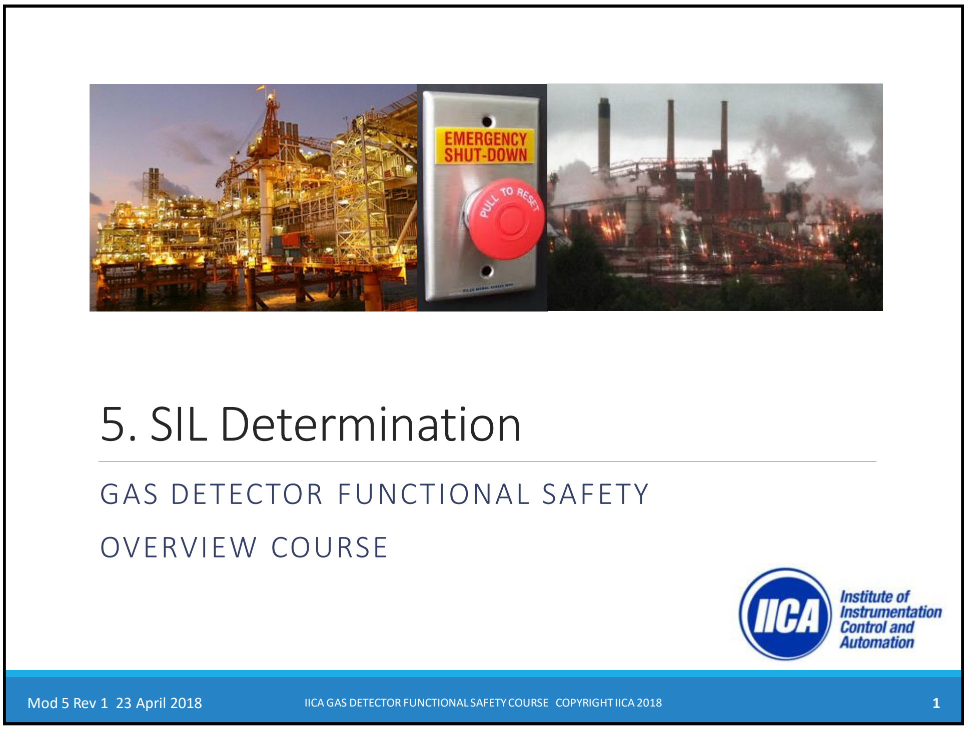
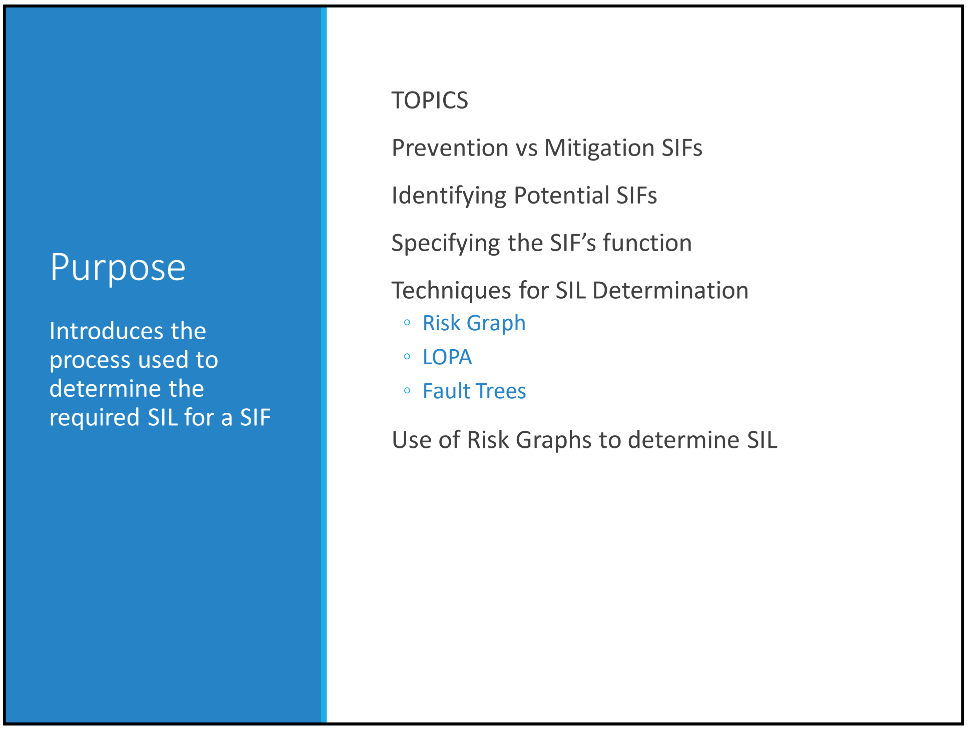

