (EMC) and IEC 62682 Ed 1.0 ALARM management are both new indispensable referenced documents

Clause 3: Abbreviations and definitions

There are new abbreviations:

- Bypass, compensating measures, conservative approach, field device, failure mode, fault exclusion, harmful & hazardous event, hazardous situation, instrumented system, Mean Repair Time (MRT), Mean Time To Restoration (MTTR), Mean Permitted Repair Time (MPRT), mode of operation (of a SIF): Low demand mode & High demand mode, module, operating environment, operating mode (process), performance, process risk, process safety time, SIS subsystem, systematic capability

There are definitions completely re-written or that have more notes:

- Common Cause failure, common mode failures, dangerous failure, detected-revealed-overt, prior use, random hardware failure, safe failure, safety manual (functional), software, full variability language (FVL), systematic failure

There are definitions deleted:

- Electrical/electronic/programmable (E/E/PE), external risk reduction facilities, Independent department, proven in use, safe failure fraction, template (software)

Clause 4: Conformance to this International Standard

- Nothing changed from Ed. 1.0

Clause 5: Functional Safety management

- A procedure SHALL be in place to manage competence of all those involved in the SIS life cycle + periodic assessment SHALL be carried out.
- Everyone claiming Functional Safety compliance SHALL have a functional safety management system in place.
- The emphasis on planning the Functional Safety Assessment (FSA) is stronger in Ed 2.0 as all notes from Ed. 1.0 became a SHALL requirement now
- Functional safety assessment is depending on time in operation now
- Functional safety assessment SHALL be carried out prior to the hazards being introduced
- Functional safety assessment SHALL be carried out during the maintenance and operation life cycle phase.
- Functional safety assessment SHALL consider the impact analysis during the MOC
- Functional safety audit SHALL be performed by an independent person not undertaken work on the SIS.
- The SIS software, hardware and procedures used to develop and execute the application program shall be subject to configuration management and shall be maintained under revision control.

Clause 6: Safety lifecycle requirements

- Application program SIS safety life cycle requirements.

Clause 7: Verification

- Additional descriptive requirements for testing are added

Clause 8: Process hazard and risk assessment

- Security risk assessment SHALL be carried out (guidance in ISA TR84.00.09 and IEC62443-2)

Clause 9: Allocation of safety functions to protection layers

- When risk reduction requirement is greater than 10,000 and is considering multiple protection layers, then further analysis is needed for independency between those layers, common cause of failure of SIS and the cause of the demand, common cause of failure with other layers, dependencies from common operations, maintenance, inspection or test activities
- Single BPCS protection layers ≤ 10, no more than one BPCS layer when BPCS is the initiating demand source on that layer. No more than two BPCS layers SHALL be claimed when the BPCS is not the initiating source of the demand.
- Each layer SHALL be independent and separate from the initiating source

Clause 10: SIS safety requirements specification (SRS)

- Application program safety requirements (this used to be called the software SRS in Ed. 1.0 but has been rewritten in Ed. 2.0)
- SIS architecture requirements
- Process safety time. This is a new requirement (is also in IEC61508 Ed. 2.0)
- Proof test implementation requirements

Clause 11: SIS design and engineering

- Safety manual for all devices, covering operations, maintenance, fault detection and constraint associated with the SIS
- Design resilience to identify security risks
- Communication by safety protocol or other appropriate techniques
- Hardware fault tolerance (HFT) simplified by eliminating SFF from Ed 1.0 and is following Route 2H from IEC61508 Ed. 2.0, alternatively Route 1H from IEC61508 Ed. 2.0 can be used which is based on type A & B and SFF again.
- Systematic capability requirements for certified devices SHALL be in accordance with IEC61508-2 and IEC61508-3
- All devices selected on the basis of prior use SHALL be indentified by a specified revision number and SHALL be under the control of a management of change procedure.
- Maximum time the SIS is allowed to be in bypass SHALL be defined and compensating measures that ensure safe operation SHALL be provided during bypass
- Quantification of random failure SHALL take into account Proof test effectiveness (coverage), credibility of data used (documented) and data uncertainties

Clause 12: SIS application Program Development

- Besides the clause 12 - title that has changed from application software into application program development, there was also a major re-write from the application program requirements. Ed. 1.0 - 17 pages has been reduced to 5 pages in Ed. 2.0
- The requirements for SIS application development are part of the clause 10-SRS now
- Application program design SHALL allow by prescriptive requirements details an functional safety assessment during the program design phase
- Application program implementation requirements are also newly described
- Application program requirements verification (review and testing) by a competent person NOT involved in the original development
- Application program methodology and tools SHALL comply with the safety manual(s)

Clause 13: Factory acceptance testing (FAT)

- FAT has become NORMATIVE in Ed. 2.0 was informative in Ed. 1.0
- The FAT planning SHALL specify a list of prescriptive requirements

Clause 14: SIS installation and commissioning

- Nothing changed from Ed. 1.0

Clause 15: SIS safety validation

- Minor re-write of some recommended requirements for planning, testing and assessment

Clause 16: SIS operations and maintenance

- Bypass SHALL only be permitted when there are compensating measures providing adequate risk reduction
- Operating procedures SHALL be developed to define the compensating measures necessary to ensure functional safety during bypass or disabling the SIS including the maximum time allowed
- Status and duration of all bypasses SHALL be recorded in a bypass log
- Procedures for data collection
- Procedures for the quality (coverage) and consistency of proof testing

Clause 17: SIS modification

- Modification SHALL not begin before FS assessment is completed as part of the MOC

Clause 18: SIS decommissioning

- Nothing changed from Ed. 1.0

Clause 19: Information and documentation requirements

- Nothing changed from Ed. 1.0

7.6 References

- CCPS – Guidelines for Safe and Reliable Instrumented Protective Systems (2007)
- IEC – IEC61508 Ed. 2.0 Functional Safety of electrical/electronic/programmable electronic safety-related systems, parts 1-7 (2010)
- IEC – IEC61511 Ed. 1.0 Functional Safety: Safety Instrumented Systems for the Process Industry sector, parts 1-3 (2003)
- IEC – IEC61511 Ed. 2.0 Functional Safety: Safety Instrumented Systems for the Process Industry sector, parts 1-3 – (CDV version 65A/691/CDV – 2014)
- Norwegian University of Science and Technology NTNU 2012 - Changes /What is it with IEC61511?, Mary Ann Lundteigen
- TÜV Rheinland International Symposium 2012 – IEC61511-1 Ed. 2, Initial Reflections on an Evolving Standard, Dirk Hablawetz – BASF SE
- TÜV Rheinland International Symposium 2014 – IEC61511-1 Ed. 2, When and what, Heidi Fuglum and Cato Bratt – ABB Norway

Chapter 8 IEC61511 Ed. 2.0 - SIS Safety Requirement Specification (SRS)

Important Note:
This chapter presents a general overview of the SIS Safety Requirement Specification (SRS) - Normative Part 1: Framework, definitions, system, hardware and application programming requirements", edition 2.0. This is based on the FDIS version (65A-61511-1-Ed2-IS-FDIS-OE, 2015-06-17, FDIS=Final Draft International Standard). At the time of editing this chapter the forecasted publication date of IEC61511 Ed. 2.0 – part1 is for 2016-02. Please note that there may be additional or different changes to the final published version of the IEC 61511 Ed 2.0.

8.1 Introduction

In 2003 the Health and Safety Executive (HSE) from the UK released the 2nd edition of a study called 'Out of control: Why control systems go wrong and how to prevent failure?'. This was based on 34 international incidents, concluding that 44% of the causes were related to specification issues. It is clear that when it comes to safety specification, there should be no assumptions on how to build, operate or maintain it.

Despite having the IEC61511 Edition 1.0 out since 2004, observations from a Functional Safety Competency Trainer point of view, it is clear that the majority of the participants know what the purpose of a SRS should be, unfortunately the only thing most people have in common is the title of the document "Safety Requirements Specifications or simply SRS".
There is plenty of evidence that in general the Process Industry is struggling to meet the SIS safety requirements (10.3 - IEC61511-1). One has to say that, although the content of the SRS is explained in a bullet list, there is very little guidance of how to implement those, therefore many projects are left with a serious gap on 'what should have been described' versus 'what cut/copy paste' many engineer manage to reproduce again.

The 61511 Ed. 2.0 part 1 has again a normative requirement to develop a SIS Safety Requirements Specification (Phase 3, clause 10) with some additional (new) requirements compared to edition 1.0 in clause 10 as one of the more important activities of the safety life cycle. The SRS requirements should address the basic and functional design specifications and should be prepared before starting design, installation and operation. The aim is to have every single Safety Instrumented Function (SIF or safety loop) described in such a way that anyone wherever and whenever need to understand the SIF; or build-, maintain-, operate-, repair- and test- that SIF; will have a precise, clear, verifiable, maintainable and feasible information available.

8.2 Content of the SRS

The SIS SRS may be a single document or a collection of several documents including procedures, drawings and corporate standard practices. The SRS should be the master document. Referenced documents are subordinate to the SRS. Of course 1 single SRS document is easier to maintain and control, multiple and various documents all linked together can lead to more human – failures (systematic) failures, and this is exactly what a good engineering practice standard like the IEC61511 is trying to avoid. However, all is depending on the owner organization practices and standards.

The SIS SRS will be a key document that should be generated in Phase 3 (clause 10, Safety requirements specification for the safety instrumented system) and preferably be finished (although reality it never is) before starting at Phase 4 (clause 11, SIS design and engineering & clause 12, SIS application program development).
There is also a recommendation from the IEC61511 standard to perform a Functional Safety Assessment (FSA) known as 'stage 1' in the lifecycle assessment by an independent senior competent person(s), in order to determine that the SRS document meets the functional safety objectives.
These requirements may be developed by the Hazard and Risk Assessment (HRA) team and/or the project team itself. Final validation of the SIS is carried out using this SRS document. However, the SRS will need to be maintained and be available for those that need it for the duration of a complete lifecycle of any project. It is not just valuable for the design phase only, the SRS will remain a key document for the successful operation and maintenance of the SIS system.

Inputs to the SRS are coming from the preceding life cycle phases:

- Phase 1 (clause 8, Process hazard and risk assessment)
- The hazard description
- The frequency of occurrence
- The consequence
- Phase 2 (clause 9, Allocation of safety functions to existing protection layers)
- This is typically done by Layer Of Protection Analysis (LOPA)

When the tolerable risk cannot be met, then additional protection layers will need to be specified in the SRS for the SIS:

- Specifies requirements for system architecture, hardware configuration, application program and system integration
- Specifies techniques and numerical targets (SIL levels) to measure the performance of the SIS

Typical content of a SRS may contain things like:

- General Functional SIS Requirements that all SIFs have in common within the SIS, e.g. user interface for the operator/maintenance personnel, etc.;
- Specific SIF Safety Functional Requirements, HOW it should work;

- Specific SIF Safety Integrity Requirements, HOW well it should work;
- Specific SIF Safety Integrity Requirements, HOW well it should work and HOW long it should work for;
- Application Program Safety Requirements
- Non-Functional SIS requirements, such as code and standard, application specific standards, environmental conditions, client-plant-project specific guidelines, etc.

8.2.1 General Requirements (61511-1, clause 10.2)

There is no such thing as one 'generic' SRS that can be used for everyone and every application in the process industry. The SRS will need to be customized to the client or plant/ project specific guidelines and specifications.

However, there are some general requirements that could be applicable for all, below are some examples given:

- What type of process application (continuous or batch)?
- What type of general hazards and their potential to harm people, environment and capital investment?
- What process or facilities are in the neighborhood?
- Which environmental conditions can influence the SIS equipment?
- Which standards, codes and local legislation are applicable?
- What type of utility supplies, e.g. net power, uninterrupted power supply (ups), diesel generated power, instrument air compressor, etc.?
- What is the required Plant Life Time for the SIF?

8.2.2 SIS Safety Requirements (61511-1, clause 10.3)

Similar as the previous edition of the 61511 part 1, clause 10.3 contains in total 29 requirements as an itemized list. Those requirements **SHALL** be sufficient to design the SIS and **SHALL** include the below description of the intent and approach applied during the development of the SIS safety requirements as applicable. The word **SHALL** make those individual requirements **mandatory** to consider for every project providing you claim compliance to the IEC 61511 standard.
Below are some potential example(s) based upon personal interpretation and experiences of such requirements

8.2.2.1 A description of all the Safety Instrumented Function necessary to achieve the required functional safety

Following the demand on the Safety Instrumented Function (SIF), a detailed description of the actions that are designed to interface with that SIF to prevent the hazardous condition. Sometimes the SIF can be referred to as the IPF (Instrumented Protective Function) list of all Safety Instrumented Function (SIF), Equipment Protective Functions (EPF) and Manual Protective Functions (MPF).

Example:

- Low level (LAL-103) in a LNG tank 100A causes the suction pump (P-101) to trip;
- LAHH-201 shall protect the LP Gas system from Hi Hi level of LP Gas Scrubber by closing ESDV-203;
- High-high storage tank level (LAHH-901) closes tank inlet valve SDV-904;
- High reactor temperature (TAH-506) closes the two reactor feed valves XV-501A and XV-501B;
- High column temperature (TAH-333) closes the re-boiler steam valve XV-301.

Describe the following:

- Process variables being measured and which devices used (typically a tag name);
- Process conditions under which SIF need to act (trip point or alarm);
- Logic of the SIF that needs to be executed;
- Final element or action that the SIF will result in (actuator(s), safe state, tag name).

8.2.2.2 A list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification

This is typically done by a field I/O or tag list, but in relation to 'how' the SIF functionality is built or connected to those tag names, a detailed SIF or a safety loop description supported by a loop diagram is recommended.
Every single SIF can contain several devices or subsystems as the IEC61508 defines them.

Example of a simple 1oo1 SIF graphical represented in Figure 88.

Figure 88, Example of a simple 1oo1 SIF

8.2.2.3 Requirements to identify and take account of common cause failures

The potential common causes that could affect fault tolerant / redundant architectures need to be identified. The definition for common cause failure (CCF) in the standard is Beta Factor (β) and is expressed in percent (%). This needs to be defined by the design engineers and will depend of course on what type of redundant channels, devices or instruments are being used.

The Beta Factor is used for the reliability calculation of the SIF and needs to be clearly identified as this will influence the Probability of dangerous Failures on Demand (PFD) result. Commonly found in the industry are numbers in the range from 2% to 10-15%, all depends on how conservative you will be when estimating potential common cause failures. Special attention needs to be given to those SIFs who are at the SIL performance boundaries because a 2% versus a 15% Beta Factor may well mean decreasing one SIL band. Some companies have guidelines based on the IEC61508-6, annex D, example:

- 5% between identical devices from the same manufacturer used in a redundant configuration;
- 2% between diverse devices from different manufactures used in a redundant configuration.

Beware that common cause failure is often confused with common mode failures or systematic design failures. Using two pressure transmitters on the same measurement line is not a common cause when that tap gets blocked or isolated, but a systematic design failure. Or when you lose instrument air supply and multiple valves are closing, this is not common cause failure but a common mode failure (CMF).

8.2.2.4 A definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated

This specification should define the safe state of the process for each identified function in terms of which flows should be started or stopped, which process valves should be opened or closed and the state of operation of any rotating equipment (pumps, compressors, agitators). If bringing the process to a safe state involves sequencing, the sequencing should also be identified. When defining the final elements, consideration should be given to the benefits of diversity, for example, shutting off the product stream and shutting off the steam flow to reduce high pressure.

Beware that the ‘safe state’ of the process for one SIF may not be the safe state of the overall process. Sometimes confusing as the subsystem or instrument may also have a safe state definition that has nothing to do with the overall safe state of the process, example:

- Safe state of a process could be closing the gas valve to a furnace;
- Safe state of an interposing relay with a normally open contact used in a de-energized to trip function, will be calling an open contact the safe state.

8.2.2.5 A definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system)

This specification defines the potential new hazards that may be the result of several simultaneous safe states of the process units. Assume that you lose instrument air and had no buffer capacity or the backup compressor does not takeover to keep the process running, many different SIFs may get activated spuriously, or go to the safe state, leading maybe to a massive load for the flair header to handle that could go beyond the flair mitigation system capacity. Although some of the process units went to a safe state, a new potential hazard may occur because of that.

