Safety Instrumentation – including Safety Integrity Levels (SILs)

by

Steve Mackay

www.idc-online.com www.eit.edu.au

EIT Micro-Course Series

- Every two weeks we present a 35 to 45 minute interactive course
- Practical, useful with Q&A throughout
- PID loop Tuning / Arc Flash Protection, Functional Safety, Troubleshooting conveyors presented so far
- Go to http://www.eit.edu.au/free-courses
- You get the recording and slides

www.idc-online.com www.eit.edu.au

Where are we now …….

Safety wise

It can't possibly happen to us ……….

Flixborough, England, June 1, 1974: "It was a still, warm, sunlit afternoon. One moment the teacups were tinkling and the kettles whistling. The next moment, a blast of nightmarish intensity as the giant plant blew up and blotted out the sun."--Humberside Police Report

Nypro Chemical Works, Flixborough, UK: 1 June, 1974

Cyclohexane vapour cloud ignited
Blast equivalent to 15 tons of TNT

28 killed

CAUSE:
Faulty temporary piping design by poorly qualified design team

Accident led to the Control of Industrial Major Accident (CIMAH) Regulations - now superseded by COMAH.

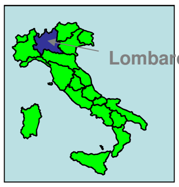
www.idc-online.com www.eit.edu.au

Lcmesa, Seveso, Italy 10 July 1976

1976
Trichlorophenol (TCP) is an intermediate used to produce the disinfectant hexachlorophene. Unexpected exothermic reaction caused pressure build-up and release of Dioxin by-product.

1983
41 barrels containing the toxic residues go missing and are eventually found and incinerated in late 1985

1995
Civil lawsuits still proceeding



CAUSE:
Management failure by all parties in the post-accident phase

Resulted in the Seveso I Directive that has influenced much subsequent legislation.

www.idc-online.com www.eit.edu.au

Three Mile Island, Pennsylvania 28 March 1979

#2 Reactor
No deaths or injuries

CAUSE:
Inadequate control room instrumentation and poor emergency response

The term 'cognitive overload' was born. Raised awareness of HMI issues.

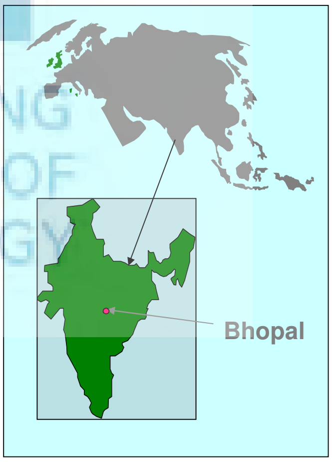
Bhopal, India Union Carbide 3 December, 1984

Dangerous chemical reaction occurred when a large amount of water got into the MIC storage tank #610

Exothermic reaction exploded the storage tank

40 tons of methyl isocyanate spread for 2 hours 8km down wind over the city of 900,000 inhabitants

More than 3,800 died and 11,000 disabled



CAUSE:
Management Failures + Disabled safety systems

Resulted in several governments passing legislation that required better accounting and disclosure of chemical inventories

TEXACO

Milford Haven, UK
24 July, 1994

Texaco Refinery

CAUSE:
Operators lacked adequate information on which to make decisions following an earlier incident. Contribution from Alarm Overload

Refer to the HSE report on this incident - ISBN 0 7176 1413 1

Sonat Exploration Company
(Now El Paso Production Co.)

Louisiana,
4 March, 1998

Catastrophic Vessel over-pressurisation

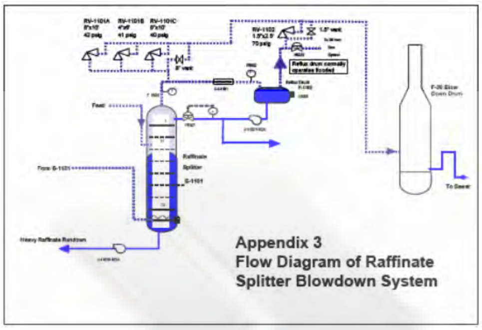
4 killed

CAUSE:
Maloperation of the plant, no plant operating procedures, inadequate vessel relief devices, and absence of any process hazard analysis (PHA) on the original plant design.