EMERGENCY
SHUT-DOWN
PULL TO RESET

5. SIL Determination

GAS DETECTOR FUNCTIONAL SAFETY OVERVIEW COURSE

IICA Institute of Instrumentation Control and Automation



Purpose

Introduces the process used to determine the required SIL for a SIF

TOPICS

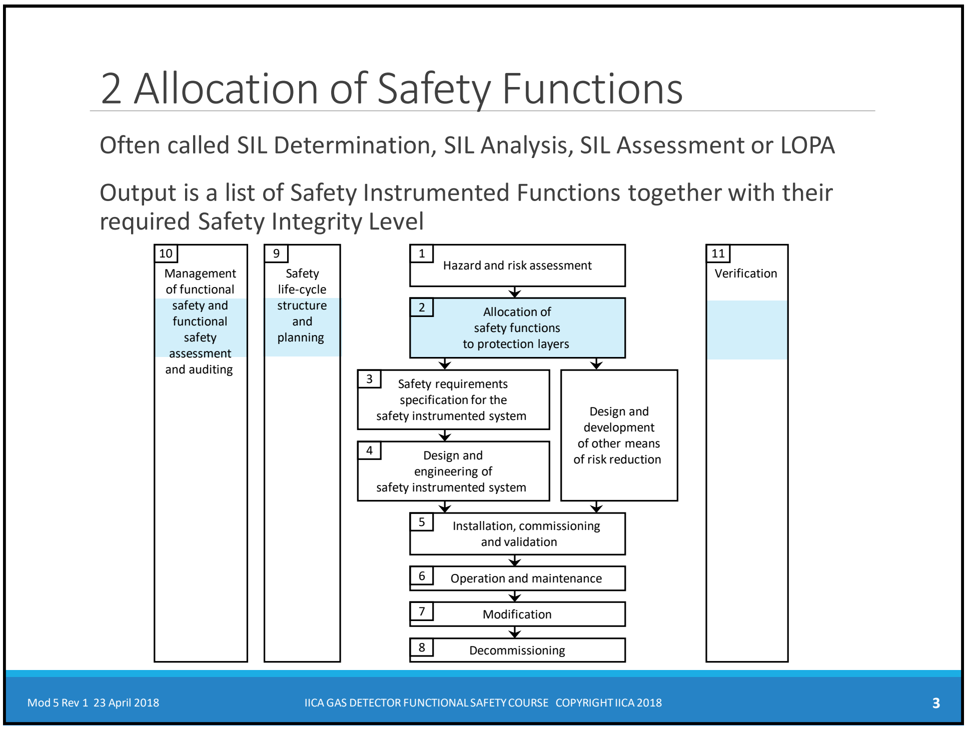
Prevention vs Mitigation SIFs

Identifying Potential SIFs

Specifying the SIF's function

Techniques for SIL Determination
- Risk Graph
- LOPA
- Fault Trees

Use of Risk Graphs to determine SIL



2 Allocation of Safety Functions

Often called SIL Determination, SIL Analysis, SIL Assessment or LOPA

Output is a list of Safety Instrumented Functions together with their required Safety Integrity Level

10 Management of functional safety and functional safety assessment and auditing

9 Safety life-cycle structure and planning

1 Hazard and risk assessment

2 Allocation of safety functions to protection layers

3 Safety requirements specification for the safety instrumented system

4 Design and engineering of safety instrumented system

Design and development of other means of risk reduction

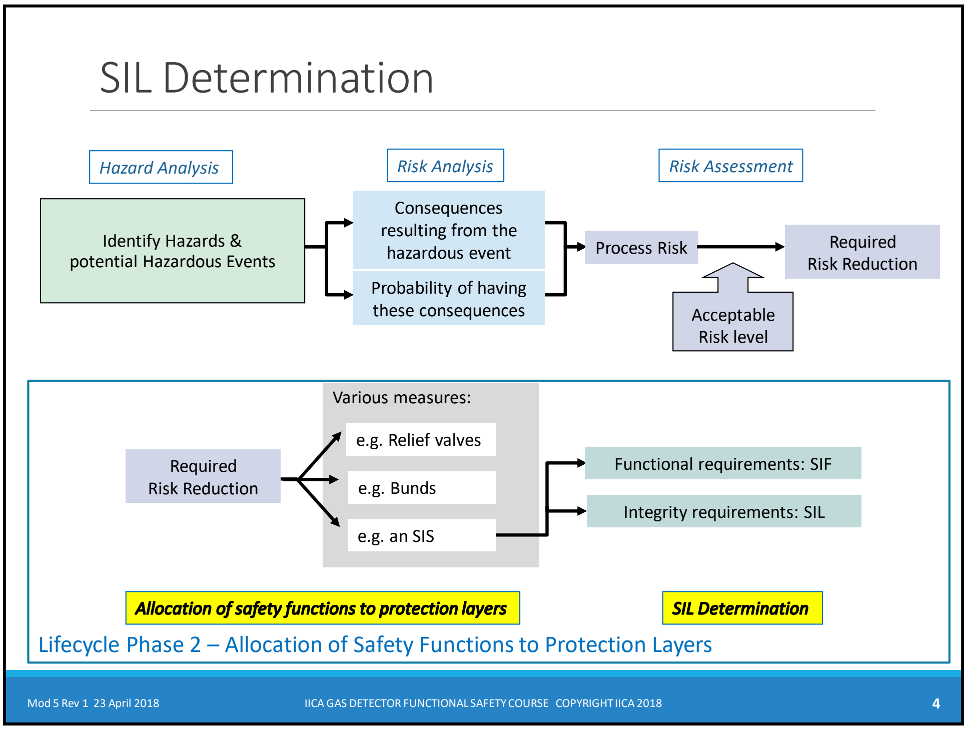
5 Installation, commissioning and validation

6 Operation and maintenance

7 Modification

8 Decommissioning

11 Verification



SIL Determination

Hazard Analysis

Risk Analysis

Risk Assessment

Identify Hazards & potential Hazardous Events

Consequences resulting from the hazardous event

Probability of having these consequences

Process Risk

Required Risk Reduction

Acceptable Risk level

Required Risk Reduction

Various measures:

e.g. Relief valves

e.g. Bunds

e.g. an SIS

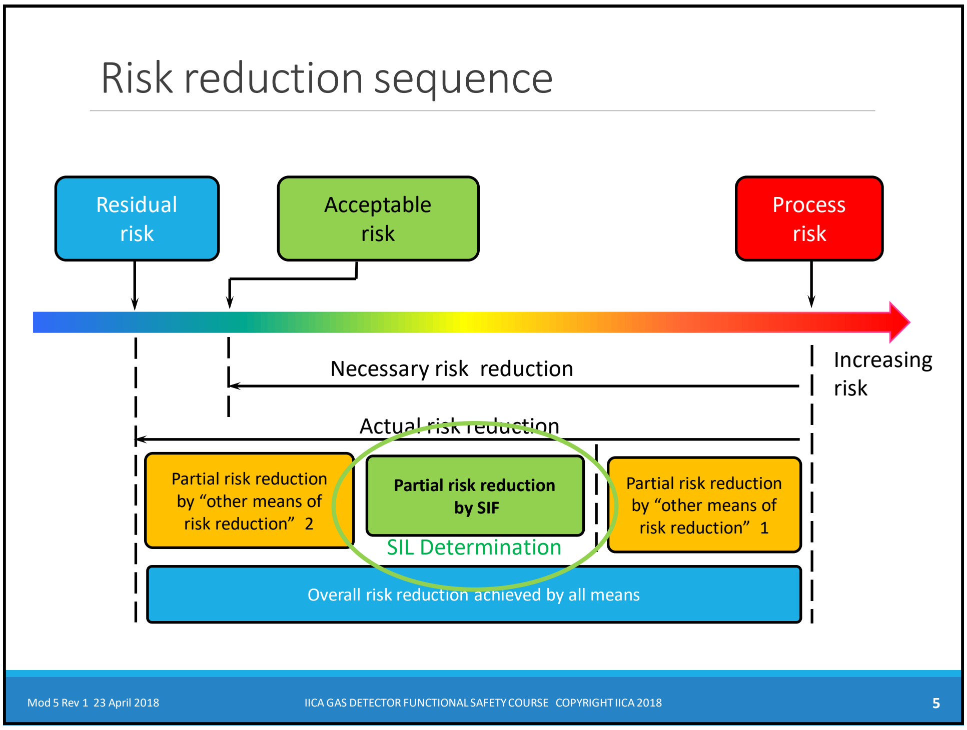
Functional requirements: SIF

Integrity requirements: SIL

Allocation of safety functions to protection layers

SIL Determination

Lifecycle Phase 2 – Allocation of Safety Functions to Protection Layers



Risk reduction sequence

Residual risk

Acceptable risk

Process risk

Increasing risk

Necessary risk reduction

Actual risk reduction

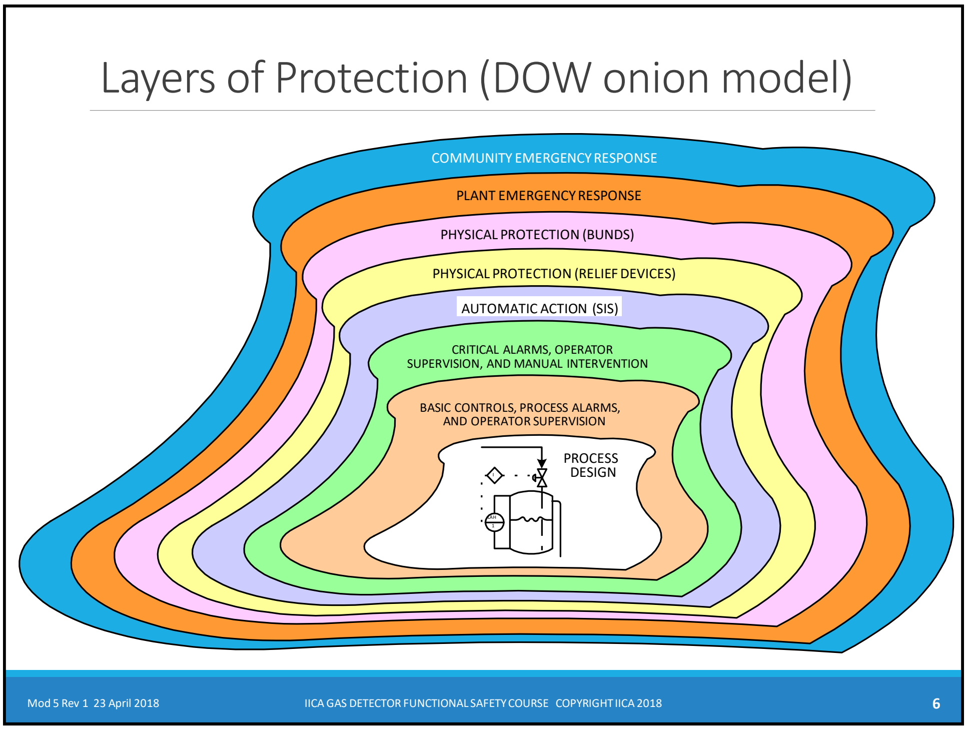
Partial risk reduction by "other means of risk reduction" 2

Partial risk reduction by SIF

SIL Determination

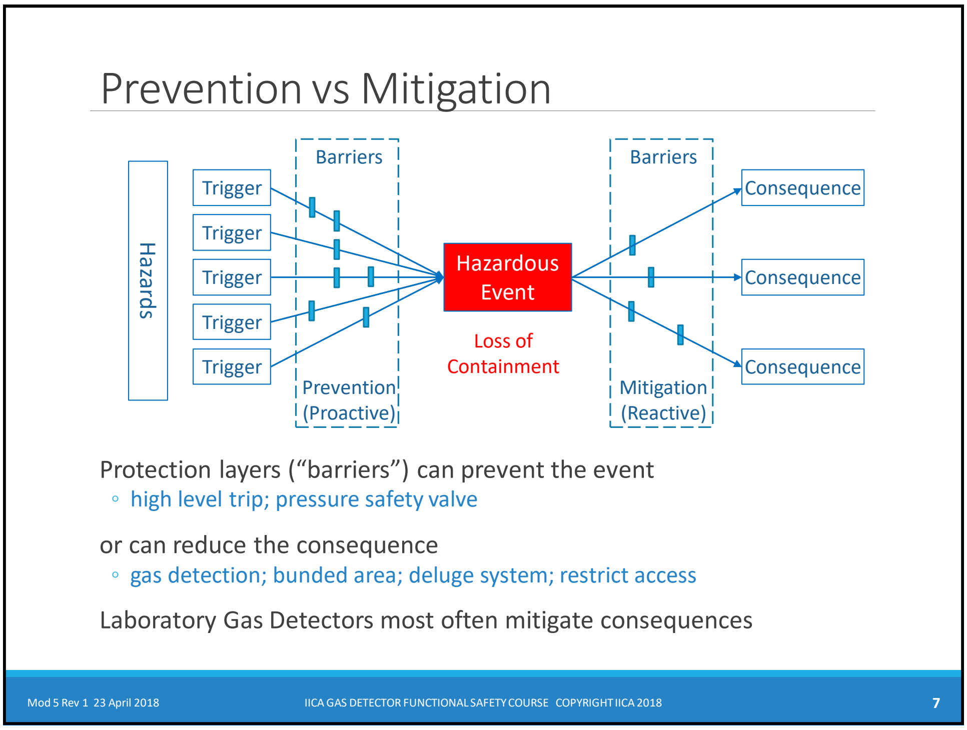
Partial risk reduction by "other means of risk reduction" 1

Overall risk reduction achieved by all means



Layers of Protection (DOW onion model)

COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY RESPONSE
PHYSICAL PROTECTION (BUNDS)
PHYSICAL PROTECTION (RELIEF DEVICES)
AUTOMATIC ACTION (SIS)
CRITICAL ALARMS, OPERATOR SUPERVISION, AND MANUAL INTERVENTION
BASIC CONTROLS, PROCESS ALARMS, AND OPERATOR SUPERVISION
PROCESS DESIGN



Prevention vs Mitigation

Hazards

Trigger
Trigger
Trigger
Trigger
Trigger

Barriers

Prevention (Proactive)

Hazardous Event

Loss of Containment

Barriers

Mitigation (Reactive)