8.2.2.6 The assumed sources of demand and demand rate on each SIF

During the risk assessment phase, there is an estimation made on how often the SIF will be activated / demanded or needed. This is based on assumptions made starting from the initiating event to the target tolerable / acceptable frequency. This is of course depending on the potential initiating event likelihood and the correct functioning of your SIF function. If you have a SIF demand rate that was estimated to be activated 1 in every 100 years, but is demanded 2 times a year during operations, then it needs to be investigated what the reason is for that higher demand rate.

Example:

- Maybe the process conditions have changed, operators do not follow the procedures which were used during the assumptions being made in the risk assessment;
- The device reliability under your operation conditions does not reflect the failure rate (PFDavg) that was estimated during the reliability analysis;
- etc.

If, however, the increased demand rate is higher than initial assumption and justified to be correct, then you will need to re-assess the risk and take appropriate actions to redesign the SIF in order to achieve the tolerable frequency.

Demand rate should be monitored during the lifecycle of the SIF, that is also why the Functional Safety Management in the IEC 61511-1 (5.2.5.2) states: Procedures shall be implemented to evaluate the performance of the SIS against this definition to compare the demand rate on the SIF during actual operation with the assumptions being made during risk assessment when the SIL requirements were determined.

8.2.2.7 Requirements relating to proof test intervals

The proof test interval is usually determined at the beginning of the SIS design in order to achieve a minimum RRF or PFDavg for the SIF. The SIF design shall allow for testing of the

SIF either end-to-end (from process fluid at sensor to process fluid at actuation end) or in segments (from process fluid at sensor to for example the analog input (AI) from a safety plc).

Proof test interval should consider things like:

- test duration;
- state of the tested device (off-line/on-line);
- state of the process during test;
- detection of common cause failures;
- prevention of errors (such as the SIS remains isolated after test complete);
- test documentation requirements;
- archiving requirements;
- the need to ensure management is aware of what is planned;
- the need to ensure adjacent and other impacted areas are aware of the impending test;
- the technical qualification and experience of the person(s) developing the test procedures;
- the technical qualification and experience of the person(s) implementing the test procedures.

Beware that the proof test interval is a defined period on 'how frequent you will need to test' that SIF in able to maintain the SIL performance and consequently the RRF. The proof test interval needs to be realistic and achievable by the end-user, so the design of the process and process operations will need to allow the proof test to be performed as required to maintain that SIL performance and RRF. When the defined proof test interval cannot be achieved, then the consequence is that the SIF is no longer performing as estimated and the expected risk reduction factor is degrading in function of time. Besides the proof test interval, there is something equally, if not more important, called proof test coverage that you should be considered (see below 8.2.2.8).

8.2.2.8 Requirements relating to proof test implementation

In the beginning of the functional safety standards, many people considered that the proof test interval or frequency was sufficient to achieve or maintain SIL performance on the SIF. However, that was based on the assumption that:

- the test interval frequencies are being applied;
- the test quality will return the device in a to be good as new state or at least functioning 100% correctly;
- the proof test of the SIF functionality is under the same process conditions as the SIF will have to prevent the potential hazard.

The proof test procedure and the reliability analysis of the proof test facilities should include for example:

- the estimated durations of the physical proof tests, because for example when executing a proof test of a redundant architecture under process condition, the SIF will be less (safety) available than originally designed but that depends yet again on the design

architecture;

- the state of the process (running or stopped) during proof tests execution, many facilities nowadays have planned shutdown let's say every 5 years. When the plant was designed before consideration for on-line testing, then there will be no other possibilities than to test only every 5 years. But when the plant or process unit is in a planned shutdown, then the process conditions available during that time may not reflect the ideal (real) proof test conditions and that should be described;
- the state of the tested device during the proof tests (on line or off line). If the tested device is off line (i.e. unavailable) during proof tests this may be an important contributor to its PFDavg, testing a high pressure valve on a test bench with low pressure or instrument air may not be reflecting the potential failure that you should be able to reveal under critical process or on-line test conditions;
- the proof test coverage description to explain what exactly needs to be tested in order to claim 50-75-90% coverage. In other words, the proof test coverage of 100% is very idealistic and most likely not possible in reality for the whole SIF. Typical ranges found in the industry vary between 40-90% best case. The below picture (Figure 89), is based on a simulation of 70% proof test coverage (Et) or effectiveness, even when you keep the proof test interval (frequency) at exactly 12 months (TI), because you are only achieving 70% proof test coverage, you are moving from a SIL 2 performance in a SIL 1 performance band after 4 test frequencies (4 years) in this example. Sure that even though you maintain the yearly proof test interval the SIL performance 'predictively' will degrade in time and you will end up after a certain time with no SIL achievement at all;

The following graph shows an example of PFD and PFDavg variations in case T-proof test is carried out once a year with 70% effectiveness: SIL 2 level is maintained only for about 4 years; the SIF then downgrades to SIL 1.

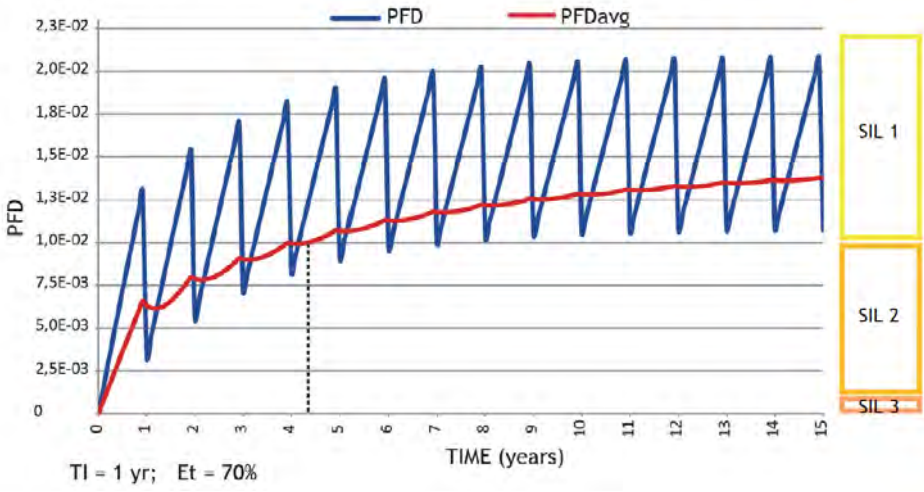


Figure 89, Example of PFD and PFDavg variation in case T-proof test is carried out once a year with 70% effectiveness

- the failure which may be caused by the proof tests themselves, (e.g., failure due to the change of state needed for testing purpose), completely irrelevant to the process industry but an easy to understand example is an airbag in a car. If you would want to test the airbag, you can only do (use) it once;
- the possible staggering of the proof tests for similar redundant devices in order to de-correlate the proof tests, when having identical redundant devices in a SIF, testing policy in overlapping time periods may be considered;
- The possibility for the proof test to return an incorrect result about the health of the SIS, example:
  - proof test affected by a fault associated with the proof test itself;
  - the human error during proof tests (e.g., no detection of an actual failure, omission of a test, proof tested or repaired device remaining off line after proof test or repair completion, or etc.).

Proof test is sometimes referred to as T-proof -, functional -, or function - test.
Since the proof test efficiency is so dominant in the future for retaining the SIF in an acceptable – assumed performance band, manufacturers (E.g. GM International) are providing a Safety Manual, sometimes called Functional Safety Manual, where the information is given on how much proof test coverage (%) or efficiency you can achieve performing specific tests and document the results of that test.
Below is a functional description of a SIL 3 Repeater Power Supply HART from GM International (Figure 90).

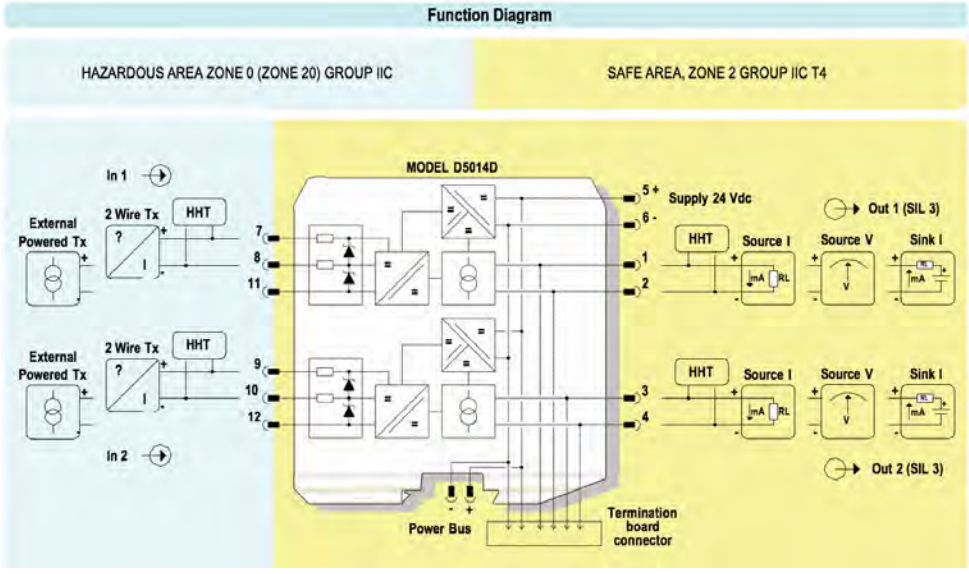


Figure 90, Functional diagram of a SIL 3 Repeater Power Supply HART from GM International

Example of the Safety Function and Failure behavior of the above device:

The model D5014 is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behavior is described from the following definitions:

- fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
- fail Safe: failure mode that causes the module to go to the defined fail-safe state without a demand from the process;
- fail Dangerous: failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
- fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure;
- fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in the safety logic solver is configured to detect Low failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure;
- fail “No Effect”: failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure nor a dangerous failure. When calculating the SFF, this failure mode is not taken into account;
- fail “Not part”: failure mode of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

The 2 channels of the D5014D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent from each other, not containing common components. In fact, the analysis results for D5014S (single channel) are also valid for each channel of D5014D (double channel). This analysis is also valid for D5014D as Duplicator of 2 wires Transmitter Input Signal, but considering safety function is only applied to the channel configured as passive input.

Failure rate data: taken from Siemens Standard SN29500.

The Functional safety manual will also give you a summary of the Failure Rate Table and the potential PFDavg for use of that device in a SIF in relation to a proof test interval and proof test coverage (Figure 91).

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	135.30
λ_{du} = Total Dangerous Undetected failures	14.25
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**149.55**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**763 years**
$\lambda_{no\ effect}$ = "No Effect" failures	201.25
$\lambda_{not\ part}$ = "Not Part" failures	20.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**371.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**307 years**

Failure rates table according to IEC 61508:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	135.30 FIT	14.25 FIT	90.47%	0%	90.47%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes 10% of entire safety function:

T[Proof] = 1 year	T[Proof] = 15 years
PFDavg = 6.36 E-05 Valid for **SIL 3**	PFDavg = 9.54 E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 1.91 E-04 Valid for **SIL 3**	PFDavg = 1.27 E-03 Valid for **SIL 2**

Systematic capability SIL 3.

G.M. International ISM0103-6 **D5014** - SIL 3 Repeater Power Supply

Figure 91, Failure Rate Table and the potential PFDavg

The table shown in Figure 91 makes an assumption of a proof test coverage = 99%, that would not be very practical if you are not advised, or instructed, on how to achieve that. Therefore, it is also mandatory to include in the safety manual by the manufacturer an explanation on how, and what exactly, you need to test and document in order to achieve that PFDavg - SIL performance of that device, see

Testing procedure at T-proof

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test. **The Proof test 1** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to high alarm current and verify that the output current of the repeater reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.
3	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to low alarm current and verify that the output current of the repeater reaches that value. This tests for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 30 % of possible Dangerous Undetected failures in the repeater.

The **Proof test 2** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the **Proof Test 1**.
3	Perform a two-point calibration (i.e. down scale as 4 mA and full scale as 20 mA) of the transmitter connected to the input of the repeater. Then set the transmitter to impose some input current values of 4-20 mA range and verify that the correspondent output current values of repeater are within the specified accuracy. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 99 % of possible Dangerous Undetected failures in the repeater.

Figure 92, Example of a testing procedure at T-proof

Referring to the table in there are two proof test procedures being proposed with the possibility to reveal either 30% (proof test 1) or 99% (proof test 2). This is a detailed example of what you should try to retrieve on every single device by the manufacturer. Since the IEC61508 April 2010 release, the safety manual is mandatory and shall provide you this kind of information.

Beware that the proof test coverage is a defined percent value of 'how good or realistic you can test the SIF functionality under the same process condition as the SIF will have to prevent the potential hazard'. Same as with the proof test interval (8.2.2.7), when the proof test coverage is not realistic or achievable during the SIF proof test, then the consequence is that you cannot proof or reveal certain hidden failures. That would mean that the SIF is potentially degraded in functionality and not performing any longer as estimated, so the expected risk reduction factor is also degrading in function of time.

8.2.2.9 Response time requirements for each SIF to bring the process to a safe state within the process safety time

The process safety time is defined as the time period between a failure occurring in the process or the Basic Process Control System (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed.
This information should come from the process specialist to explain how long it takes from an abnormal condition to go to a safe state with that process unit.

The response time requirement for the SIF is including every interface or device used in that

SIF to go to a safe state, response time to consider and defined are:

- Sensor response time, including rate of change of the process condition;
- Isolator response time;
- Safety PLC response from input – logic – to output, including filters and the influence from potential diagnostic limitation, degradation, restrictions in time cycle, delays in case of internal failures, in other words 'worst-case scenario' should be considered;
- Interposing relay which will be most likely the minimum contribution to the complete SIF response;
- Typically, the final element response time will be the largest contribution to the overall SIF response time, of course exception always exist. The response time should include all subparts or devices needed to achieve the safe state and is usually restricted by the size of the valve (E.g. Valve size [inch] x 1.5 = xx [seconds] that the valve may need to go from process state to a shutdown state. If the final element is a valve, then you should add 20-40% margin on the valve response time to compensate for the valve stroke time degrading over time because of potential wear out.

An appropriate response time from sensing the parameter at the trip set point to completion of necessary actions to terminate the hazard, including those for dynamic effects, is less than half or equal the process safety time (SIF response time ≤ process safety time / 2). This is a rule of thumb used in the process industry and is referred to in several application standards and guidelines, but is not defined in the IEC61511. Often confused in discussions with engineers, the process time ≠ process safety time, example:

- The production of recipe A in the reactor may be 1 week = process time;
- To stop the reaction of recipe A and go to the process the safe state may take 40 seconds = process safety time.

A process safety time of less than 1 second is rare in the process industry, but extremely fast acting processes do exist and I am fortunate to have worked with one to learn it the hard way. A SIF protecting a Low Density Poly Ethylene (LDPE) reactor from explosion by an exothermic reaction getting out of control which leads to extreme high temperatures (1300 °C) and high pressure (2700 Bar), so the release of product via fast acting three-way vent valve (Fail to Open, F.O.) to a water scrubber / vent system needs to be extremely fast ≤ 1 second. It is nearly impossible to achieve here the rule of thumb and try to design a response time of 500mSeconds (= process safety time / 2) as the temperature measurements along may take longer (700 msec.) to sense and transmit their value to the safety plc application program.

In the above example the SIF response time would be defined as:

- Temperature sensor subsystem ≤ 700 msec.
- Logic solver sub-system ≤ 150 msec.
- Final element sub-system ≤ 150 msec.

8.2.2.10 The required SIL and mode of operation (demand/continuous) for each SIF

This definition should be containing the target RRF (1/PFD) that the SIF needs to achieve in order to comply to the assumption made during the hazard and risk analysis HRA. A simple 'SIL 1' as target is not sufficient as you still have a band performance to consider for that 'SIL 1' where the range can be the RRF= (>10 - ≤100). In other words, you can have a very good performing SIL 1 - SIF (RRF = 90) or can have a very bad performing SIL 1 – SIF (RRF = 20). Therefore, many companies apply the rule to achieve a magnitude higher than the required SIL that was found during the risk analysis targeted RRF factor.

