3. AS IEC 61511 Overview

GAS DETECTOR FUNCTIONAL SAFETY

OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Purpose

Introduce
AS IEC 61511

TOPICS

Introduces the main functional safety standard used in the process industries

Explains some basic concepts and terminology

Introduces the lifecycle that is used for the rest of this course

AS IEC 61511

FUNCTIONAL SAFETY: SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRIES

IEC 61511 - Title

Functional safety:

Safety Instrumented Systems

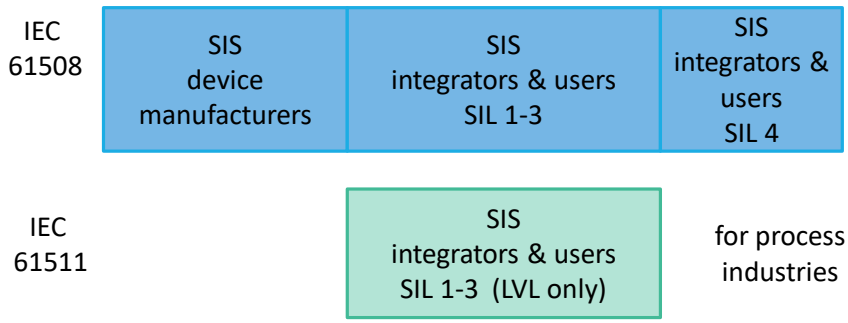
for the process industry sector

Safety Instrumented System =
E/E/PE Safety Related System in IEC 61508

Only for process industry sector

- Uses more familiar terminology than IEC 61508
- Greatly simplified in places

IEC 61508 or IEC 61511



Integrators & users in the process industries can use either IEC 61508 or IEC 61511

IEC 61511 is generally simpler to apply

IEC 61511-1, 2 & 3

Functional safety: Safety Instrumented Systems for the process industry sector

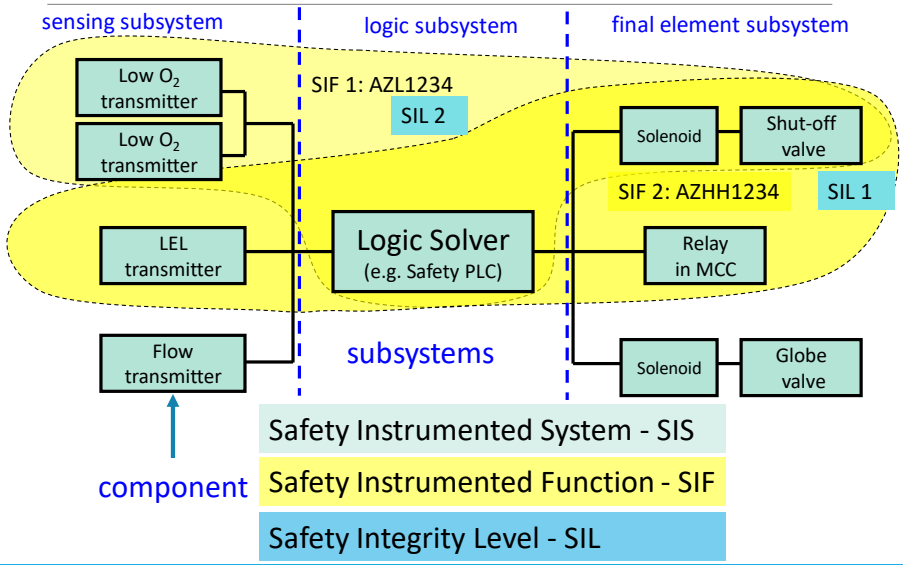
Part 1	Framework, definitions, system, hardware and software requirements	Normative
Part 2	Guidelines in the application of part 1	Informative
Part 3	Examples of methods for determining safety integrity in the application of hazard & risk analysis	Informative

2003 All three parts published as IEC standard
2004 Adopted unchanged in Australia as AS IEC 61511-x:2004
2014 Edition 2 Committee Draft for Voting (CDV) May 2014
2016 Edition 2 published by IEC as IEC 61511-1/2/3:2016 with part 1 corrigenda and many typos
2017 Edition 2.1 published incorporating corrections
2018 Adopted unchanged in Australia as AS IEC 61511-x:2018

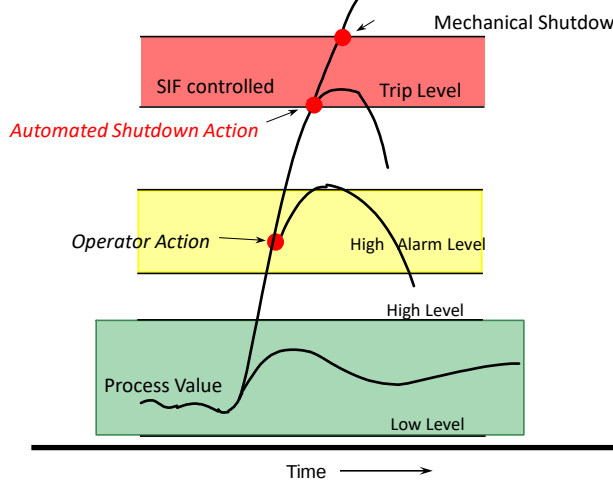
This course is based on IEC 61511-1:2016 Ed.2.1 (= AS IEC 61511-1:2018 Ed. 2)