Consequence
Consequence
Consequence

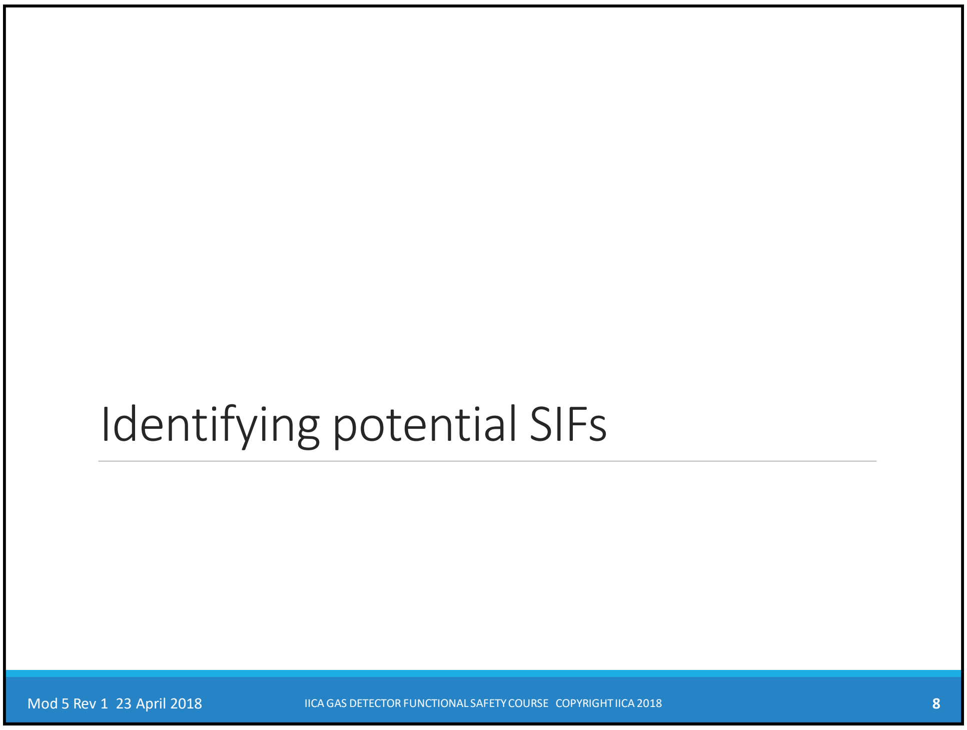
Protection layers ("barriers") can prevent the event

- high level trip; pressure safety valve

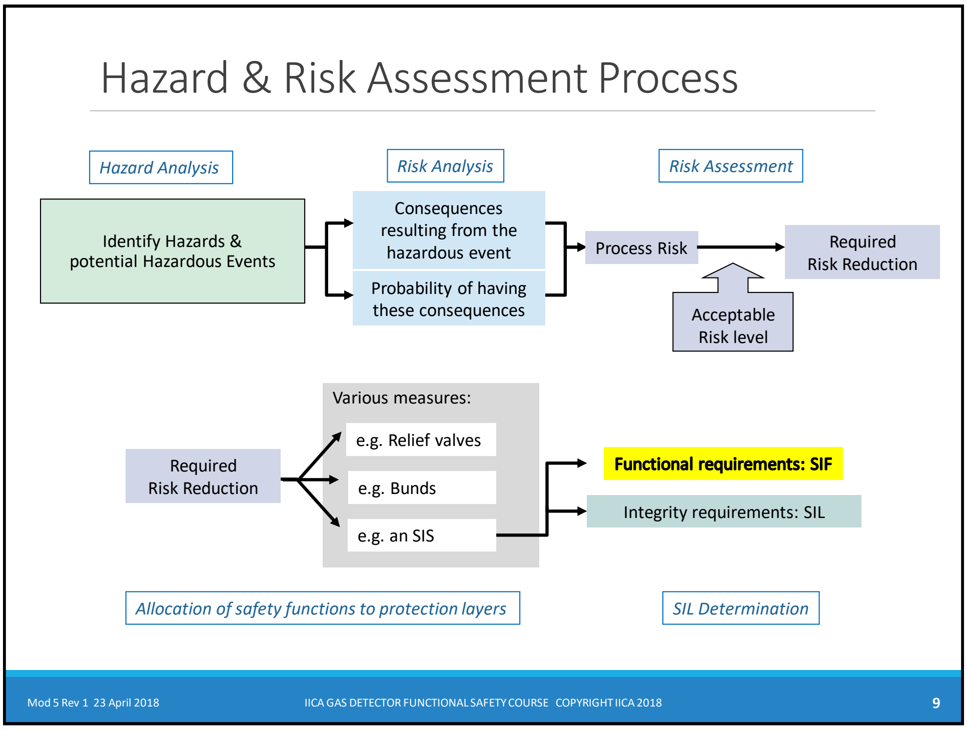
or can reduce the consequence

- gas detection; bunded area; deluge system; restrict access

Laboratory Gas Detectors most often mitigate consequences



Identifying potential SIFs



Hazard & Risk Assessment Process

Hazard Analysis

Identify Hazards & potential Hazardous Events

Risk Analysis

Consequences resulting from the hazardous event

Probability of having these consequences

Risk Assessment

Process Risk

Acceptable Risk level

Required Risk Reduction

Required Risk Reduction

Various measures:

e.g. Relief valves

e.g. Bunds

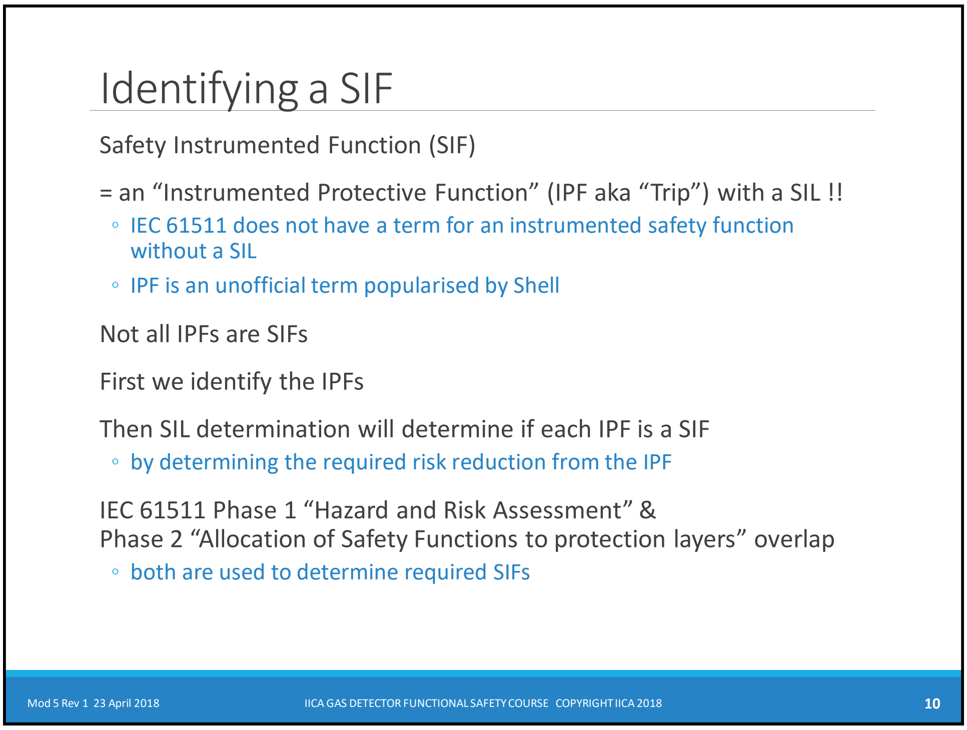
e.g. an SIS

Functional requirements: SIF

Integrity requirements: SIL

Allocation of safety functions to protection layers

SIL Determination



Identifying a SIF

Safety Instrumented Function (SIF)

= an “Instrumented Protective Function” (IPF aka “Trip”) with a SIL !!