The modes of operation to define are:

- low demand (expressed in PFDavg), mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year. Typical example could be a shutdown valve in a refinery;
- high demand (expressed in PFH), mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year. Typical example could be the drain valve of a reactor that is opened once a week after finishing a batch production;
- continuous mode (expressed in PFH), mode of operation where the SIF retains the process in a safe state as part of normal operation. Typical example could be a temperature interlock on a chemical reactor preventing an exothermic reaction to get out of control or in a batch process where the safety valve is also used for controlling the process as part of normal operation.

The majority of the safety functions found in the industry are normally in a low demand mode of operations, whereas the high demand and continuous mode of operations are rarely found.

8.2.2.11 A description of SIS process measurements, range, accuracy and their trip points

A list of the SIS sensors, calibration & operation range, accuracy and the alarm and trip point should be defined. An example is shown in Table 35.

Tag	Calibration Range	Normal Operation Range	Accuracy	Pre-trip alarm	Trip Point
PT101A	0-60 bar	10-35 bar	2%	38 bar	46 bar
TT305B	0-300 °C	150-250 °C	3%	260 °C	280 °C
PT591	0-550 bar	140-420 bar	2%	440 bar	480 bar

Table 35, List of the SIS sensors, calibration & operation range, accuracy, alarm and trip point

Additionally, a transmitter range can be defined for the process measurement trip point to be used within a certain band (%) performance of that transmitter range, example for a pressure transmitter could be 5% to 90%.

8.2.2.12 A description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves

Here you need to define the SIF specific action that needs to be executed in order to meet the criteria for a successful operation of that SIF function. Example, closing both train HIPPS valves on 2oo3 pressure transmitters tripping by having PT101A/B/C and PT102A/B/C initiating the trip as a PAHH101 signal to the HIPPS safety interlock XYZ to close valves QSV-101A and QSV101B. Additional PAHH101 will also initiate ESD 2 level closing all the train ESD valves ESDV101 A/B/C/D.

8.2.2.13 The functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissive for each SIF

In this definition you describe the functional relationship of the inputs and outputs (I/O) for the SIFs and the logical relation between them, see Table 36 below. Alternatively, a P & ID together with the cause and effect diagram or narratives explaining which alarm or input conditions is triggering which output is often being used for that. However, multiple documents referring to each-other can lead to potential human error as information is usually very hard to keep up to date to whatever modification has been done or simply went missing over the years of operations.

SIF #	SIL	Sensor	Description	Final element Safe State
SIF # 001	3	PT101A PT101B PT101C	If pressure exceeds 120 bar in the upstream part and is measurement in a 2oo3 configuration	Close both valves QSV101A and QSV101B in 15 seconds
SIF # 002	2	LT639	If level is below 5%	Stop the suction pump P001 and close valve LV101
SIF # 003	1	FT308 TT305	If flow exceeds 25 L/min and temperature is below 10 °C	Close valve ESV 471 and open MOV 209

Table 36, Functional relationship of the inputs and outputs (I/O) for the SIFs

8.2.2.14 Requirements for manual shutdown for each SIF

Almost all plants have them, the typical red mushroom or emergency shutdown button. These are usually an independent or additional way to bring the SIF to a safe state by the means of manual activation of a ‘shutdown’ button. This should be specified if any of those buttons are

present in the SIF and how to operate and release them as there are various types with or without key latching mechanism.

8.2.2.15 Requirements relating to energize or de-energize to trip for each SIF

This may sound very simple or straightforward, however it will take some engineering capability if you want to mix those two concepts inside one SIS system.

A classical Emergency Shutdown (ESD) application, also known as Fail-Safe application, will work with de-energized to trip functionality, means that the SIF does not need any energy to go to the safe state. Example by loss of instrument air or loss of field instrument power the device must be able to execute the safety functionality bringing the SIF to a safe state.

That does not mean that you can remove the field power supply at once and all safety instrumented functions will be able to go to a safe state, there will be field power needed or available to shutdown the process in a certain sequence or for example to achieve the safe state with a motorized operate valve (MOV). Therefore, although it is called a de-energized application, will need the energy or power for a specified time in able to achieve the safe state of that SIF. Furthermore, the field power supply needs to be both available and reliable, example: overvoltage could damage your instruments and disable the correct functionality of that device, therefore overvoltage protection can be part of the diagnostic coverage of the power converter, example the SIL power supply from GM International (see Figure 93). Although it is called a power supply, it actually converts the power from a source such as the net power, the UPS power of a diesel generator power source into an available and reliable field power for the field instrumentation.

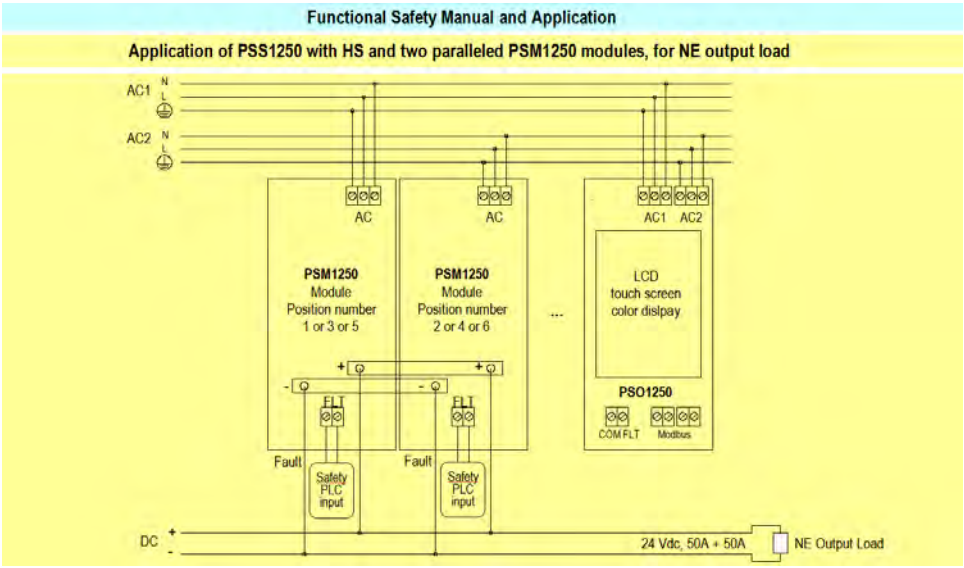


Figure 93, GM International PSS1250 Power Supply, example of application

A classical Fire & Gas (F&G) or alarming system will work with an energized to activate functionality, means that the SIF under normal operation is de-energized and will only cause a trip action in case of energy (e.g. electricity, instrument air). The concern with such type of configuration is that it is not fail safe, in other words, assume you have a wire break to your deluge system, you will not be able to energize the solenoid any longer. That is why we use line monitoring on such SIF output connection, to measure the resistance or impedance of the wire/coil in order to ensure the device is still recognized by the de-energized digital output card of the safety PLC.

With regards to the build in line monitoring functionality of the digital output card of the safety PLC, this is often lost or not working when you need to interface solenoids via an interposing relay, as most of the relays on the market are not supporting this feature. When there is a need to monitor the wiring or load failure of the SIF in an energized to trip functionality, then that specific requirement should be specified herein.

There is however a solution for that with a smart safety relay for F&G applications that supports both line and load monitoring and can provide information back to the control system of diagnostic benefits for that SIF functionality. See below Figure 94.

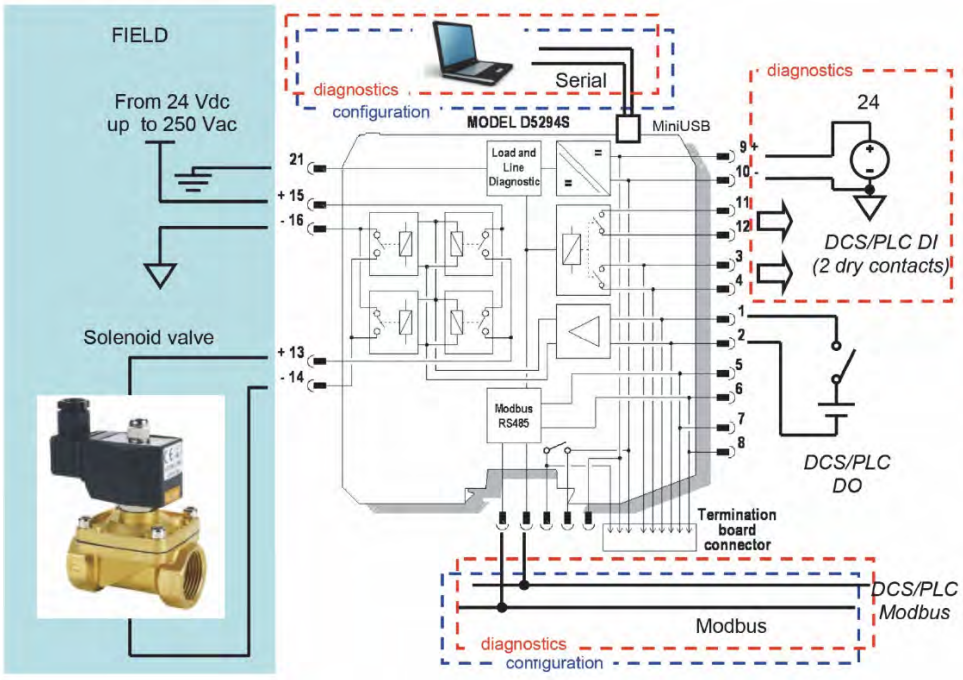


Figure 94, GM International Smart relay D5294S typical application

Since the availability of the field power supply in an energized to activate safety loop becomes a vital part to execute that safety function, is also the reason why you need to select a reliable & available power converter and supply, example the SIL power supply from GM International (see Figure 93).

8.2.2.16 Requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips)

This definition will contain all requirements for restarting the process after a shutdown, such as resetting a latching relay or valve, sometimes people use electronic reset switches in control panels. If there is specific reset action required on the SIF before starting the process up again, then this should be defined here

8.2.2.17 Maximum allowable spurious trip rate for each SIF

This is one of the odd definitions of the IEC61511 standard, as this is the only sentence where the word ‘spurious’ is used. The complete reliability prediction and PFDavg calculations is all about the dangerous failures of that SIF.
This definition of spurious trip is exactly the opposite of the PFDavg, as here you need to specify the likelihood that your process will go to a safe state without a demand, in other

words having a spurious or nuisance trip. This is useful for expressing the process or production availability and to evaluate the cost of spurious trips or downtime of the process. Unfortunately, there is no guidance in the IEC61511 standard on how to calculate that, but there are alternative guidelines or packages available on the market.

Some devices on the market may achieve a certain safety availability by increasing the architecture of the functionality inside that device, example an interposing relay with 3 contacts in a serial configuration (HFT=2) may have 3 independent contacts to open in able to de-energize the output to the final element and claim this as a SIL 3 suitable device. Using 3 contacts in a serial configuration means also that the likelihood for a spurious trip will be very high. It is therefore important to think about the potential spurious trip that such 'simple' device inside the SIF can cause. Alternative solutions exist that offer both safety availability and process availability, example is the below picture Figure 95 of the D5094S relay output module from GM International.

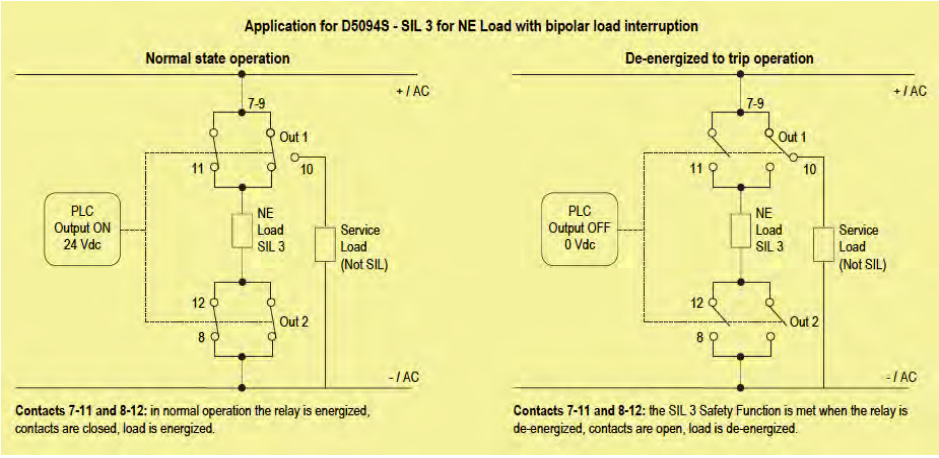


Figure 95, GM International D5094S Relay, example of application

8.2.2.18 Failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shut-down)

This definition should define the SIF potential failure mode and response of the SIS. For example, some transmitters have a built in diagnostic feature enabling signal loss and sensor failure detection (usually jumper settings in the transmitter using the NAMUR NE43 principles), so that the SIS can recognize or be alerted that the transmitter has a problem. Depending on the architecture of the transmitters used (for example a 2oo3 configuration), the operator of that failure can be alarmed and the instrumentation engineer can go and solve the failure of that device in the repair time definition that was used to calculate the PFDavg of that SIF. Another example could be a redundant safety plc architecture having a known detectable failure by the built-in diagnostics and will degrade from a redundant channel to maybe a

single channel starting a (repair) timer in which you will need to solve the failure before the timer expires and may cause a shutdown of that safety plc.

8.2.2.19 Any specific requirements related to the procedures for starting up and restarting the SIS

When starting a SIS or restart after a shutdown, special conditions may apply and should be described. Example, there is maybe a certain sequence of which valve you should line up before starting a pump, or you may want to open or close the process control valve before resetting the shutdown valve and starting up again.

8.2.2.20 All interfaces between the SIS and any other system (including the BPCS and operators)

The interfaces between the SIS and the operator should be fully described, including alarms (e.g. pre-shutdown alarms, shutdown alarms, bypass alarms, diagnostic alarms etc.) or interfaces with sequence of events recording devices.
Furthermore, interfaces with BPCS/DCS should also be fully described, the HMI graphic display could contain things like:

- Live SIF trip setting read from the Safety PLC program for a specific batch control process;
- Transmitter diagnostic information;
- Maintenance Override Switch (MOS) information;
- SIS power supply or power converter alarm information;
- SIF trip status, trip reset information;
- Etc.

8.2.2.21 A description of the modes of operation of the plant and requirements relating to SIF operation within each mode

Different modes of operation can be considered, such as start-up, normal operation, maintenance mode, degraded operation, and demand mode. List of all assumptions in relation to operations, maintenance, and testing. Assumptions can include use conditions, preventive maintenance, how to perform proof testing, and follow-up of diagnostic faults.

Example of mixing two chemical products in a reactor and maintaining a certain ratio to prevent exothermic reaction. The conditions for the SIF are different between start-up phase and during normal operation phase. For the start-up condition you may need first to introduce stream 1 without reaching hazardous conditions before ramping stream 2 to a specific ratio for the chemical reaction to start.

8.2.2.22 The application program safety requirements

This used to be called 'software safety requirements' in the first edition of the IEC61511, but has been rewritten in edition 2.0 as 'application' program safety requirements and has become a separate paragraph in part 1 which is summarized below in 8.2.3 application program safety requirements.

8.2.2.23 Requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared

The operation of maintenance override switch (MOS) should be as per a written procedure that people are trained and monitored on. Procedure must explain under what circumstances these bypasses are to be used and should include things like:

- approval authority, use of key or password to avoid unauthorized use;
- maximum time allowed to leave this bypass activated;
- instructions on how to clear;
- instructions on how to record / document the bypass;
- information on how to guarantee the safe state achievement of that SIF;
- information on how to guarantee the functional safety during the bypass operation;
- instructions on how to keep the relevant people informed of the bypass;
- instructions on how to lock out and tag out the SIF area.

New in edition 2.0 of the IEC61511 is the requirement for compensating measures that shall be taken to maintain safe operation during the bypass being active. The compensating measures should be in place before you start with the bypass.

Although bypass should be limited and not become normal practice, some clients restrict max 1 bypass per process unit at the same time and will have different times for different SIL levels of that SIF. Example SIL 1 max 24 hours, SIL 2 max 8 hours.

8.2.2.24 The specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors

When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation during the time that the SIS is in a degraded mode due to the known or detected failure. When in case of the failure, the SIS could not maintain safe operation, then a specified action to achieve or maintain a safe state of the process shall be specified and appropriate actions shall be taken.