Basic Concepts

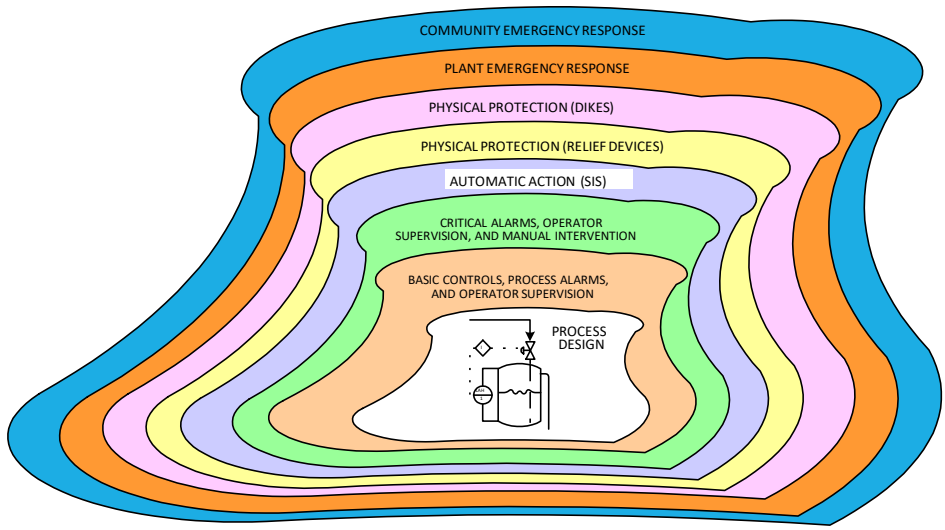
Basic Terminology



What a SIF does



Layers of Protection (DOW onion model)



Key Definitions

Hazard
- potential source of harm

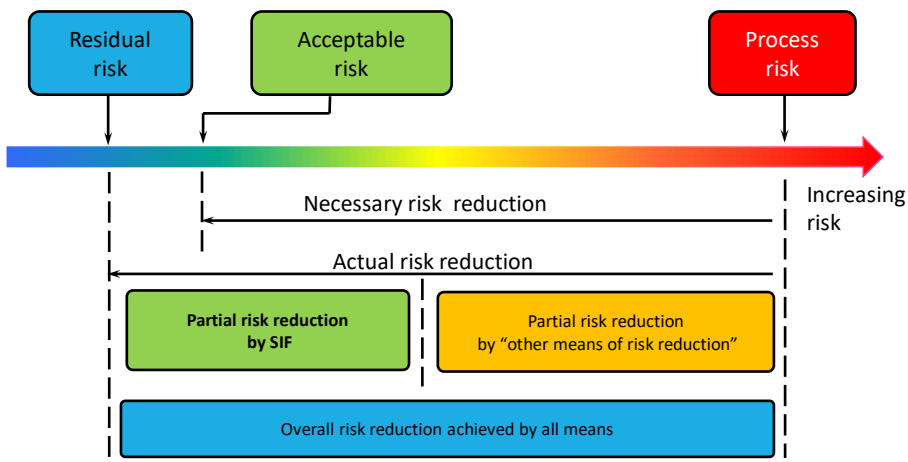
Hazardous Event
- an event resulting from realisation of a hazard
- has "consequences"

Severity
- the severity of the consequence of a hazardous event
  - units depend on type of consequence
  - e.g. no. of fatalities, dollars, …

Likelihood
- the probability of a consequence of a given event in a given time period
- may be expressed as a "frequency"

Risk
- the expected value of loss
- i.e. the combination of "likelihood" and "severity" of event consequence

Risk Reduction



Safety Integrity Levels

Target failure measures for a safety function, part of an E/E/PE safety-related system

TABLE 2: SAFETY INTEGRITY LEVELS: TARGET FAILURE MEASURES

SAFETY INTEGRITY LEVEL (SIL)	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Demand or continuous mode of operation?