- IEC 61511 does not have a term for an instrumented safety function without a SIL
- IPF is an unofficial term popularised by Shell

Not all IPFs are SIFs

First we identify the IPFs

Then SIL determination will determine if each IPF is a SIF

- by determining the required risk reduction from the IPF

IEC 61511 Phase 1 “Hazard and Risk Assessment” &
Phase 2 “Allocation of Safety Functions to protection layers” overlap

- both are used to determine required SIFs

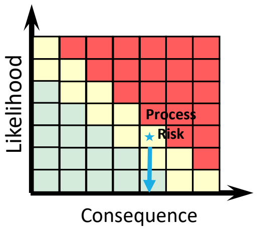
Case Study – Nitrogen SIF

Somehow we need to reduce risk

What could we do?

Let's decide to:

- measure ambient O_2 using gas detectors
- if O_2 very low isolate nitrogen supply & raise evacuation alarm



The automated isolation of the supply is a potential SIF

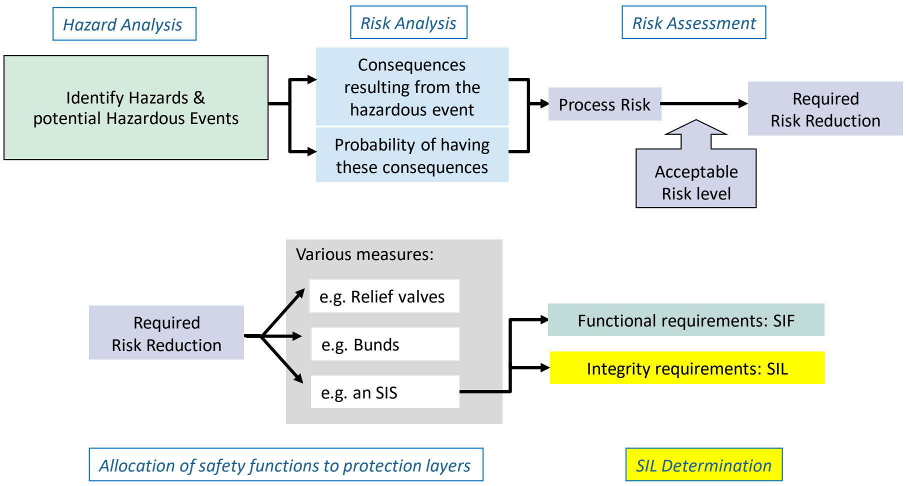
- Function: "If % O_2 < 17% then close nitrogen shut-off valve."

An alarm without automatic action should not normally be a SIF as human response is unreliable

To claim as an independent layer of protection, an alarm should be independent of the automated shutdown SIF

- e.g. use a separate sensor where possible

SIL Determination



Hazard Analysis

Identify Hazards & potential Hazardous Events

Risk Analysis

Consequences resulting from the hazardous event

Probability of having these consequences

Risk Assessment

Process Risk

Required Risk Reduction

Acceptable Risk level

Required Risk Reduction

Various measures:

e.g. Relief valves

e.g. Bunds

e.g. an SIS

Functional requirements: SIF

Integrity requirements: SIL

Allocation of safety functions to protection layers

SIL Determination

SIL Determination

Other Names

- SIL Assessment
- SIL Allocation
- SIL Classification
- SIL Selection
- LOPA
- . . .

<u>Not</u>

- SIL Verification

A team review process

- operations
- process
- control/instrumentation
- other subject matter experts as required

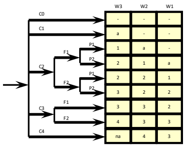
Experienced facilitator essential

- functional safety expert
- often a risk analyst or consultant

SIL Determination techniques

Risk Graph

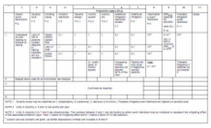
- qualitative or semi-quantitative
- a risk matrix with additional features
- particularly favoured in Europe



W3	W2	W1
-	-	-
a	-	-
1	a	-
2	1	a
2	2	1
3	2	2
3	3	2
4	3	3
na	4	3

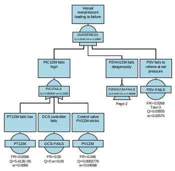
Layer of Protection Analysis (LOPA)

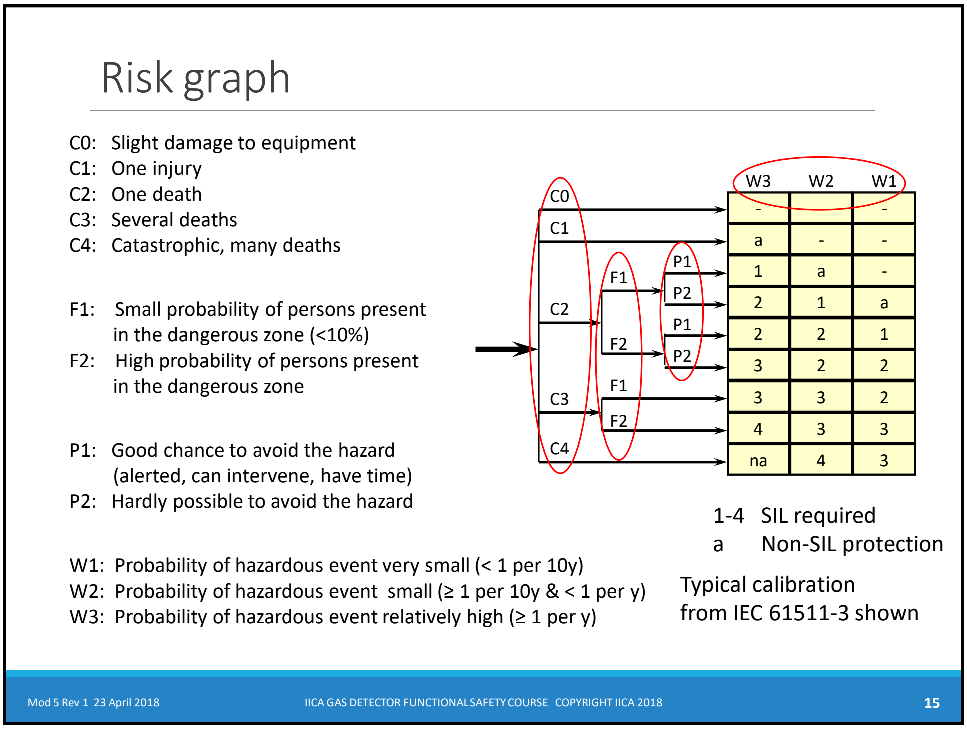
- semi-quantitative technique
- relies on simplified assumptions (e.g. independence of layers)
- most popular method today for process plants