Source Chemical Safety and Hazard Investigation Board

BP Refiner, Texas City, Tx: 23 March, 2005

During the startup of the Isomerization Unit on Wednesday, March 23, 2005, explosions and fires occurred, killing fifteen and harming over 170 persons in the Texas City Refinery, operated by BP Products North America Inc.



www.idc-online.com www.eit.edu.au

BP Refinery, Texas City Tx: 23 March 2005

It can't possibly happen to us?

www.idc-online.com www.eit.edu.au

Safety System Basics

The Safety Instrumented System

General abbreviation: SIS

AKA: Trip system, shutdown system, instrumented protection system (IPS)

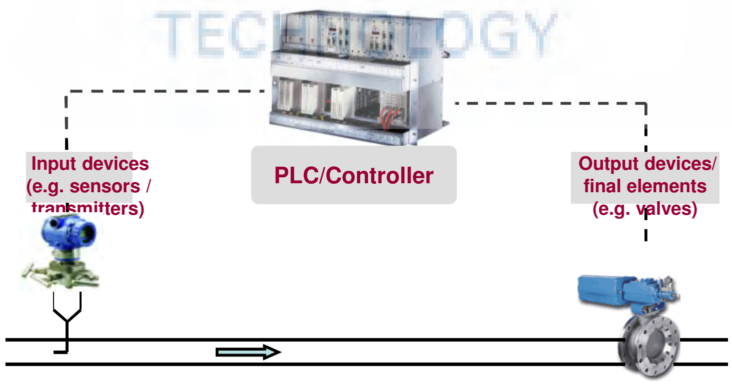
The SIS is an example of a Functional Safety System

Meaning: Safety depends on the correct functions being performed

Functional safety: Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers. (IEC 61511 clause: 3.2.25)

www.idc-online.com www.eit.edu.au EIT ENGINEERING INSTITUTE OF TECHNOLOGY

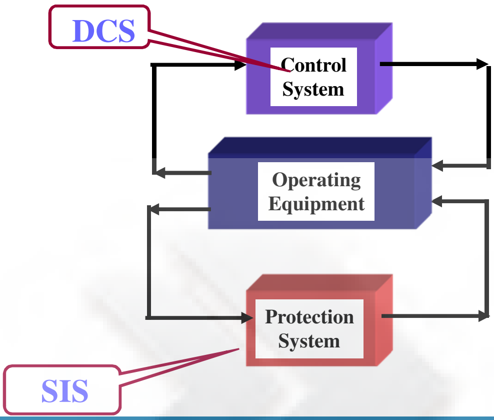
Hardware components of a Control Loop



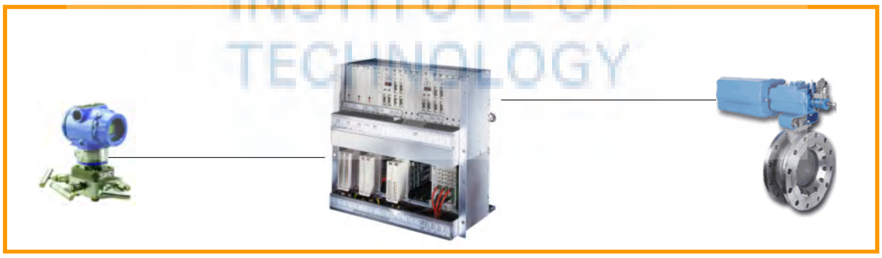
www.idc-online.com www.eit.edu.au EIT ENGINEERING INSTITUTE OF TECHNOLOGY