Example, when a failure of a pressure transmitter is known maybe the operator can monitor

a pressure gauge providing the human interaction can act inside the max response time allowed to achieve a safe state. Such human interactions need to be very carefully monitored and controlled, and if possible even avoided, as human failures or systematic failures are still the dominant contribution in any accident investigation.

8.2.2.25 The mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints

The IEC61508 ed. 2.0 introduced new definitions for Mean Repair Time (MRT), Mean Time To Restoration (MTTR), these new definitions have been copied in the IEC61511 Ed. 2.0. (8.2.2.25). Additionally, there is in the IEC61511 Ed 2.0 a new definition called the Maximum Permitted Repair Time (MPRT).

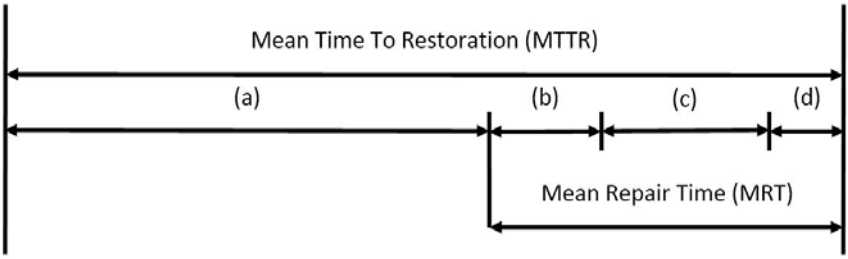


Figure 96, MTTR, Mean Time To Restoration

Mean Time To Restoration (MTTR) is the expected time to restore the SIF again and includes the following time definitions:

- (a) the time needed to find out that the failure is there, which could be off course worst-case scenario the maximum proof test interval time in case of an unknown, sleeping or hidden failure providing that the proof test efficiency or coverage will reveal the failure;
- (b) the time spent before starting the repair, which could encompass things like: is the spare part available?; is there a competent person available?; time to prepare the necessary paper work & permit and foremost the allowance from operations to start the work;
- (c) the effective time to repair, how long will the physical repair time take, example to replace a failing digital output module is obviously faster than replacing a 20-inch shutdown valve;
- (d) the time before taking the component/device back into operation, you will need to re-test, re-verify, re-assess before taking the SIF back into operation and of course update all the documentation.

MTTR times were often specified in the past as 8-24-72 hours to be used in the PFDavg calculation of that SIF. Referring to Figure 94, the largest contribution in the MTTR definition is

most likely the time needed to find out that the failure is there or time (a).
Assuming that the proof test interval on a Fail to Close (FC) shut down valve is for example 9 months, and the SIF has been working as designed, so the shutdown valve has not been operated or demanded, then the potential failure (E.g. stuck open) could not be revealed before you try to proof test that SIF. So worst case the time (a) could be maximum the proof test interval, before time (b), (c) & (d) will even start.
The selection of the MTTR time can only be justified when you have all the times (a) (b) (c) (d) realistically defined according to the end-users' capabilities of testing-revealing and repairing the failed SIF. The MTTR will definitely be more than 8-24 or 72 hours as many reliability reports were (are) based on.
Furthermore, the Maximum Permitted Repair Time (MPRT) can be defined as the maximum duration allowed to repair the fault after it has been identified.

8.2.2.26 Identification of the dangerous combinations of output states of the SIS that need to be avoided

Dangerous combinations of SIF output states need to be addressed within the SIS. Example:

- Simultaneous blow-down by opening all the blow-down valves at once may create a new hazard that needs most likely to be avoided;
- Opening all the relieve valves to the flair mitigation system could exceed the capacity of the flair and will create a new hazard.

8.2.2.27 Identification of the extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors

The SIS equipment may be limited exposed in time to the potential environment extremes during shipping, storage and installation. Although during installation the physical plant location environment starts to kick in, whereas for shipping and storage (like a clean and dry warehouse) may not be the real problem.
For sure during the operations of the SIS, which may have an expected lifetime of 10-15-20 years, the impact of the environment needs to be identified and listed here in this definition and will be unique for that specific plant. A reason more why generic SRSs simply will not work, example a multinational company may have factory in different parts of the world, and although the process/production and instrumentation used may be identical, the extremes of some environments can influence the correct functioning of that device.
Example of some extreme, non every day thought of environment parameters that have nothing directly to do with temperature, humidity etc.:

- A European chemical company has a factory based in Texas-USA dealing with an insect called mud dauber, that likes to build a nest of mud in the vent of the valves, so they

need to install a mud dauber screen. None of the European based sites had to consider that;
- A production plant in Angola was dealing with another animal called monkey which creates unexpected changes to valves by changing or manipulating the hand operated valves, so they need to remove all wheels-handles or secure them as keeping those animals out of the plant was nearly impossible.

Of course the above examples are very extreme but it may start you thinking.
The more common parameters of environment conditions that should be listed are:
- Maximum and minimum external equipment temperature;
- Maximum and minimum internal (auxiliary room) equipment temperature;
- The atmosphere concentrations limits;
- The maximum wind speed;
- The ATEX zone consideration;
- The electrical classification;
- Is there potential flooding, earthquake, lightning or related factors;
- Etc.

8.2.2.28 Identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes

During normal operation mode when there is no failure present, no bypass active and maintenance proof testing is going on, then the SIS obviously should work the way it is intended and design, but when you are in start-up mode of a process or a unit, there may be special conditions applicable only during that time frame. Some examples:

- The safety function in relation to the fire eye of a furnace, during the initial start-up sequence the fire eye will detect no fire but has to leave the gas valve open in order to start up. During normal operation that same fire eye that would detect ‘no’ fire will need to shut down the gas supply by closing that gas supply valve;
- When maintenance is going on a specific section of a process unit, that particular SIF will be disabled or bypassed, but you may need a secondary or additional SIF to bring the process to a safe state if needed;
- When the air compressor is off line because of maintenance, you will need to foresee compensating measures to counterbalance the availability of that instrument air by maybe increasing the buffer size for that period and add an additional backup compressor.

8.2.2.29 Definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire.

A major accident can cause risk for people, environment and capital investment, so we need to design for failure and try to be prepared for the worst-case scenario. When you are designing preventing and mitigation layers that would fail because of the major accident, then that layer was maybe not appropriate or wrongly designed?

Looking at the SIF subsystem or devices, the power supply, the intrinsically safe isolator, the safety plc, the high integrity safety relay, etc. are usually installed in a sub-station or instrumentation building and are protected as far as reasonably practicable from major accident events. Nevertheless, if you have an earthquake followed by a tsunami like the nuclear disaster in Fukushima-Japan, then even those systems will fail.

What is usually listed under this specification and in relation to this specific SIF are:

- Are the shutoff valves equipped with fire proof jackets?
- How long can the valve remain open in case of a fire?
- How long can the firewall withstand the fire?
- Is the field cabling flame retardant (IEC 60332) / fire resistant
- (IEC 60331)?
- How long can I maintain the field power supply for the SIS to bring the process to a safe state?
- Etc.

8.2.3 Application Program Safety Requirements (61511-1, clause 10.3.5)

This used to be called ‘software safety requirements’ in the first edition of the IEC61511, but has been rewritten in edition 2.0 as ‘application program’ (AP) safety requirements. Same as in edition 1.0, the application program (AP) of the SIS shall be in accordance with the application program safety requirements specification or simply the AP SRS. The main purpose is again to help the application programmer to program the correct integrity and to avoid systematic failures that are usually made when you do not have the detailed specification, but a mix of documents like cause & effect, narratives, P&ID, some interlock description etc. Application programmers will typically make an interpretation, based on their experiences, of the information provided and when they have made the wrong assumption because the information was not clear, then that will need to be found during testing, validation and assessments.

The IEC 61511 standard has therefore the following normative requirements under AP verification, review and testing (clause 12.5):

- A competent person not involved in the original development shall review the AP including its documentation;

- The approach used for the review and the review results shall be documented;
- AP shall be verified through review, analysis, simulation and testing techniques using written procedures and test specifications;
- The verification shall confirm that the AP functionality meets the SRS and that there are no unintended side effects with respect to the SIF.

The AP verification shall address the following:

- Conformance to the AP design specification, the defined means and procedures, and the requirements of safety validation and test planning;
- exercising of all parts of the application program and range of data conditions;
- testing for failure conditions (i.e., negative testing);
- timing and the sequence of execution;
- testing of communications to and from the SIS; (e.g. overload);
- integration of the off-line application program with the logic solver hardware and the underlying PE;
- testing reload CPU, influence diagnostics, failure constraints & timers.
- internal data flow checks to confirm that the logic solver is not just apparently working, but is working as expected;
- - when required, integration of the application program and 3rd party devices;
- I/O data mapping to the AP, including data type and range;

During testing, modifications to the AP shall be subject to an impact analysis in order to determine all AP parts impacted and the necessary re-design and re-verification activities

The results of AP testing shall be documented and include:

- The versions of the AP and its supporting documentation being tested;
- The versions of supporting software and test tools;
- Names of the test/review persons + time & date;
- Description of the test/review + time & date;
- The test/review results, whether the objective and criteria have been met;
- In case of failing the test, the reason, analysis, correction details and re-test requirements.

The AP SRS shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The AP safety requirements that have already been specified in the SRS does not have to be repeated as a separate AP SRS.

The input to the AP SRS for each SIS subsystem shall include things like:

- the specified safety requirements of each SIF, including sensor voting etc.;
- the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;
- any requirements arising from the safety planning as part functional safety management.

The AP SRS shall be:

- specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS;
- sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out;
- Consider a comprehensive list of bullet points under paragraph 10.3.5 IEC 61511 part 1.

The AP SRS shall be expressed and structured in such a way that they:

- describe the intent and approach underpinning the AP SRS;
- are clear and understandable to those who will utilize the document at any phase of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by all users (e.g., plant operators, maintenance personnel, application programmers);
- are verifiable, testable, modifiable;
- are traceable back through all deliverables including the detailed design documents, the SRS and the H&RA that identifies the required SIF and SIL.

IEC 61508 Ed.2 and IEC 61511 Ed.2 are certainly the leading standards in terms of safety related equipment: The knowledge of their requirements and the ability to fulfil them are essential to both manufacturers and customers.

This manual is updated according to the latest edition of both standards and includes a new chapter about Safety Requirements Specification.

ISBN: 978-88-942087-0-2
ISBN-A: 10.978.88942087 / 02
Retail price: € 50,00

www.gminternationalsrl.com

gmi technology for safety

FUNCTIONAL SAFETY VOCATIONAL TRAINING

Functional Safety Engineer (TÜV Rheinland) Safety Instrumented System

rev. 2019-00

TVC FUNCTIONAL SAFETY SERVICES

Sample QUESTIONS

Sample Questions

(Only 1 answer per question is the most correct & complete answer)

1. The best source for failure rate data of safety device is:
   - ○ a. An industry database
   - ○ b. A functional safety data sheet
   - ○ c. Application, plant or factory specific data
   - ○ d. Manufacturing prediction data

2. Which one is the false regarding functional safety and its assessment?
   - ○ a. Good management require proper documentation procedure
   - ○ b. Assessment is best done by those who executed work since they are most familiar with it
   - ○ c. The standard specifically requires a certain competency of the assessor
   - ○ d. The standard specifically addresses proper resourcing of the safety project

3. Why is verification and validation important?
   - ○ a. It shows how each safety function fulfills its requirements
   - ○ b. It insures that the safety requirements specification is correct
   - ○ c. It determines whether the safety system does what it is required to do
   - ○ d. a, b and c are correct

4. Which of the following methods is not usually part of analysis phases of the safety life cycle?
   - ○ a. Layer of protection Analysis (LOPA)
   - ○ b. SIL Verification Analysis
   - ○ c. HAZOP
   - ○ d. Risk Analysis

5. Periodic proof testing of safety Instrumented functions:
   - ○ a. Is never required
   - ○ b. Increases the SFF and reduces the architectural constraints
   - ○ c. Is only needed for SIL 3 or 4
   - ○ d. None of the above

6. Each compliant item must have a safety manual, a safety manual is a document used

- a. To document dangerous failures of a product
- b. To provide end-user with information on product usage in safety application
- c. To list electrical safety categories
- d. To provide the legal department with a place to put all liability restrictions

7. How much more risk reduction does a SIL4 system provide than a SIL1

- a. A factor of 1000
- b. A factor of 3
- c. A factor of 10
- d. A factor of 100000

8. What is the purpose of documentation in the functional safety industry?

- a. To effectively perform the phases of safety lifecycle
- b. To support the functional safety assessment tasks
- c. To support verification tasks
- d. All of the above

9. What does likelihood analysis fit in the IEC safety lifecycles?

- a. As part of the safety system installation and commissioning
- b. As part of the hazards and risk analysis
- c. As part of the coverall scope definition
- d. As part of the safety requirement allocation

10. The safe failure fraction (SFF) plays an important role when verifying safety devices. Which statement is true?

- a. When the SFF goes up the PFD goes down
- b. A fail safe design has a low SFF
- c. A good periodic proof test improve the SFF
- d. None of the above

11. How does a Safety instrumented system most typically reduce risk?

- ○ a. Reduce likelihood of harm
- ○ b. Reduces the magnitude of harm
- ○ c. stratifies legal requirement
- ○ d. satisfies managerial requirements

12. What are the two main components of risk?

1. Frequency of occurrence
2. Magnitude of consequences
3. Duration of harm
4. Safe distance from harm

- ○ a. 1 & 2
- ○ b. 2 & 3
- ○ c. 3 & 4
- ○ d. None of the above

13. Two HART transmitters (type B devices), each of SIL 2 rating according to IEC 61508, in redundant safety architecture

- ○ a. Make SIL 3 but an additional PFD calculations needs to verify this
- ○ b. Make SIL3 as the architectural constraints are improved due to the higher fault tolerance
- ○ c. Do not make automatically SIL 3
- ○ d. None of the above

14. Markov is a technique used to do what?

- ○ a. Estimate SIL level of a Hazard
- ○ b. Calculate availability of a function
- ○ c. Calculate the Safe Failure Fraction (SFF) of an device
- ○ d. Calculate probability related to system behavior

15. The following are key consideration for upgrading safety devices or equipment

- a. Compliance with plant standards & requirements
- b. compliance with national & international standards & regulations
- c. Obsolete technology
- d. All of the above

Answers:

1-c / 2-b / 3-d / 4-b / 5-d / 6-b / 7-a / 8-d / 9-b / 10-d / 11-a / 12-a / 13-c / 14-d / 15-d

General INFORMATION:

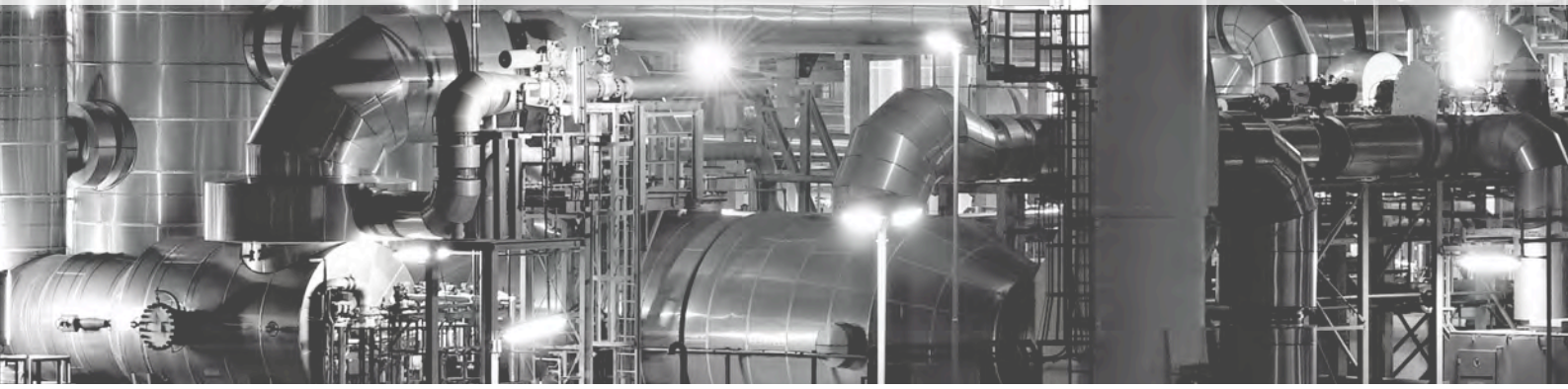
- *the average score from +750 (non trained) people on the above questions was 9.75 / 15*

This page is intentionally left blank

FUNCTIONAL SAFETY VOCATIONAL TRAINING

Functional Safety Engineer (TÜV Rheinland) Safety Instrumented System

rev. 2019-00



TINO VANDE CAPELLE

LinkedIn - resume

Within the TÜV Functional Safety Program:

TÜVRheinland®
Precisely Right.