Fault Tree Analysis (FTA)

- quantitative technique
- rigorous analysis
  - particularly if used with Markov Modelling
- needs specialist skills
- analyst prepares, for later team review





Risk graph

C0: Slight damage to equipment
C1: One injury
C2: One death
C3: Several deaths
C4: Catastrophic, many deaths

F1: Small probability of persons present in the dangerous zone (<10%)
F2: High probability of persons present in the dangerous zone

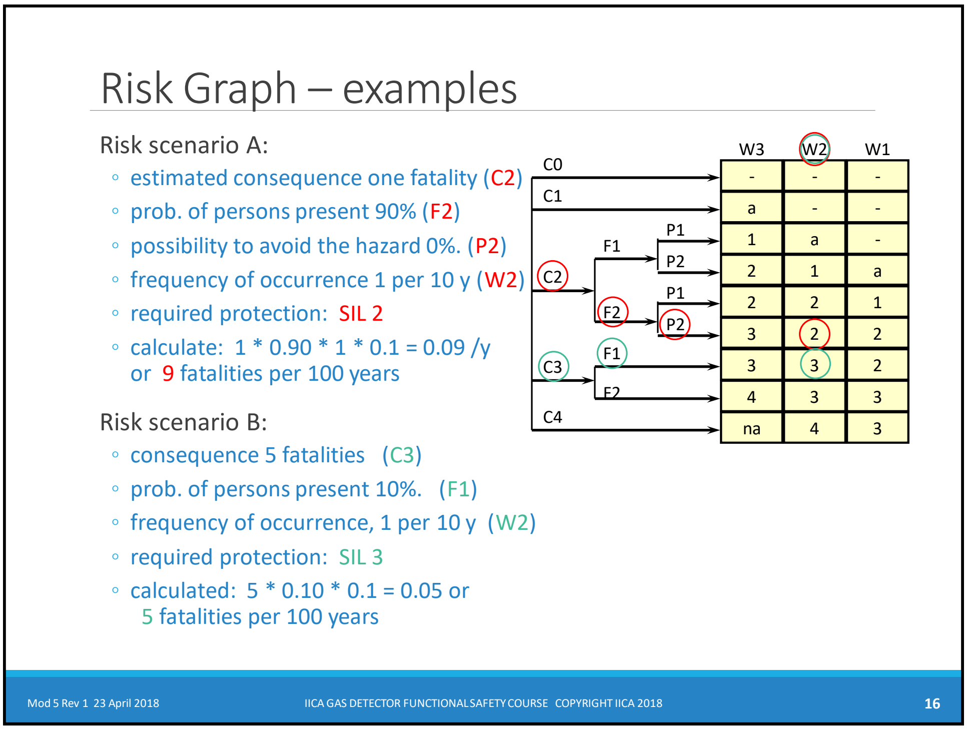
P1: Good chance to avoid the hazard (alerted, can intervene, have time)
P2: Hardly possible to avoid the hazard

W1: Probability of hazardous event very small (< 1 per 10y)
W2: Probability of hazardous event small (≥ 1 per 10y & < 1 per y)
W3: Probability of hazardous event relatively high (≥ 1 per y)

	W3	W2	W1
C0	-	-	-
C1	a	-	-
C2 F1 P1	1	a	-
C2 F1 P2	2	1	a
C2 F2 P1	2	2	1
C2 F2 P2	3	2	2
C3 F1	3	3	2
C3 F2	4	3	3
C4	na	4	3

1-4 SIL required
a Non-SIL protection

Typical calibration from IEC 61511-3 shown



Risk Graph – examples

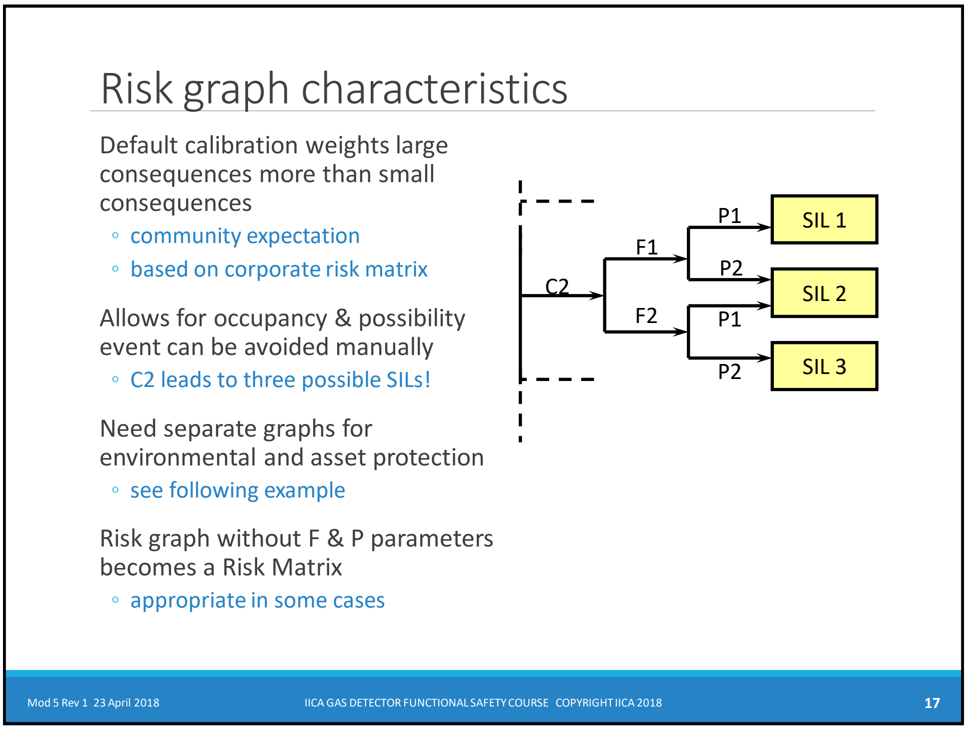
Risk scenario A:

- estimated consequence one fatality (C2)
- prob. of persons present 90% (F2)
- possibility to avoid the hazard 0%. (P2)
- frequency of occurrence 1 per 10 y (W2)
- required protection: SIL 2
- calculate: 1 * 0.90 * 1 * 0.1 = 0.09 /y or 9 fatalities per 100 years

Risk scenario B:

- consequence 5 fatalities (C3)
- prob. of persons present 10%. (F1)
- frequency of occurrence, 1 per 10 y (W2)
- required protection: SIL 3
- calculated: 5 * 0.10 * 0.1 = 0.05 or 5 fatalities per 100 years