Process Control Versus Safety Control

Separation of safety controls from process controls

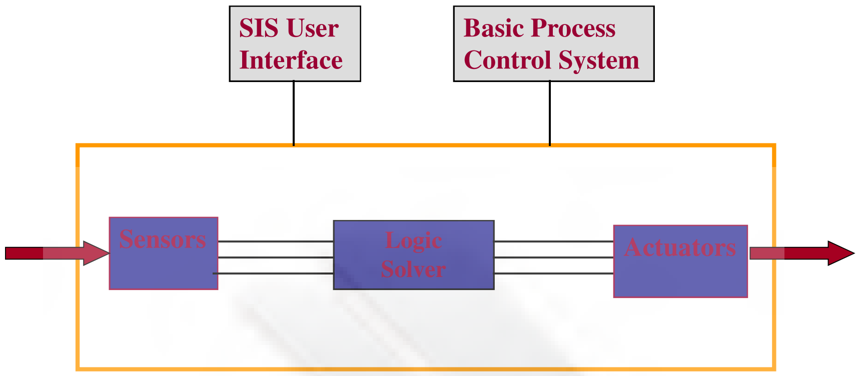


Scope of a Safety Instrumented System



Definition of a Safety Instrumented System

Fig 1.3

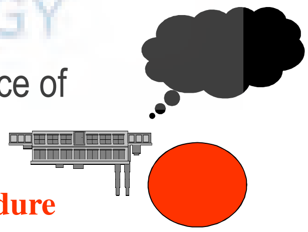


3 Sub-systems: Each subsystem must meet SIL target

www.idc-online.com www.eit.edu.au

Safety System Basics

- All types of safety measures are intended to reduce risk of harm to people, the environment and assets.
- The risks are due to the presence of HAZARDS:



Hazardous Process or Procedure

HAZARD:
An Inherent physical or chemical characteristic that has the potential for causing harm to people, property or the environment

www.idc-online.com www.eit.edu.au

What Is Hazard and What Is Risk?

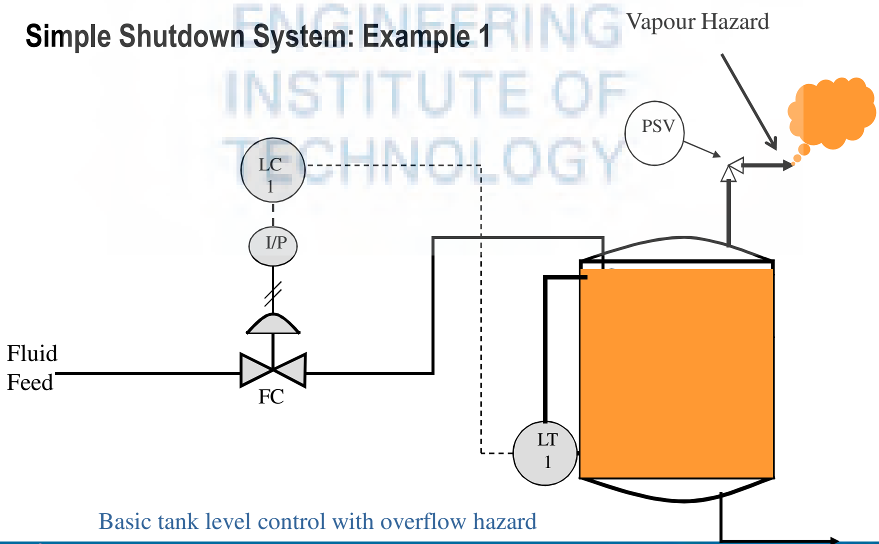
Hazard

An inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment.