Tino Vande Capelle

Senior Functional Safety Expert & Trainer, Safety & Security for Industrial Automation and Control Systems SIS & IACS
United Arab Emirates

Summary

Tino Vande Capelle is providing 'INDEPENDENT' Functional Safety Consultancy as freelance & self-employed for equipment manufactures, consultancy firms, EPC's, End Users in the Oil & Gas, Chemical, Petrochemical, LNG, Mining, Refining and Petroleum Industries.

He was educated in Belgium where he gained qualification in Automation & Critical Control Systems. During his 30 years career, in a variety of areas such as LNG, Petrochemical, Refining and Petroleum Industries, he gained significant experience performing Technical Management, Marketing & Technical consultancy, hardware & software engineering, process control engineering, troubleshooting and field instrumentation using advanced control, distributed control, scada, emergency shutdown, fire & gas, compressor control and PLC systems.

In August 2005, Tino has become a Functional Safety Expert & Trainer for Safety Instrumented Systems (SIS) with the new International Functional Safety Accreditation program from the TÜV Rheinland Group. His FS Expert ID is 109/05 and can be found on the TÜV Rheinland website (www.tuvasi.com).

Tino has been responsible for engineering, implementation, training and customer services for Safety Critical Systems and rotating machinery equipment.

He is a registered Professional Engineer in Belgium and a senior member of the Instrument Society of America. He holds patents in the control systems area and has written several papers involving critical instrumented systems.

Specialties: Teaching Functional Safety has become my passion (Nov 2008).

Contact

1101, Fortune Executive Tower, JLT
P.O. Box: 111365
Dubai, United Arab Emirates
tinovc2015@gmail.com

www.linkedin.com/in/tinovc (LinkedIn)
www.tinovc.com (Company)

Top Skills

Functional Safety
Teaching
Instrumentation
Control Systems Design

Languages

Flemish (Native or Bilingual)
English (Full Professional)
Dutch (Native or Bilingual)

Functional Safety Consultancy

Written by my former VP TWW - Triconex: He has an unique blend of technical and business sense not normally found, coupled with an engaging personality that is very "customer friendly"

Verbally fluent in Dutch/Flemish, English, German and (limited - French) languages

Experience

TinoVC
Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor
September 2004 - Present
world-wide

Providing ‘INDEPENDENT’ Functional Safety Consultancy Services as freelance & self-employed for equipment manufactures, consultancy organizations, EPC’s, End Users in the Oil & Gas, Chemical, Petrochemical, LNG, Mining, Refining and Petroleum Industries.

Services including:
• Functional Safety (FS) management & coaching
• Independent FS auditing & assessments
• Customised FS teaching & training
• FS competency review program with the Process Industry leading accreditation program from TÜV Rheinland as FS Expert & trainer (TÜV Rheinland, #0109/05, SIS)

G.M. International s.r.l.
Director - Functional Safety Services
November 2013 - Present
Dubai, United Arab Emirates

Continue to provide world-wide Functional Safety seminars, workshops, consultancy and TÜV Rheinland FS Engineer SIS competency review program with main expertise in the field of Safety in the Process Industry, Engineering in the Oil & Gas, Chemical and Petrochemical and associated industries.

G.M. International is the only company of his kind that is a official approved 'Course Promoter' of the flagship training Functional Safety Engineer SIS of TÜV Rheinland. I am one of the first 5 original appointed Senior Functional Safety Expert & Trainer (ID: 0109/05) for SIS systems with the International Functional Safety Accreditation program from TÜV Rheinland. Having taught more than 2000 people over the last 13 years world wide gave me the maximum exposure to practical issues,problems and questions allowing me today to help engineers applying IEC61511:2016 in a understandable, acceptable and foremost a practical way.

HIMA Paul Hildebrandt GmbH + Co KG

Director - Functional Safety Consultancy

July 2000 - March 2015 (14 years 9 months)

world-wide

Provide world-wide Functional Safety seminars, workshops, consultancy and TUV Rheinland FS Engineer competency review training with main expertise in the field of Safety Critical Systems Engineering in the Oil & Gas, Chemical and Petrochemical and associated industries.

One of the first 5 original appointed by TUV Rheinland as Functional Safety Expert & Trainer (ID: 0109/05) for SIS systems with the International Functional Safety Accreditation program from TUV Rheinland.

Triconex Europe (now Schneider Electric)

Director of Engineering and Technical Services

1995 - 2000 (6 years)

Responsible for the Engineering-, Customer Services-, Turbine- and Training-departments. The above teams were based in various Triconex offices such as Paris/France, Slough/UK, Moscow/Russia and Zoetermeer/The Netherlands. Besides these offices, I have developed, worked with and supported several international systems & integrator houses, OEM's and 3rd party channels to market, i.e. Netherlands, France, UK, Italy, Russia, Spain, Bulgaria, Czech Republic to name a few.

Achieved as the 1st Triconex office worldwide a company safety procedures by implementing and compliance to the IEC61508 (old IEC1508) Safety Standard.

Although Technical was my first responsibility, I was also heavily involved in Marketing and Sales assistance.

PICASS (Independent freelance)

DCS & ESD Consultant
1992 - 1995 (4 years)

Independent Freelance contractor at FINA Refinery (now Total) for the Fuel Oil Upgrading Project (F.O.U.P.) Was main coordinator & consultant for all DCS (HONEYWELL) and ESD (Triconex, Siemens, Honeywell, HIMA) system design, engineering and installation + comissioning of all above with EPC (Foster Wheeler Italy, Fluor Daniel Holland/Haarlem & USA/Irvine, Tractebel Brussels)

Honeywell contractor

Software Application & Control System Engineer
November 1988 - August 1992 (3 years 10 months)

Multiple projects in Europe, as an application engineer with responsibility for configuration and development of all aspects of the TDC 3000 system, consultancy and technical support during the critical client – acceptance period and on site client resident engineer for all software aspects support during all phases of the project.

Distrigas (now Fluxys Belgium)

Instrument, ESD and F&G engineer
November 1985 - 1988 (3 years 2 months)
Zeebrugge - Belgium

Implementation of software changes and system hardware maintenance on Foxboro (FOX 300, Videospec IV, Microspec) and Allen Bradley (PLC 3, Advisor). Maintenance of field instrumentation starting from pre-commissioning, commissioning and start-up phases of a large scale Liquid Natural Gas terminal

Education

Katholieke Hogeschool Brugge-Oostende

BEng (EComE), Automation and Critical Control Systems

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

127 people have recommended Tino

"I was so lucky as to attend Tinos training course in Stavanger Week 47/18. With limited knowledge of the topic, I was worried that the course would be too extensive, and the exam too hard. But Tino managed to guide me through the 3 days of training, with ease! A lot of information was given, but in a clear and understandable manner! Well structured lectures, and useful exercises and homework, made me capable of passing the final exam. I highly recommend Tino and his FS Engineer (TÜV Rheinland) SIS training!"

— Trudy Dreier, *Principal Instrument Engineer at Aibel. November 27, 2018, Trudy was a client of Tino's*

"I was particularly impressed by the energy he radiated and the way he kept me concentrated even after several hours of hard work. My knowledge about functional safety before the course was limited to just few activities I practice at my everyday work, so I had to learn a lot. Was it worth the effort? Absolutely. ... "

— Janez Kokalj, *Principal CTO at Elsing d.o.o. July 9, 2018, Janez was a client of Tino's*

"I attended Functional Safety Engineer (TUV Rhineland) SIS course in Croatia last week. I really enjoyed the class. Tino is experienced, knowledgeable and excellent instructor who gave a great explanation of the subject. He has a lot of experience in process industry and he is able to give example from practice for every topic that he teaches. The course is well organized and suitable for wide range of engineers, from beginners to the experts. I would strongly recommend this course to anyone involved in process industry."

— Ivan Sabados, *Project Manager at S.C.A.N. d.o.o. June 17, 2018, Ivan was a client of Tino's*

"Last week, June 5th to June 8th, I was in Tino's class for the FS Engineer (TUV Rhineland) SIS Training held in Opatija, Croatia. In a first place I was wondering what can I learn for only 3 days, but with certainty I can confirm that with Tino you can learn a lot, even for 3 hours. Tino is really good teacher and for sure amazing functional safe expert. Course is well organised and really useful, for short period Tino has managed to completely change our approach and way of thinking about functional safe. For every our question Tino has had example from practice as an answer, what was wonderful. I also had a chance to speak and change some experience with Tino beside course and I see Tino as a person who really enjoy in his job and invests all his efforts to be only better and better. Tino I really want to thank you for knowledge and experience you shared us, I enjoyed in every second at you course and hope you would come again in Croatia to teach a new generation of functional safe engineers. "

— **Ivan Sarađen,** *Instrumentation and Control System Design Engineer at Scan projekt d.o.o.*
June 13, 2018, Ivan was a client of Tino's

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

"Tino is a great teacher that made a subject that at times can be quite heavy, easier to grasp. I would definitely recommend attending one of Tino's courses. ... "

— Chris Whitmore, *Contract Safety & Controls Engineer April 24, 2018, Chris was a client of Tino's*

"Tino was a great tutor on the TUV Rheinland approved Functional Safety course, its heavy going but he made it manageable and enjoyable. Thanks a lot for a good few days and a great outcome, I passed!! ..."

— Karl Ainscough-Gates, CEng FS Eng Project Engineer, Power Generation. Functional Safety. April 24, 2018, Karl was a client of Tino's

"I was in Tino's class for the FS Engineer (TUV Rhineland) SIS Training. It was a rigorous 3 days of class work with an exam the 4th Day. Though rigorous, Tino is a complete teacher with amazing in depth knowledge of the subject. He delivers his teachings with easy to relate illustrations, seasoned with occasional humours and passion that leaves his students in total appreciation of the subject. I've been to many training classes in past 20 years I must say Tino's class rank among the best I've attended. It was very educative, riveting and refreshing in every positive way. I am not surprise Tino comes highly recommended, he knows his stuff and he's a great Teacher! "

— David Tetenji, MIET FS Eng Snr.Specialist,Electrical, Controls and Instrumentation Engineering at ExxonMobil. April 24, 2018, David was a client of Tino's

"I feel lucky to have trained by you for my Functional Safety Engineer course. It was a three days class with full of experience, scenarios and examples with which the standard was covered. The course was very well planned and organised within the time. The course material was handy to refer, which can be used for future references also. Class room exercises helped to understand. The home work questions and next day review helped to remember daily lessons and clarify doubts. All the concepts were explained very clearly, with correlation with our current industry and this helped understand easily and remember answers during the exam. Hope to apply this knowledge to the development and execute and maintain a successful project. Hope you have recovered from ill. Once again, thank you. Take care. "

— **hemac Chander,** Asst Design Manager at Habu Technology. March 23, 2018, hemac was a client of Tino's

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

"Last Week I took part to his FS course: Great Course, Great Teacher, Great Content. Thanks to Tino I improved a lot my knowledge, I can only strongly recommend him and his course!!! Thanks Tino!!!! ... "

— Luca Brambilla, *Project Electrical Engineer - F&G Engineer. March 22, 2018, Luca was a client of Tino's*

"I got the opportunity to attend his FSE course last week in MIlan (March 2018). Finally the dark aspects of this discipline have unfolded, preparing me to face these issues without fear. Many Thanks Tino ... "

— Sergio Fusaro, Techinal Manager, Co-owner - Next Tre srl. March 20, 2018, Sergio was a client of Tino's

"The FS course was exactly I was expected. I came to check if my thoughts are on the same page with FS standards. Tino just pointed on those gaps that I always had concerns. Now I became more confident and can recommend to everyone to follow Tino's FS courses. Thanks Tino!!! ... "

— Albert Vartic, Senior Instrumentation & Control Engineer, FS Eng (TÜV Rheinland, #16148/18, SIS) at OMV Petrom. March 15, 2018, Tino was a client of Albert's

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

"Dear Tino, I followed your course October 2017 and I must admit that that it was challenging. 3 days in a row followed by an exam on the 4th day. Not easy at all. But I learned a lot. I am now more confident as a safety advisor to discuss functional safety with out engineers and to develop in my company safe, reliable and functional safety systems. Beside that I have now a new network of competent people in the field. As process safety ambassador for Umicore I certainly will recommend the training in the next phase of our journey to process safety implementation. Thanks again."

— Massant Marc, *Manager Technical Safety, Umicor*e, was Tino's client

"Making non-sense should passing a training course successfully, but not mentioning how extensive knowledge of instructor along with his personal attitudes played a great role to achieve so. I recently passed course "Functional Safety" under Tino's instruction & guidance quite efficiently & effectively, leading to learn an enormous amount of practical knowledge of "Functional Safety" never thought before. And don't hesitate to recommend Safety Engineers, Process Engineers and Instrument Engineers to gain benefits of attending this course. Wishing the best and with the best wishes for all aspects of his life"

— Siroos Molazadeh, *Principal Control & Instrument Engineer at Jam Petrochemical Company projects(Brownfield and Greenfield),* was Tino's client

"I recently took part in a functional safety engineering course lead by Tino and I successfully passed the final examination; a success that I share with Tino; so I strongly recommend him as a knowledgeable trainer for those seeking such specialty in the field of functional safety "

— Saeed Beheshti Maal, *Control & Instrumentation Technical Manager, Nargan,* was Tino's client

"I was Part of the TUV Functional Safety course held at Abu Dhabi in Sept'2017. Tino gave the training on Functional Safety with easiness using his vast experience and knowledge .He also shown some videos of the real stories of industry accidents to enhance the importance of Functional Safety. The participants were relatively smaller in numbers and the atmosphere of the class room was excellent. Training was very useful , practical and inspiring me to follow the safety standards. I strongly recommend this course to anyone who involved in Functional Safety Management"

— **Jouhar N,** *Lead Engineer, Schneider Electric*, was Tino's client

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

"I attended 3 days Functional Safety Engineer course at Abu dhabi and consider myself fortunate to join this course taught by FS expert Tino. Tino is Senior Expert in Functional Safety practicing for many years & involved on many International Standards Committee. I personally like his unbiased & independent views relating to FS design & implementation for fulfilling the requirements stated by IEC Standards. For me, personally Functional Safety Specification, SIS Design & Implementation , Verification & Validation was real take away. I felt that 3 days course was really engaging due to its structured topics covering all aspects of Functional Safety with regards to the relevant IEC & ISA standards. I would recommend this course to anyone who is involved & practicing Functional Safety in their profession"

— **Shripad Pande**, *MBA, Project Management Professional*, ADMA-OPCO, was Tino's client

"I attended the TUV Functional Safety course at Abu Dhabi in Sept'2017. Tino gave a complete overview of Functional Safety with all stages of the FS lifecycle, combined with real stories of accidents/disasters to establish the importance of FS, without dwelling into too many calculations, formula etc.,. I could get a complete picture of FSMS. I was impressed with Tino's knowledge, vast experience , complete mastery over the subject and his motivation to participants in preparation and performing the follow-up exams. I strongly recommend this course to anybody involved in Functional Safety Management"

— Padmanabhan Ramabhaskaran, *Control & Electrical Engineering Section Leader, ADNOC Offshore,* was Tino's client

"I took part in the functional safety training in March 2017 and Tino was my trainer. The training itself was very interesting and useful for me as for System Integrator and real life examples from Tino made it easy to understand even the most complicated topics. Great training by very experienced trainer"

— **Andrey Gumennyy**, *Deputy Director, System Automation Service Ltd*, was Tino's client

"I've attended Tino's FS Engineer training course in Milano in March 2017. It was impressive demonstration of how to provide an insight into very broad and complex subject in very limited time by combining lectures, discussions, exercises and homework tasks. Strongly recommended!"