IEC 61511-1 Ed.2 3.2.39

a) Low demand mode: … where the SIF is only performed on demand … and where the frequency of demands is no greater than one per year

- Failure Measure: Average Probability of Failure on Demand (PFD_{avg})
- IEC 60079.29.3 allows Low Demand mode > once per year

or

b) High demand mode: … where the SIF is only performed on demand … and where the frequency of demands is greater than one per year

- Failure Measure: Probability of Dangerous Failure per Hour (PFH)

or

Continuous mode: … where the SIF retains the process in a safe state as part of normal operation

- Failure Measure: Probability of Dangerous Failure per Hour (PFH)

Examples - car

Low Demand mode
- airbags

High Demand Mode
- brakes

Continuous Mode
- steering

Safety Integrity Level vs. Risk Reduction

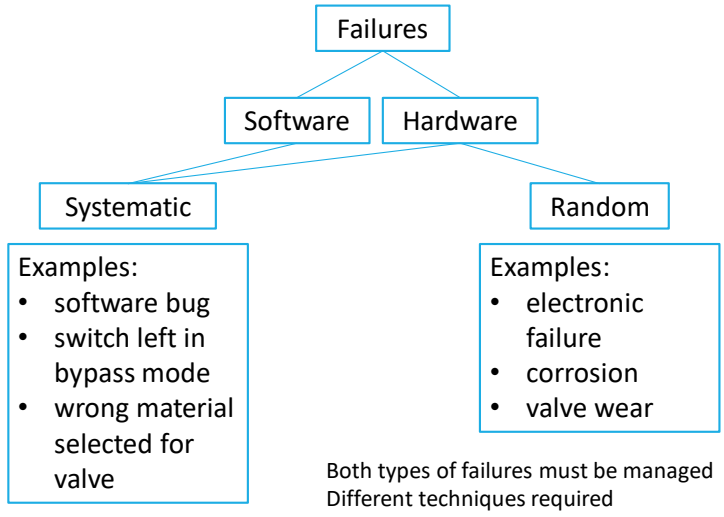
SIL	Risk Reduction Factor (RRF)	Probability of Failure on Demand (PFD_{avg})	Safety Availability
4	> 10,000	$\geq 10^{-5}$ < 10^{-4}	> 99.99%
3	> 1,000 ≤ 10,000	$\geq 10^{-4}$ < 10^{-3}	> 99.9 ≤ 99.99%
2	> 100 ≤ 1,000	$\geq 10^{-3}$ < 10^{-2}	> 99 ≤ 99.9%
1	> 10 ≤ 100	$\geq 10^{-2}$ < 10^{-1}	> 90 ≤ 99%
BPCS*	≤ 10	$\geq 10^{-1}$	≤ 90%
	$= 1 / PFD_{avg}$	$= 1 / RRF$	$= 100(1 - PFD_{avg})$

Used to specify SIL required — Used to specify SIL achieved

* Basic Process Control System

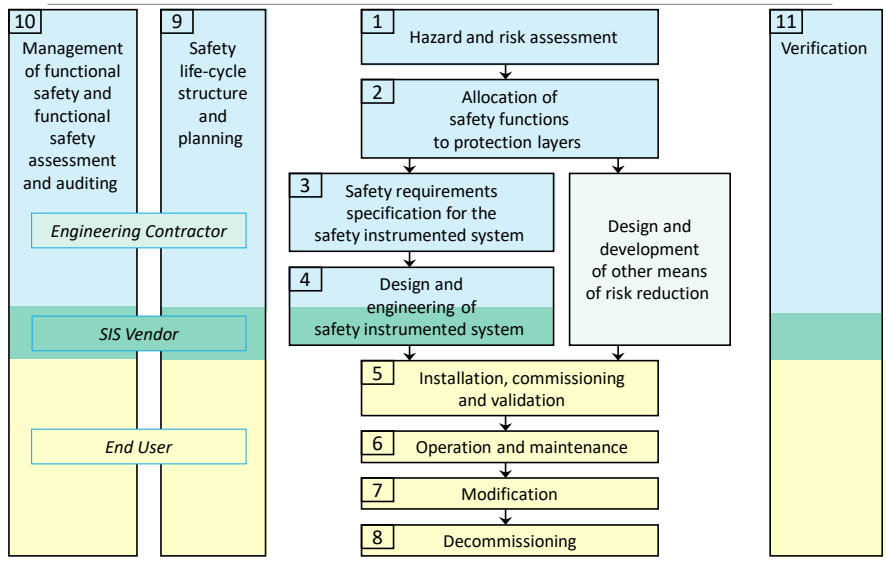
For Low Demand Mode SIFs only

Different failure types



Both types of failures must be managed
Different techniques required

Functional Safety Lifecycle – IEC 61511



Complying with IEC 61511

Target SIL must be specified for each SIF based on hazard and risk analysis

Processes for SIS throughout lifecycle must comply

Each SIF must meet target SIL requirements for

- random failure rate (PFD_{avg})
- Hardware Fault Tolerance (architectural constraints)
- Systematic Capability for each component
  - Field devices, logic solver, shutdown valves etc.

Not just "TÜV certification"

- though it helps !

Not just meeting PFD_{avg} target

Summary

Overview of IEC 61511 & key concepts

Key terminology and concepts

Functional Safety

Safety Instrumented System (SIS)

- implements . . .

Safety Instrumented Functions (SIFs)

- which each have a . . .

Safety Integrity Level (SIL)

- a measure of the risk reduction of the SIF and hence the "reliability" required
- Systematic and Random Failures

Functional Safety Lifecycle

How to comply

Questions?