	W3	W2	W1
C0	-	-	-
C1	a	-	-
C2 F1 P1	1	a	-
C2 F1 P2	2	1	a
C2 F2 P1	2	2	1
C2 F2 P2	3	2	2
C3 F1	3	3	2
C3 F2	4	3	3
C4	na	4	3



Risk graph characteristics

Default calibration weights large consequences more than small consequences

- community expectation
- based on corporate risk matrix

Allows for occupancy & possibility event can be avoided manually

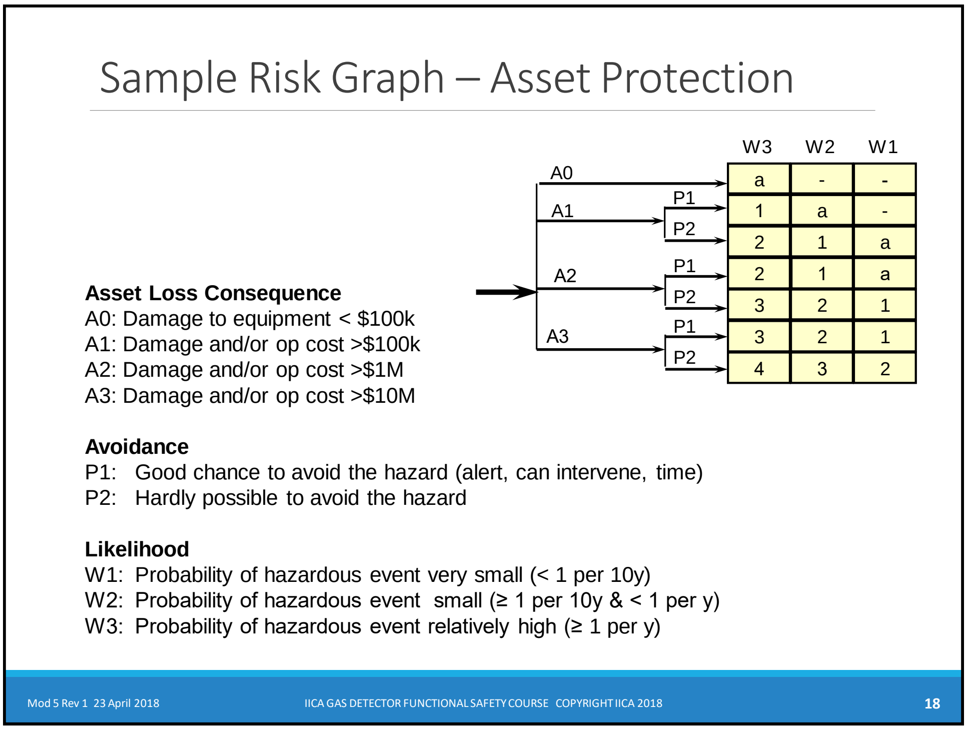
- C2 leads to three possible SILs!

Need separate graphs for environmental and asset protection

- see following example

Risk graph without F & P parameters becomes a Risk Matrix

- appropriate in some cases



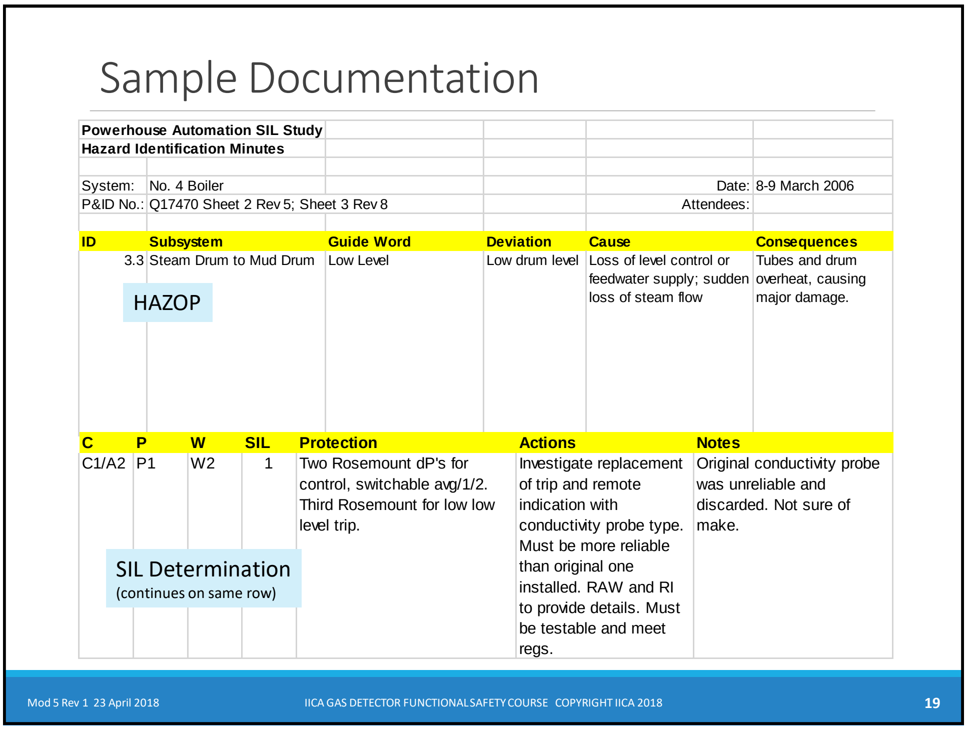
Sample Risk Graph – Asset Protection

		W3	W2	W1
A0		a	-	-
A1	P1	1	a	-
	P2	2	1	a
A2	P1	2	1	a
	P2	3	2	1
A3	P1	3	2	1
	P2	4	3	2

Asset Loss Consequence
A0: Damage to equipment < $100k
A1: Damage and/or op cost >$100k
A2: Damage and/or op cost >$1M
A3: Damage and/or op cost >$10M

Avoidance
P1: Good chance to avoid the hazard (alert, can intervene, time)
P2: Hardly possible to avoid the hazard

Likelihood
W1: Probability of hazardous event very small (< 1 per 10y)
W2: Probability of hazardous event small (≥ 1 per 10y & < 1 per y)
W3: Probability of hazardous event relatively high (≥ 1 per y)