— **Davor Sinka,** *Project Leader, Risk Analysis & Emergency Preparedness, Enconet d.o.o,* was Tino's client

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

"To whom it may concern, I highly recommend the TÜV Functional Safety Engineer training class by Mr. Tino Vande Capelle which I attended myself in January 2017. In just 3 days Tino succeeded to get the utmost out of each of the participants by using his knowledge, experience and anecdotes in the field of functional safety. He challenged all of us to interact, no time to lay back. It personnaly delivered me the insight into the lifecycle model of functional safety. This training really is value for money! Thanks, Tino"

— Remko Schulte, *Managing Director, XXact Safety Solutions B.V,* was Tino's client

"Tino, thank you for the TÜV Functional Safety training. Thanks to your functional safety expertise and passion i passed the exam with flying colours! Cheers!"

— **Dennis van den Hout,** *Senior Software Engineer, Raster*, was Tino's client

"Hi Tino, thanks for the very usefull, practical and high level TÜV Functional Safety training! It was tough, theoretical and an awful lot in a short time, but you kept it interesting and possible to pass. Great!!"

— **Claudia van Batenburg,** *Business Development Manager, Raster Industriële Automatisering B.V.*, was Tino's client

"Capacity in approaching to the topics and teaching the participants into the SIS is stunning. Even hardly understandable and complicated parts of lectures Mr. Tino brilliantly explained in simple and efficient way as well that Functional Safety is not only that but also ongoing process of the people, equipment and procedures. It was a pleasure to attend the lectures and gain real knowledge of Functional safety. Tino, thank you for dedication and passionate work to share great personal knowledge. I highly recommend this TVC Course to anyone who wants to extend knowledge of Functional Safety"

— **Vladan Djokic,** *Project Manager ,VPC East*, was Tino's client

Tino Vande Capelle

Safety Instrumented System & Functional Safety Expert, Freelancer & Independent Contractor

tinovc2015@gmail.com

"I participated in a Functional Safety Course delivered by Tino in Teheran, Iran, Oct 30 - Nov 2 2016. The course was very useful and really challenging. Tino brought his vast engineering experiences with the demands for practical application of functional safety standards IEC 61508 and IEC 61511 in the process industry. His teaching skills and vast knowledge resulted in easy understanding of the subject and it was rich enough to achieve process safety in desired level in practice in every life-cycle phase. He also taught us the safety culture and not compromising safety. I highly recommend this course to all engineers and managers involved in process functional safety. Dear Tino, thanks for the great experience."

— Laleh Rabiee, *Instrumentation & Control Expert, MAPNA Group Co.*, was Tino's client

"As an engineer who has spent years in South Pars Gas Filed as a significant mega project, I think I wasn’t lucky to find Tino sooner. He is more than a good trainer who explains, demonstrates and shares practical functional safety knowledge with you. As a great one he inspires you to follow functional safety concepts in each life-cycle phase of process industries. I highly recommend him to all I&C engineers interested in functional safety and SIS to participate in his program or use his consultancy since it will change your frameworks. Thanks TUV Rheinland, GM International and Tino as TVC for presenting the first Functional Safety program in Iran. "

— Soroush Salajegheh Tazerji, *Project Leader, Kermantablo co*, was Tino's client

"I attended the Functional safety training held by Tino in October 2016 and I recommend it to anyone interested in the subject. The concept of the well thought presentations, full-filled very often with practical examples and lessons learned from the industry together with interaction with the participants, opens new view of the complex matter related to achieving functional safety. "

— Darko Gjorgjievski, *Technical Expert, Exmar*, was Tino's client

"Tino's teaching skills, devotion and enormous knowledge showed me a new world of engineering in a way that it was absolutely easy to understand, clear to try looking for answers and, what is the most important, rich enough to start asking questions. FSE and SIS itself, exist in my company since it was designed, I have worked on it day by day, year by year, but I recently and finally realized what has to be done in near future

(ASAP) to achieve process and equipment safety on a satisfactory level. Thank You Tino, and all the best both in life and in a career (I don't have a doubt about it.)"

— Slobodan Mitreski, *Technical Support Sector Director, HIP Petrohemija a.d.*, was Tino's client

"I have attended in the Functional Safety training in March 2016, Manchester UK . Tino is a true professional with a broad safety experience. I would strongly recommend Tino's Functional Safety Engineering course to anyone involved in safety related business."

— Dimitris Kotoulas, *Electronic Engineer, Hellenic Petroleum*, worked directly with Tino at TinoVC

"I attended the FS Engineer (TÜV Rheinland) training held in February 2016 in the GMI offices in Milan (Italy). Tino's experience is incredible and the way to present the arguments is clear and effective. He's always available for any clarification and creates a very positive atmosphere. Nothing is more true of his words at the end of the course "Remember to check out your SOFTWARE in ALL YOUR safety related devices/systems and READ & UNDERSTAND your certificates/reports/safety manuals and documentation before dreaming that you are SAFE" Thank you Tino"

— Luca Bartoli, *PRODUCTION MANAGER, Vinyloop Ferrara S.p.A. - Inovyn*, was Tino's client

"I have attended Tino's TUV training in November 2015. The way he conducted the training was excellent. Though the topic was little difficult, he managed us to understand the concept with real world examples. Thank you Tino for the great experience!!"

— Muhammed Fasalu, *Sr. Sales Engineer, GM International DMCC*, was Tino's client

"I followed Tino's Functional Safety Engineers course at Eindhoven last week. Tino has the power to change the boring and difficult to understand text from the safety standards into clear and understandable terms and examples. Tino, thank you for the great educational experience! Hans van Hulten."

— Hans van Hulten, *Lead Hardware Engineer, Actemium Nederland*, was Tino's client

"In my more than 30 year engineering practice, I didn’t met faster and more efficient way, as it was 3.5 day Functional Safety training course (SIS), which was held in Belgrade during July, by my colleague Tino Vande Capelle, as the best manner to reconnect positive engineer’s experience with the demands for practical application of Functional Safety standards IEC61508 / 61511 in the process industry. Thank You Tino!"

— Momcilo Cuca, *Project manager for capital projects, NIS AD Novi Sad Processing Block*, was Tino's client

"I participated in the TUV FS program conducted by Tino in May 2015. The best thing about the training was the expert interpretation of the standard given to us by him. Expert interpretation means that we were told about the challenges of implementing the various clauses, where the industry and future trends of the standard

is heading to, what are the pitfalls to avoid while implementation and what to expect from a well engineered solution - and all this in simple & easy to understand way. He has an excellent teaching style and makes sure that all participants equally understand the concepts. The way he handles participant questions and answers helped me in developing a better understanding of the standard as well."

— Omer Bin Abdul Aziz, CEng, PMP, FS Eng (TUV), *Shareholder & Head of Engineering: International Projects, Avanceon MEA*, was Tino's client

"I attended the TUV FS engineer course run by Tino. The course was intensive but kept the focus on practical application of standards with real world examples from industry to highlight the relevance and importance of each topic. Tino has years of industry experience and is clearly a master of the subject, he is also a skilled trainer and delivered the course with great enthusiasm to keep everyone engaged. I would definitely recommend the course to anyone involved with safety systems. "

— Graham Paterson, *Technical Manager, EFC Group*, was Tino's client

"I participated in a Function Safety Engineering course that was taught by Tino. His instruction was excellent, as were his training materials. His wide experience in the field of Functional Safety meant that he had real-world examples to back up virtually all of the instruction topics. Tino even went out of his way to assist me with a topic (Markov modeling) that was not a major topic of the course. I would like to thank Tino for demonstrating to me clearly that Functional Safety is not just about instrumented protective systems, but that it is an ongoing process of people, procedures and equipment. Many thanks Tino. Dave Hugg - Shell International E&P Inc."

— Dave Hugg, *Senior Subsea Controls Engineer, Shell International E&P, Inc.*, was Tino's client

"It is rare to meet such an experienced and knowledgeable individual who can deliver training to a very high standard while accounting for each participants learning style. Tino's delivery is flawless, a perfect balance of informative and engaging - a real testament to Tino's skills and fantastic personality. Tino sets the bar for how training should be and others should aspire to!"

— Matthew Bates, *Process Control and Lead Safety System Engineer, BP Chemicals*, was Tino's client

"The Functional Safety Course with Tino was joyful and very useful. The material was structured very carefully by Tino, in order to allow us to have the most of the course duration, as the subject has lots of aspects to be covered in relatively short period. On the other hand, Tino's approach and effort to simplify the subject was great. Thanks Tino. "

— Ahmed Hamody, *Senior Control System Engineer, DNVGL Group - Noble Denton Marine Services*, advised Tino at TinoVC

"I Have attended the FS Eng. TUV training with Tino @ Dubai, Dec. 2014; Although the course subject itself is a very interesting topic, but with Tino' extensive professional experience in both FS engineering \ training class as instructor; that made these 3 days are brilliant,"

— Mohamed Bassiouny Attia, PMP, RMP, TÜV, *Technical Project Manager, Siemens Energy*, was Tino's client

"I participated in a Functional Safety Course delivered by Tino in Dubai, UAE, November 2014. The course was very useful, engaging and really challenging. These 3-4 days were very interesting and subject kept me focused and motivated all the time. Tino's presentation and guiding skills are really great. I would like to recommend Functional Safety Course by Tino VC to anyone working within process & functional safety and with safety instrumented systems."

— Stevan Ivkovic, TÜV FS Eng / MInstMC / MIET, *Senior Electrical and Instrumentation Engineer, Karachaganak Petroleum Operating B.V. (KPO)*, was a consultant or contractor to Tino at TinoVC

"I attended the Functional Safety course with Tino in Norway. It was an intensive three-days course which I found very interesting, and I appreciated the way Tino explained in a clear and exhaustive way all the topics related to Functional Safety."

— Ricardo Cordeiro, *Instrumentation and Control Senior Engineer - OIL&GAS Offshore Projects, Wood Group Mustang*, was a consultant or contractor to Tino at TinoVC

"I had the great pleasure of attending the course Functional Safety Engineer (TÜV Rheinland) for SIS, held by Tino in Stavanger, November 2013. He is an engaging speaker with a great sense of humor and self-irony that creates enthusiasm for ISO standards, believe it or not ... Highly recommended."

— Gisle Rugland, was Tino's client

"I completed the Functional Safety Engineer (TUV Rheineland) Training Course with Tino as our tutor in October 2014 along with 3 other colleagues Both the course documentation/content and presentation was excellent. I successfully passed the course and would now recommend this course to others as I believe the way Tino completes the course is well structured and easy to follow given the amount of information that has to be taken in. His experience in the industry also helps greatly. Thanks Tino!"

— Simon Nevin, *Service Manager, Tyco Fire & Integrated Solutions (UK) Ltd*, was Tino's client

"I attended the Functional Safety course with Tino on October 2014 in Milan. It was an intensive three-days course which I found very interesting, and I appreciated the way Tino explained in a clear and exhaustive way all the topics related to Functional Safety, which sometimes could be tricky or easily misunderstood. I recommend the other engineers to have the chance to brush up their professional knowledge on Safety by following this Functional Safety course provided by Tino."

— Manuel Avancini, *SW developer, Saira Electronics S.r.l.*, worked directly with Tino at TinoVC

"I had attended TUV FS Engineer Training in Dubai which is instructed by Mr. Tino. The course is a good one and Mr. Tino has good process and SIS knowledge. The explanation given by Mr.Tino during Training is good"

— Venkata Ramkumar Sanka, *SIS Lead, Synergy Engineering Consultancy*, worked indirectly for Tino at TinoVC

"I just passed the exam of Tino's TÜV Functional Safety Course in July 2014 in Shanghai China. Within 3 days Tino could manages to transmit all the key points to us, which should be kept in mind if you touch Function Safety. Normally if a trainning is more than 2 days, then it will be boring, but not with Tino, and belive me you will not fall into a sleep! I would like to strongly recommend Tino's training and the FS Eng.course."

— Xiaolei Cai, was Tino's client

"I have attended training on functional safety in Mar 2013 in Rome. It was a very well structured, very challenging and informative course. I was impressed by Tino’s experience, expertise and practical approach. I strongly recommend Tino's training to all engineers interested in functional safety"

— Salvatore Carotenuto, was with another company when working with Tino at TinoVC

"Somethings cannot just fit into sheets of paper measuring 8 by 11inches with ink all over attempting to describe how to be safe. Somethings can only be learnt in a training with someone who has got it first hand! That is what Tino's lecture on Functional safety brought to me at UAE, April 2014 and I do strongly recommend Tino as a functional safety expert. Training from an experienced expert cannot be quantified with paper and ink!"

— Adebayo Olaoluwa Olawale | FS Eng, worked indirectly for Tino at TinoVC

"I have participated Tino's FS training in Dec 2013 in Prague .I've been impressed by his professionalism,competency and broad safety experience .I would strongly recommend both Tino's training and FS Eng.course to anyone involved in safety related business . Tino, many thanks."

— Branislav Ben#o, was with another company when working with Tino at TinoVC

"I have participated Tino's TÜV Functional Safety Course in May 2014 in Dubai.Tino's knowledge on the subject field was first rate and this was supported by his wide ranging practical experience and case studies. He has a unique and a highly creative way to pass the knowledge of Functional Safety and make people understand how to implement it. His communication skills and practical knowledge kept me interested

and focused all the time. To be honest , I greatly recommend all those who needs or wants to know what Functional Safety is (in real), to participate in Tino’s course."

— Muhammad Fakher, was Tino's client

"I participated in the Functional Safety training course given by Tino in Dubai. Even though the time is very limited Tino manages to pass all the important information about Functional Safety and highlight all the important aspects that someone has to know about this subject. The course is very practical and each concept is made clear by real examples and exercices that the participants work on. Highly recommended for everybody interested in Functional Safety!"

— Zisis Pitsiavas, was Tino's client

"The FS Engineer training was very well taught by Mr Tino Vande Capelle, all the items of the training program were covered very clearly and the exercises and homeworks have fixed the majority of the concepts. In my opinion, if the period could be extend for 4 days, starting at tuesday and, then, the weekend to be prepared to the test, more 0,5 day on monday for the test, I think that the concepts and information could be more easily absorbed by students. My sincere thanks for the training and I certainly will recommend this training for my colleagues"

— Alexandre Wasserman, was Tino's client

"I was attending Tino's TUV Rheinland FS Eng course in Prague. He has wide knowledge in area of functional safety and what is even more important, he knows how to share this knowledge with people. It was probably the best training I have ever participated in. It was a real pleasure."

— Lukasz. Wolicki, was Tino's client

"I had the pleasure of attending the Functional Safety Engineer (TÜV Rheinland) for SIS training course held by Tino in Stavanger, November 2013. The course was a practical approach to safety engineering and is highly recommended for anyone working with safety systems. Tinos skills and expertise as a course leader made this a very interesting and challenging training."

— Egil Solgård, was Tino's client

"I attended the HIMA TUV Functional Safety Engineer training delivered by Tino in Houston, TX, June 2013. The course was challenging, engaging and informative and Tino's presentation skills and energy about the subject kept me motivated for the full 3 days. I highly recommend this course (especially if Tino is presenting) to anyone working with safety systems."

— Ed Crather, was with another company when working with Tino at TinoVC

"I attended the (HIMA) TUV FS Engineer course in Sydney, April 2013 presented by Tino. Prior I wasn't too enthusiatic at the thought of sitting in a classroom for 4 days listening to someone talk about ISO standards but I can honestly say the entire week was totally absorbing. Tino's knowledge of the standards and ability to explain, and relate these to first hand pratical experience was extremely effective and impressive. He was always open to questions and discussions throughout the course which he delivered with engaging humour which for me made the course extremely enjoyable, all the while managing to convey the intracies and pitfalls we must be aware of in our futures as FS Engineers. In short, a really enjoyable and informative course."

— Craig Scott, was Tino's client

"I attended FS Engineer course in Perth and it was a wonderful experience. Not only the content of the course but the knowledge and experience tino shared was remarkable. He engaged class very well and discussions helped to understand some concept in depth."

— Zuhaib Hayat, worked indirectly for Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino has exceptional knowledge of functional safety. He is able to draw on past experiences to help students gain an understanding in the Functional Safety course. His presentation skills, delivery of information both presented and in documents is accurate, suit the purpose it is intended, easy to understand and accessible and available. If anyone is thinking of gaining the TUV Rheinland Functional Safety Engineer qualification then I cant recommend Tino enough. Thanks Tino for getting me through it."

— Anthony Barker BEng (Hons), was Tino's client

"I have just completed the TÜV FS Engineer training in Manchester, run by Tino. The small group worked really well, and the passion and knowledge shared by Tino to the whole group made the course very personable. Tino is an excellent communicator of both his knowledge and passion and ran an exceptional course, thanks again."

— Keith Bird, was Tino's client

"I had the great pleasure of attending the Functional Safety Engineer (TÜV Rheinland) for SIS training course held by Tino. Tino is a true expert in the field of Functional Safety, who provides a brilliant training experience. I would recommend anyone in the market of functional safety, to attend one of Tino's courses."

— Pedro Pinho, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino is a true expert in the field of Functional Safety, who provides a brilliant training experience. I would recommend anyone in the market for functional safety training, to attend one of Tino's courses."

— David Gabriel, was Tino's client

"I attended the TUV Functional Safety course of october 2013 in Breda. From the first hour Tino succeeded to get our attention with his enthusiastic personality. Rather than digging into detailed calculations Tino gave a complete overview of Functional Safety with all stages of the FS lifecycle, combined with real stories of accidents/disasters to proof the importance of FS. I was surprised by Tino's knowledge of the subject and no question remained unanswered. During these three days Tino kept us motivating to study well the course in order to pass the exam. Therefore, I can highly recommend this course to anybody involved in Functional Safety."

— jan verbist, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I attended the TUV functional safety engineer course at HIMA in Houston, September 2013 delivered by Tino. Having completed the ISA84 SFS for a previous employer I had good knowledge of functional safety going into the course. Tino's expert subject and industry knowledge makes him great for the delivery of this type of course. He is clearly very enthusiastic and energetic about Functional Safety which is shown in the way he delivers and teaches. I would highly recommend Tino's services to anyone working in functional safety or needing FS training. Overall a great experience and I look forward to having the opportunity to work with him in the future."

— Michael Shaw CEng, was Tino's client

"I had the opportunity of attending the Functional Safety course given by Tino. A great teacher for a great course! I will make sure to recommend colleagues, who want to improve their knowledge and experience, to attend the course given by Tino."

— Kris Dumon, was Tino's client

"I participated to a TÜV FSE course delivered by Tino in Belgium, September 2013 (HIMA). When you have the change to follow a TÜV FSE course given by Tino, don't hesitate, because Tino is a real expert on Functional Safety and his course is from high quality!"

— Bram Waelput, was Tino's client

"The quality of training, the detail of the content and its application coupled with the historical perspective that only comes from someone with professional experience in the industry made the training opportunity a value. At any opportunity, I would recommend anyone seriously interested in expanding their knowledge of Functional Safety to jump at any training course offered by Tino."

— Horace Bussey FS Eng (TÜV Rheinland, # 7073/13, SIS), was Tino's client

"I have worked with HIMA safety system for more than 12 years back in my company HITEC in Iran and I had learned almost all of my knowledge related to Functional Safety from Tino. He was my instructor for

the TUV FS Engineer training course I attended in Paris 2007. I strongly recommend Tino's training to all engineers interested in functional safety since not only Tino is an Expert Instructor but also he is a generous teacher."

— Amir Moutameni, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I participated to a TUV FSE course delivered by Tino in Sydney, April 2013 (HIMA). I highly recommend Tino for the Quality of his training course. He's a brillant orator and a real expert on Functional Safety. Nicolas"

— Nicolas Lazare, was Tino's client

"I have the honour of being part of TÜV Functional Safety Course delivered by Tino in Dubai March-2013. Certainly Tino is one of the best SMEs in the field of functional safety. I really liked his excellent cross-references to real life situations. SIS standards IEC-61508/61511 seem to be on his finger tips. I would recommend this course to anyone designing, commissioning or maintaining safety related control systems."

— Naveed Shaukat, was Tino's client

"I had the pleasure to be trained by Tino in Rome , March 2013...I have appricieted the level of knowledge and capability of topics teaching ..in such an "easy" and kind mode...Thanks Tino...."

— ROBERTO TONICELLO, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I had the pleasure to complete a Functional Safety course, which took place in Brisbane Australia with Tino. He has a unique and a higly creative way to pass the knowledge of Functional Safety and make people understand how to implement it. I have also found Tino as a very genuine and straightforward person who can work with so easily. He helped me a lot in understanding the principles of Functional Safety and renew my intrest on a subject which is so important."

— Georgios Skraparis CEng MIET, was Tino's client

"I attended the TUV Functional Safety Engineering course run by Tino in Brisbane in October 2012. Tino has a very good reputation and I found this to be well deserved. I enjoyed the course and have already used some of the things I learnt. I would recommend this course to anyone who is involved in Functional Safety."

— Stephen Lowis, was Tino's client

"I attended a Functional Safety course run by Tino in Houston in Sep 2012. I was impressed not only by Tino's knowledge of the topic but also of the info he had 'around' the FS topics - people and companies involved, role of politics and vendors - he really knew FS inside out! I am glad to have attended his course.

Tino's an effective trainer. He transferred a lot of knowledge during the three-day course and at the same time kept us all involved, through Q&A and little jokes here and there - made the could've-otherwise-been-boring course interesting throughout. I'd recommend Tino as a trainer of and an authority on FS topics."

— Aasim Waheed, was Tino's client

""Tino was my instructor for the TUV FS Engineer training course I recently attended in Dubai 2012. I have worked with HIMA safety system before in my company PDOC, but many concepts related to safety systems, weren't really understood with confident, until I attended this excellent course that opened my eyes and made me feel comfortable working with SIS systems. To be honest , I greatly recommend all those who needs to know what (practical) Functional Safety is, to participate in any of Tino's courses or seminars, even after you have been certified, he is a "proven in use" Expert Instructor."

— M.Sc. Eng ESAM KHUDR , CAP, CPE ,TÜV FS Eng , GMC, was Tino's client

"I have attended training on functional safety in May 2012 in Milan. It was a very well structured, very challenging and informative course. I was impressed by Tino's experience, expertise and practical approach. I strongly recommend Tino's training to all engineers interested in functional safety."

— Angelo Golemme, was Tino's client

"Tino was the trainer at the Functional Safety Course I attended in Sydney in March 2012. Tino's knowledge of the subject and and passion in delivering the material made it by far the most valuable course I have attended on Functional Safety. Tino made the material intersting and the exam a breeze. Thankyou for good and interesting week. Cheers, Peter Shumack"

— Peter Shumack, was Tino's client

"I just completed the TUV functional safety engineering program offered by Tino. He is a first class trainer who owns his subject and he can relate it to everyone in the room regardless of experience. Very well done. I recommend it highly to anyone who wants to further their understanding of functional safety."

— Roger Van Nuis, worked with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I had the pleasure of attending the TUV Functional Safety Engineer Course taught by Tino. He is extremely knowledgeable on the topics covered and does a wonderful job of explaining the subject matter related to functional safety both from a historical perspective and current issues. Tino is truly a Functional Safety Genius."

— James R. Folse, worked with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino was our trainer for TÜV FS Eng certification course held in September 2012 in Houston. It was a great learning experience and Tino proved himself to be an excellent trainer, an expert on Functional Safety and a considerate human being. I am greatly impressed with his knowledge on the subject as well as his ability to train people."

— Ahsan Shabbir, was Tino's client

"I attended the "TUV Functional Safety Engineering" course, held in Melsele (Belgium), september 2012. Tino was the trainer during that course. Tino is a very passionate trainer and his perfect knowledge of funtional safety, combined with a famous practical experience and his personality makes this course the best I've ever had durin my carreer as project engineer. Thanks to Tino, I have a complete view of what funtional safety is all about. Thanks Tino!"

— Bart Claes, was Tino's client

"Tino is a great instructor. He knows his material and the background for why things are done one way or another. You can tell Tino has field experience, not just book knowledge. I learned a lot in his class."

— Heath Stephens, was Tino's client

"I highly recommend Tino. I completed TÜV FS Engineer training where I learned a lot, got strong backgrounds what Functional Safety is all about. Tino’s communication skills and practical knowledge kept me interested and focused all the time. He was very good at explaining and pointing out the important details of FS. Thank you very much for you time it was great experience."

— Szymon Olesiak, was Tino's client

"I attended the TUV training course that Tino conducted in Houston in April of 2012. While I have been associated with Tino and have heard many coworkers and clients praise his training capabilities, this was the first chance I had to experience it personally. Tino is a great teacher with tremendous subject knowldege, the thing that impressed me most was the fact that he was able to present the subject matter in a down to earth, real world manner. Functional Safety, in my estimation is all too often treated to academically. Tino was able to make it very real world. We will continue to use Tino for such courses and I highly recommend him to anyone seeking knowledge or advice on this subject."

— Buddy Creef, worked with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I've attended the TUV FS training course teached by Tino in 2012.. As I have attended in my process career (more than 17 years) many trainings programs of all kinds. I have to say in all honesty! This was so far the most professional and well organised training course that I have particpated in. Keeping a class room of more than 10 persons focused, intrested and charing valuable knowledge about functional safety with each other

during a 3-4 day training course. Is an achievement on it's own! Educating me enough in order for me to succeed in the exam was the second achievement :-) Thx, Tino !"

— Johnny Jenkinson, was Tino's client

"Tino was our Functional Safety Engineering Trainer in the Perth Session of March 2012. Undeniably, Tino is an absolute Master of his topic of Functional Safety. Coupled with this Tino's outstanding presentation skills and natural mentoring ability, Tino is able to captivate his audience. Tino selflessly shared vast professional experience and was able to pick real life examples, seemingly at will, that the various members of the audience would easily relate to. I highly recommend Tino and the TUV Functional Safety course for everyone involved in plant design and/or management. Thank you Tino for the new insight and understanding!"

— Kelvin Oakes, was Tino's client

"Tino is a passionate teacher when it comes to Functional Safety, his knowledge is unquestionable and he is extremely good at emphasising why functional safety in the process industry is critical for all. The course he presented was extremely worth while and it will make you think twice before you accept its SAFE."

— Alex Jukes, was Tino's client

"Good Course. I learnt a lot out of this three days course. Highly recommend Tino for any type of safety related consultancy or teaching work. Tino is quite approachable. He has deep understanding of standards and concepts."

— Harit Jani, was Tino's client

"The TUV FS training I attended from Tino in feb 2012 was excellent. Tino really proved to be an expert in the field of functional safety. He answered all my questions and cleared many misconceptions about Functional Safety. His presentation was full of passion and energy. I feel more competent after attending training from him, thank you sir. I wish you all the best."

— Muhamad Usman Younis, was Tino's client

"I have attended Tino's training on functional safety between 19-22 February 2012 in Dubai. It was a fantastic training, well-organised, well-structured, practical. Tino's expertise on the subject and his teaching skills gave me a clearer insight into functional safety. I strongly recommend Tino's training to all engineers who are interested in functional safety as starter/complementary/refresher."

— Abdulkadir Cans#z, was Tino's client

"Approachable, Expert in Functional Safety Engineering, a Good Leader, a Good Communicator- this is what TVC is. I first met TVC at ADIPEC 2010 in Abu Dhabi. We had a brief chat and we discussed only Functional Safety Engineering. I must say that Functional Safety Engineering is truly TVC's passion. His understanding of the subject, pros and cons of the ticklish issues like SFF/device reports is great. The Gentleman actually calls up the certification agency if he finds that there is some issue with the device certification data."

— Vinod Pal Singh, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I was a student at Tino's Brisbane TUV course, which I found very informative as Tino has excellent knowledge and skills in functional safety. I can confidently recommend this course and Tino as a trainer to anyone at any engineering level. Keep up the great work mate."

— Rob Samardali, was Tino's client

"Tino was our Functional Safety Engineering Trainer in the Tokyo Session of 2011. Besides his mastering of the topic, his high presentation skills and his mastering of all the other mendatory aspects required by the job, Tino had this special wilingness to share his rich professional experience with the perfect strangers we were. I strongly recommend his course and other Functional Safety related services for any organization looking for efficiency and professionalism. Thank you Tino and see you probably during the Functional Safety Expertise session."

— Abderrahmane Nafa, was Tino's client

"I attended the FS Training Course in Prague, Czech Republic in December 2011. I already practice safety engineering as an occupation but completed this course to enhance my knowledge and understanding of functional safety. This was about the best I could have hoped for, a truly exceptional course with an exceptional teacher and I thoroughly enjoyed it and learned a lot from it. Tino used his own personality well to provide a new insight into safety within industry and the passion with which he delivered the course ensured that the message was clearly received. Now I’m sure I and all of the other course members will be much more functionally safe in the future."

— Simon D Jackson, was Tino's client

"I attended Tino's TUV certification course in Prague and it was the best safety training I've ever been on. Tino is a real expert and I liked he explained complex safety norms based on his personal experiences gained on real projects he worked on."

— Jan Kvac, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I attended a 4 day course in Functional Safety recently and Tino delivered the course. Tino's knowledge and experience on the subject was extremely good. In his unique and creative way he ensured that the class understood the importance of functional safety in relavent industry. I have worked in the oil and gas industry since 1976. I learnt a lot about functional safety in spite of this. Tino was great."

— Prakash Iyer, was Tino's client

"Tino has been the trainer for the Functional Safety Engineer course I attended in Rome last October. I was impressed by his completeness: expert, experienced, detailed, pratical, understandable and friendly; and all features over the top! I enjoyed each moment of the course. His passion and interest for the Functional Safety has been very contagious. Tino is a FS autorithy."

— Fabio Bellina, was Tino's client

"Je suis heureux de recommander Tino Vande Capele pour la qualité de la formation Sécurité Fonctionnelle qu'il anime avec brio pour HIMA, en collaboration avec TüV Rheinland. Tino parvient à expliquer en termes simples les normes CEI61508 et 511, et sait se mettre à la portée de son auditoire. Les exemples et anecdotes cités au cours de la formation sont pertinents et témoignent de l'expérience cumulée de Tino dans le domaine de la Sécurité Fonctionnelle."

— Stéphane Papoz, was Tino's client

"Tino has been the trainer for the TUV FS Certification course I attended in Rome. His great skills in keeping his students' attention high, together with his experience in Industrial Plants and Functionally Safe Applications made his interesting course also easier to follow, though concentrated in few intense days. I feel like suggesting him as a teacher: with the appropriate prerequisites, as required by the application procedure, everyone can take benefit by his FS course, seeing Functional Safety as something to be kept in our minds in all the phases of ours and our team's work."

— Ranieri Margheri, was Tino's client

"I've been valuing Tino's great professionalism, as one of the participants to his TUV Functional Safety course for Engineering Professionals in Rome. Such trainings require a particular ability to make far-from-immediate concepts come across; this quality, although expected by any attendants, cannot be taken as granted. Tino fulfilled my best expectations thanks to his *proven-in-use* knowledge and his communication gift with us class. Moreover I also appreciated the professional fair approach to practical applications without falling into temptation to turn a Training about Safety Standards into advertisement for given Safety Products."

— Federico Bistarini, was Tino's client

"I attended a training in Oct, 2011 for TUV Functional Safety Engineer conducted by Tino in Abu Dhabi. I found Tino be very effective trainer with in depth knowledge of the subject area. He presented the subject matter in a way which made it very interesting and relevant with the practical world. He could give very specific examples because of his accomplished career. He really is an authority in Functional Safety."

— Kashif Ijaz, PMP, PMI-RMP, TUV FS Eng, CAP, was Tino's client

"Tino has a profound knowledge of functional safety and a natural way to share his experiences with his students. Thank you very much for the training."

— André Pinheiro, was Tino's client

"Tino facilitated at Functional Safety Engineer training course. I was impressed with his experience and expertise and the manner in which he brought a practical approach to the subjects making them that much more relevant. Tino has a friendly but focused approach to the training which made the course that much more enjoyable for all those who attended."

— John King, was Tino's client

"Tino presented a recent TUV course on Functional Safety at New Plymouth, New Zealand. The course was informative and detail orientated but was made fun by Tino's unique perspective, obviously gained from his many years spent in Industry. I highly recommend this course."

— Christopher Jones, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I recently attended the TUV Functional Safety Course presented by Tino. I found him to be extremely knowledgeable on the subject, with many first hand accounts. His teaching method is first rate and he is passionate about his subject, he made the course interesting, which in turn made it easier to grasp."