Sample Documentation

Powerhouse Automation SIL Study
Hazard Identification Minutes

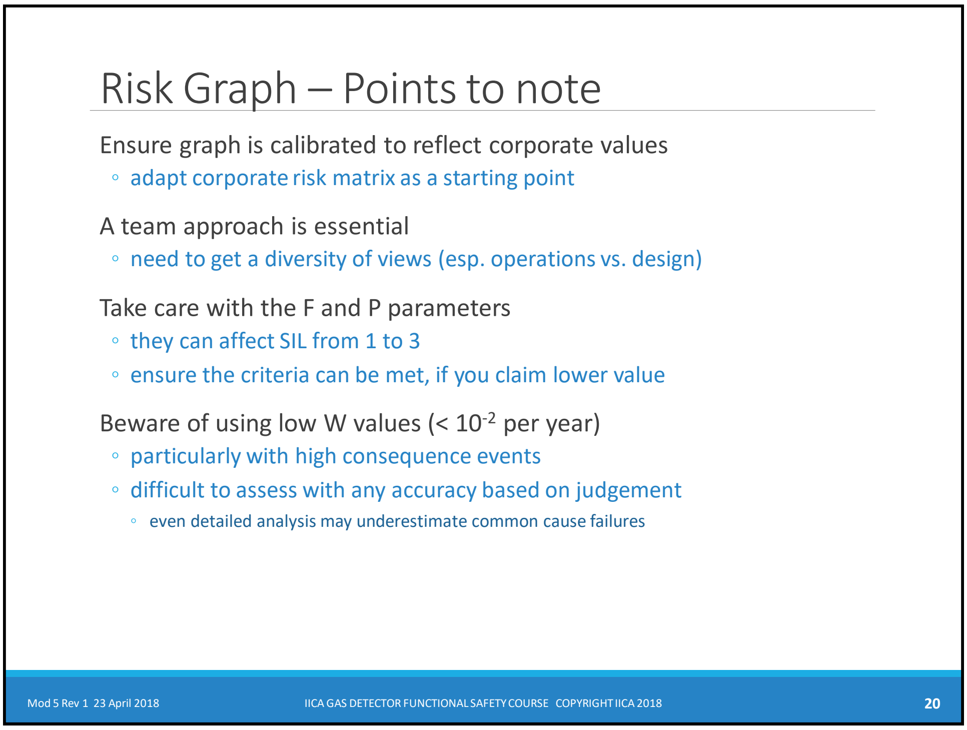
System:	No. 4 Boiler	Date:	8-9 March 2006
P&ID No.:	Q17470 Sheet 2 Rev 5; Sheet 3 Rev 8	Attendees:	

ID	Subsystem	Guide Word	Deviation	Cause	Consequences
3.3	Steam Drum to Mud Drum	Low Level	Low drum level	Loss of level control or feedwater supply; sudden loss of steam flow	Tubes and drum overheat, causing major damage.

HAZOP

C	P	W	SIL	Protection	Actions	Notes
C1/A2	P1	W2	1	Two Rosemount dP's for control, switchable avg/1/2. Third Rosemount for low low level trip.	Investigate replacement of trip and remote indication with conductivity probe type. Must be more reliable than original one installed. RAW and RI to provide details. Must be testable and meet regs.	Original conductivity probe was unreliable and discarded. Not sure of make.

SIL Determination
(continues on same row)



Risk Graph – Points to note

Ensure graph is calibrated to reflect corporate values
- adapt corporate risk matrix as a starting point

A team approach is essential
- need to get a diversity of views (esp. operations vs. design)

Take care with the F and P parameters
- they can affect SIL from 1 to 3
- ensure the criteria can be met, if you claim lower value

Beware of using low W values (< 10^{-2} per year)
- particularly with high consequence events
- difficult to assess with any accuracy based on judgement
  - even detailed analysis may underestimate common cause failures

Case Study – SIL Determination

Likely consequence:

- one fatality (C2)

Probability of persons present:

- normally occupied when nitrogen in use, so assume > 90% (F2)

Possibility to avoid the hazard

- if no independent warning alarm 0%. (P2)
- if independent warning alarm 90% (P1)

Frequency of occurrence

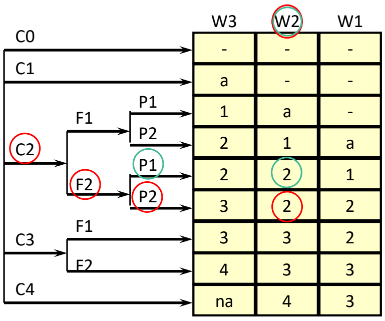
- frequency of leak > 1 per 10 y (W2)

Required protection

- SIL 2

Note if likely consequence >1 fatality need

- SIL 3
- unless occupied < 10% of time and frequency < 1 per 10y



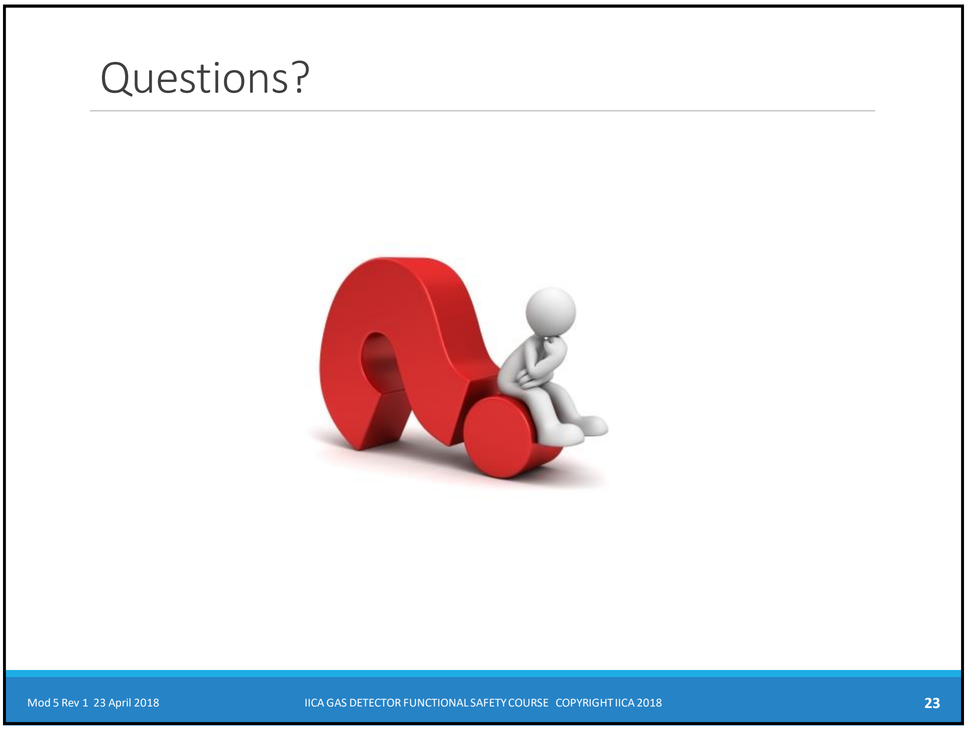
W3	W2	W1
-	-	-
a	-	-
1	a	-
2	1	a
2	2	1
3	2	2
3	3	2
4	3	3
na	4	3

Summary

The use of Risk Graphs for determining the required SIL

We have now decided:

1. We need a SIF
   - that protects against asphyxiation of personnel due to nitrogen leaks
2. The function the SIF needs to perform
   - “When % O_2 < 17% then close nitrogen shut-off valve.”
3. The required SIL of the SIF
   - SIL 2



Questions?

Mod 5 Rev 1 23 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 23