— Kevin Sykes, was Tino's client

"I recently attended the Functional Safety Training delivered by Tino and was thoroughly impressed by his delivery and professionalism. His depth of understanding is significant, both at the theoretical level (what the standards say) but more importantly for the end user, at the practical level (how to meet the intent of the standard and what to watch out for when you do). I would thoroughly recommend Tino's Unbeatable Value (TuV) ;-)"

— Simon Hehir, was Tino's client

"Prior to the FS Training course conducted by Tino, I thought FS Course is too difficult to digest. But Tino makes it easy in a simple step-by-step approach with the specially prepared slides. He has an unique ability to put a complex topic in simple format. He provides real-life examples how the end-user or the designer

or system integrator overlook safety aspects and brings the fundamentals we all should focus about FS. His guidance will very valuable for anyone not only in FS Training but also for someone seeking consultations in latest in safety standards and conceptual design related to a safety projects. I strongly recommend Tino when it comes to FS Training and implementation."

— Kamath Rammohan L, was Tino's client

"I recently attended TUV Functional Safety Engineer course conducted by Tino. I must admit that I have learnt a lot from this program and Tino really helps to bridge the understanding of this " dry and complex " subject with his excellent training skills that peppered with real life examples. I especially enjoyed the practical student exercises that enhance my understanding on various Hazard Risk Analysis methodologies, what and how to define a safety function and a practical example of what to look out for in a certificate . To sum it up, I highly recommend anybody seriously considering trying for TUV Functional Safety Engineer certification to attend Tino's course."

— Alvin CJ Chin, worked with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I was attended the HIMA FS trainin "TUV FS Program for Engineering Professionals" and Tino was excellent lector."

— Milan Beranek, was Tino's client

"Being a participant on Tino's TUV Functional Safety SIS course in Prague was a great experience, Tino delivered the course with enthusiasm and energy. I recommend anybody seriously considering trying for TUV Functional Safety Engineer certification to attend Tino's course. This is a tough subject but Tino delivers the material in a way that makes perfect sense to all levels of intelligence."

— David Tomblin, worked directly with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino was my instructor for the TUV FS Engineer training course i recently attended (october 2010): to be honest, before starting the "class", i was wondering how i could ever keep my attention and interest with no blackouts for 8 hours a day, as this is not such easy stuff to teach, and not an easy stuff to learn. Well, my doubts were soon gone: Tino has a terrific capability to keep the attendants focused, an extraordinary ability to make the "students" understand and catch which the key-points for each topic are and outstanding communicative skills he can transfer his knowledge through. It's a matter of method,passion, experience and committment and Tino has all of them."

— Michele Calabrese, was Tino's client

""I just recently attended an excellent TUV Functional Safety Certification course, put on by HIMA Americas. The course was very challenging and informative. The instructor, Tino Vande Capelle, did a most outstanding job presenting the course material. He is an Expert in Functional Safety and really knows his

business. His course is very fast paced and he keeps you on your toes. I felt like I was drinking from a fire hose with all the material that was presented during the week and the four hour exam at the end of the week was a real mental workout, the toughest since college. I highly recommend this TUV Functional Safety course and especially Tino Capelle as the instructor.""

— Mark Imper, was Tino's client

"I took Tino's TUV Functional Safety Certification Course in Sept. 2010 and recommend both the course and Tino as an instructor. Tino's broad experience in functional safety and his willingness to speak frankly about his experience make him a very effective instructor."

— Greg Hardin, worked with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I attended Tino's Functional Safety Engineer Certification course in Shanghai (China) in March 2010. This is not the first functional safety training that I have attended, but it was the best. I would like to thank Tino for his excellent training and I would recommend Tino to any company wishing for an excellent instructor in the field of Functional Safety."

— Timur Berendiaev, was Tino's client

"On March 23-26th this year, Tino give us a Functional Safety Engineer training course in Shanghai. Tino made these boring concepts simple and interesting. 3 days time flies very fast.His erudition and professional really impress us."

— Nicolas Xu ##, worked indirectly for Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino was my trainer during the "TUV Functional Safety Engineer" training and certification in March 2010 at Hima Shanghai. He impressed me with his very well structured training program and his excellent presentation skills. What makes him for our class and me outstanding is the fact that his deep knowledge about functional safety is not only base on theory and international standards but considerably more on the experience in the field and real life. He knows well how to guide his trainees through the jungle of codes and standards. His training includes examples from real life as well videos which creates an interactive communication between him and his trainees. I learned a lot about functional safety in this training. To bring it in one sentence “Tino is an excellent and competent teacher”. I would like to thank Tino once again for his excellent training and I strongly recommend Tino as a functional safety trainer and expert."

— Kamil Zima, was Tino's client

"Tino has shown me a path through the jungle of Functional Safety, 61508 and 61511."

— S. Junied Ahmed, was Tino's client

"Tino is a very good teacher of safety features. I highly recommend his functional safety course. In his lecture, the points are clearly organized, often introducing good examples, easy to understand and answer the questions of participants to the point. Not only that, he will provide the precautions described in an orderly sequence that is derived from a variety of questions. Also, the atmosphere of the lecture which comes from his personality is full of enthusiasm, not to be bored at all. Of course you are required to prepare advance basic knowledge, and the amount of assignment of reviewing the day's lecture is quite a few. But if you master the gist of his advice as well, 'TUV Functional Safety Engineer' is definitely going to be one of your credentials."

— Yuki Mikami, was Tino's client

"I studied for TUV Functional Safety Engineer with Tino Vande Capelle as the teacher and he is a very experienced person in the area of Functional Safety where he can explain the content with very practical examples. Especially the practical approach to his field of expertise makes the information quickly accessable and understandable."

— Ruud Geldhof, was Tino's client

"I attended a Functional Safety class in Belgium in November 2009 were Tino was the trainer. Coming from a Chemistry background this training was my introduction to Functional Safety. In only three days Tino increased my Functional Safety knowledge upto a level required for my current role as PSM Engineer. Tino's pleasant way of teaching and his high level of experience in the field made this course interesting from the beginning till the very end."

— Laurus van der Wekke, was Tino's client

"I attended Tino's TUV Functional Safety Certification Course during 10/12/09 - 10/15/09 at Houston. This program is very well structured and rich in contents. At the end of the course you not only have a very good chance to pass the test and become a Functional Safety Engineer but more importantly you learned the knowledge and will have completely different attitude toward the process industry safety system implementation. I strongly recommend any professionals whose job relates to the industry safety to take this course, your career and company will be benefited greatly. Tino has lots of industry experience, his knowledge and humorous personality makes him an outstanding instructor. I am so glad that I took the course and got to know him so if I ever have needs; I know he is the best person to help and through his contacts and connections I won’t be alone. Thank you again Tino, can’t express enough about my thanks."

— Tony Wu, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino has been instrumental in improving the SIS skill sets for my company bringing real life experience and fact based training to the table. Obtaining TUV Certification was the next step in fulfilling my company's

directive and Tino has made that happen. I would recommend Tino to all who are looking to achieve SIS Certification and to those that are looking to have their company's compliance to IEC 61508 and IEC 61511 authenticated. He is an extremely competent and uncompromisable asset to our industry."

— Bob Brown, was Tino's client

"I had the privilege of attending Tino's Functional Safety Engineering Course in Houston Texas October 12-15. Tino was both engaging and factual in his teaching of this important subject. I would recommend Tino to any company wishing for an excellent instructor in the field of Functional Safety. By far, this was the best course and best instructor I have ever encountered."

— Laurie Poe, worked with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino was my teacher during a TUV Functional Safety training course; I can say that Tino has a deep knowledge of safety-related issues, not only from a theoretical point of view but also from a practical point of view. He was able to answer many of my questions about problems I encountered in the development of petrochemical plants. I'd like to add that Tino put a lot of passion in his work and my experience was quite good."

— Pietro Andreotti, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I had learned about the Functional Safety Management from my old friend working with Oil Company in India. Then I gone through various literatures and grasp some knowledge about the subject. Then with the guidance of Mr. Marc Souche of M/S TOTAL we had started a project for validating the SIL level in our plant in Messaaid, Doha. When we were stuck at a point and looking for some solutions, we came to know about the course conduct by M/S HIMA in Dubai and we registered to the course. It was a review training course for TÜV Functional Safety Certificate. I think the course is well designed to provide engineers involved in Safety Instrumented Systems with know-how on Functional Safety Management and applicable standards like IEC61508 and IEC61511 in this field. Mr. Tino had touched all aspects of functional safety management and cleared many doubts, I had in functional safety. Some of issues being negligent in the field, especially the Users like us are highlighted, Thanks to Mr. Tino for his extensive knowledge and experience in this field. 1. Architectural Constraints of SIS Loops which (I was) normally were overlooked when calculating Safety Integrity Level (SIL). 2. Claim by Manufacturers for SILx products. 3. Proven–in –use claims 4. FMEDA Reports authenticity 5. Reliability data availability, etc… The list goes on… It was one of the excellent courses I had attended in my carrier. Mr. Tino’s presentation was excellent and I do recommend that engineers and managers in Safety Instrumented System should attend this training. Additionally you will be receiving TÜV Functional Safety Engineer certificate on successfully completing the course. It is a valuable certificate to boost your carrier potentials."

— Mujeeb Kabeer, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino was my trainer for the certification course in Functional Safety Engineering that was conducted my HIMA Middle East in March 2009 in Dubai. His vast area of expertise and in depth knowledge in Functional safety helped us getting a very good knowledge in the aspects of functional safety. His way of conducting the training was highly efficient in catering to every individuals requirement. He gave many tips and notes and sample questions during the training that helped in getting certified. He presented a lot of videos and questionnaires which made the training a lot interactive and interesting. I strongly recommend Tino as a Functional safety expert and a good trainer."

— Pethusamy Rajaram, was Tino's client

"I attended a Functional Safety training course in Perth, Tino was the consultant and immediately impressed with his attitude to the course. His knowledge of the subject was excellent and he could give examples from his own work experience. He could gauge a persons understanding and give extra help and support if required. From a personal point of view I would have no hesitation in recommending Tino."

— Peter Smith, was Tino's client

"I attended the 'Functional Safety Engineering' course presented in Perth, March 2009. The course was very helpful and practical, with good quality training materials. Tino is an excellent presenter who was able to clearly communicate the concepts and provide examples from his experience to illustrate the points."

— Rebekah Reilly, was Tino's client

"As Tino's student in the HIMA TUV Functional Safety Course held in Perth in the first week of March 2009, I was very impressed with the way he delivered the course with much precision and concision in just a short space of 3 days! His unique teaching style was both so effective and captivating that it tended to generate individual's self-interest of striving to learn, think and comprehend the subject in greater depth. His vast practical experience had made possible for him to single out salient aspects of the subject which he delivered with such powerful and repeated exertion that made the sink-in-the-heads process almost a certainty. He has also demonstrated the good quality of being a personal and caring coach to his fellow students on an individual's need basis. Without any hesitation, I'd strongly recommend Tino as a Functional Safety Expert in engaging with any field of FS-related businesses."

— Peter Siew, was Tino's client

"Tino has conducted an Excellent, Well presented TUV Functional Safety Managament Training Course in Perth, Australia in first week of March 2009. He has an Exceptional Practical Knowledge in the areas of Functional Safety, SIS Standards IEC 61508 & 61511. He delivers the training in a very well structured manner and interacts with each & every participant for lots of case studies related to Functional Safety in Process Industry. I strongly recommend Tino, as a Functional Safety Expert and an Enthusiastic Trainer."

— Shrishail UTAGI, was a consultant or contractor to Tino at HIMA Paul Hildebrandt GmbH + Co KG

"Tino was my trainer for the HIMA TUV Functional Safety Engineer course. He proved to be a highly knowledgeable expert in functional safety with lots of practical experience. His teaching style is easy-going, entertaining even but highly effective. I thoroughly recommend Tino as a functional safety expert and trainer."

— TUNG NGUYEN, was with another company when working with Tino at HIMA Paul Hildebrandt GmbH + Co KG

"A long time professional with HIMA recommended that I attend a Safety Engineering training course to be conducted by HIMA Safety Training Center in Dubai, April of 2008 in order to acquire certification as Functional Safety Engineer. With a number of years of experience in the field, I was apprehensive in investing in the training course not knowing what to expect, let alone having to pass the final test given the fairly short notice to prepare. Then I read the White Paper, Functional Safety: A Practical Approach for End-Users and System Integrators, co-written by Tino Vande Capelle and Dr. M.J.M Houtermans. This well articulated paper, neatly correlated to my work on Functional Safety Engineering, which made my decision to self-finance for the course a plausible investment. For those that have worked on Functional Safety, but are unable to gauge whether the training course is for them or not, I suggest that these individuals first read the White Paper. Attending the course consequently made a lot of sense. Tino Vande Capelle conducted the training course, delivered with powerful presentations, video footage of actual hazards in the work place, group discussions, stage-by-stage exercises for self-evaluation to advance to next level, thus presenting the course with brilliance and a vital balance of text material and audio/video content. The audio/visual presentations where a favorite, where I particularly enjoyed the challenge given in coming up with various reasons on the cause of the hazard. Where I seemed to overlook some of the causes, those would be picked up by fellow course trainees and were thus shared and discussed individually. Tino also shared many of his personal experiences in the field coupled with sample Safety Requirement Specifications. I must stress that the training course is really a re-fresher course, (reading the standards alone may only help somewhat) as it impossible to accumulate the wealth of knowledge on Functional Safety in just 4 days. Tino ensures that your experience and understanding of the Standards is brought to focus and revived during the course. As a bonus, after hours, Tino provided a numerous reference materials in the form of CDs, paperbacks, web links to self-evaluating test sites, etc., to provide trainees to develop further and explore their own direction in the field. Last but not the least, who knew that the course fee covered a 5-star venue like the Hyatt - Dubai, with its unmatched ambience and hospitality."

— Joao Fernandes, was Tino's client

""Functional Safety" is an emerging concept in Australian industries.HIMA's Functional Safety Management (FSM) course is in the forefront of delivering the best knowledge outcomes for achieving world class process safety standards. HIMA's Functional Safety Management course goes into the rigour of technical requirements leading to a process safety outcome. A systematic safety lifecycle assessment with well documented process certainly emphasises on achieving target risk levels. The course content covers in depth

on crucial elements like desired reliability, writing safety requirement specifications, safety integrity level determination,proof test intervals,change management principles, independence during verification and validation. The course is well structured and is professionally well delivered.Tino Vande Capelle delivers the course with professional zeal and enthusiasm.Practical field work experience and a sound understanding of process safety issues makes Mr.Capelle truely a world class trainer. I personally have gained new perspective on functional safety management and has certainly broadened my professional outlook on process safety.I have high regards for the knowledge possessed by Mr.Tino Vande Capelle. I strongly recommend this course for all chemical or related field dealing with process safety."

— Mahesh Murthy, was Tino's client

"Tino and I worked together, since 2003, on a number of functional safety projects for HIMA internally and on client projects. Tino has a hands on approach to everything and his large network in this field makes it possible to solve any problem."

— Michel Houtermans, reported to Tino at HIMA Paul Hildebrandt GmbH + Co KG

"I brought Tino in to develop a project engineering capability and to lead the service engineers within our organization, covering Europe and Africa. He displayed strong leadership in building our technical group. He is diligent and efficient in Project Management and cost control. He is extremely effective in negotiations with clients at all levels. Tino is a team player possessing strong leadership skills. His contributions were a major reason for the success of our Business Unit."

— T. Wayne Williams, managed Tino at Triconex Europe (now Schneider Electric)

Contact Tino on LinkedIn

TRAINING FACTS

rev. 2022-00

2005-2021

FS Eng. (TÜV Rheinland) SIS training

- **201** given training
- **2586** FS Engineer SIS taught
- **79%** passing rate

2016-2021

Functional Safety and SIL introduction

- **14** given training
- **189** students taught

IEC61511 ED 2.0 2016 update course

- **43** given training
- **611** students taught

Functional Safety Management

- **4** given training
- **37** students taught

2020-2021

Online Functional Safety Webinars

- **23** given webinars
- **1744** registered attendees

All webinars are available at the **YouTube** channel from GM International - Technology for Safety

Read previous students feedback:
http://www.tinovc.com/en/testimonials/

TVC FUNCTIONAL SAFETY SERVICES

www.tinovc.com