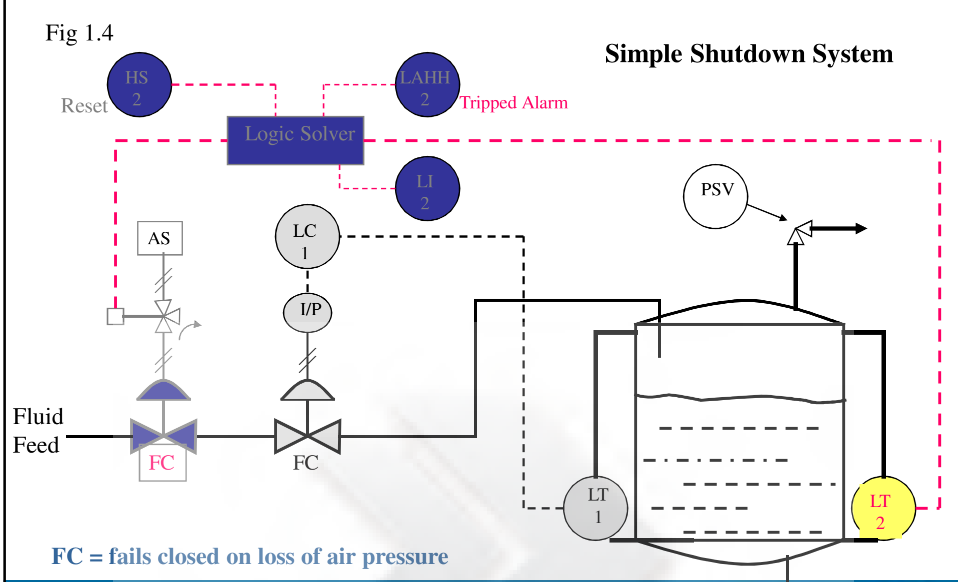
Risk

The combination of the severity and probability of an event.

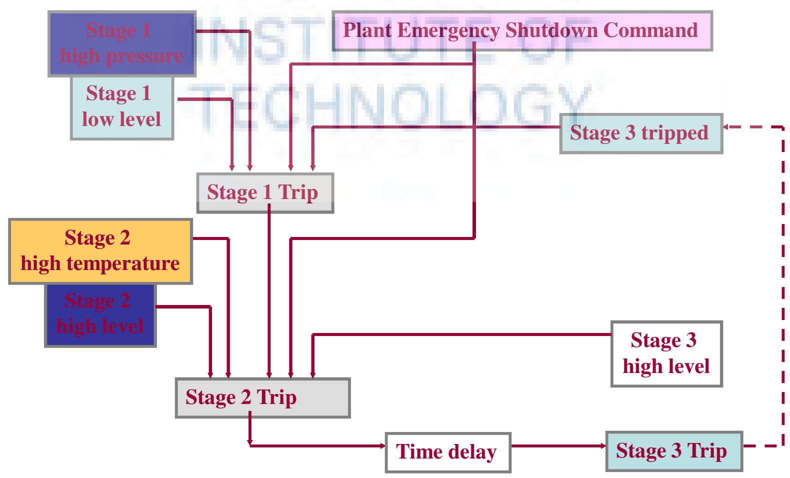
Simple Shutdown System: Example 1



Basic tank level control with overflow hazard



Typical multiple stage plant trip and ESD system



www.idc-online.com www.eit.edu.au

Fig 1.5

Risk reduction: the fast bowler

If we can't take away the hazard we shall have to reduce the risk.

Reduce the frequency and /or reduce the consequence.

Example:

Brett Lee is the bowler: He is the Hazard

You are the batsman: You are at risk

Frequency = 6 times per over. Consequence = Ouch!

Risk = 6 x Ouch!

Risk reduction: Limit bouncers to 2 per over. Wear more pads.

Risk = 2x ouch!

www.idc-online.com www.eit.edu.au

Measurement of Risk

Qualitative: High, Low, Moderate

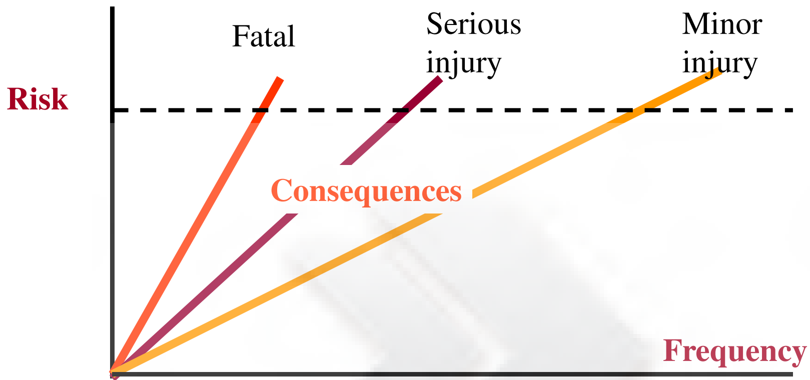
An effective measure if we all have the same understanding of the terms

Quantitative: 1 in 10 years x 5 people hurt

Effective if you can guess the numbers

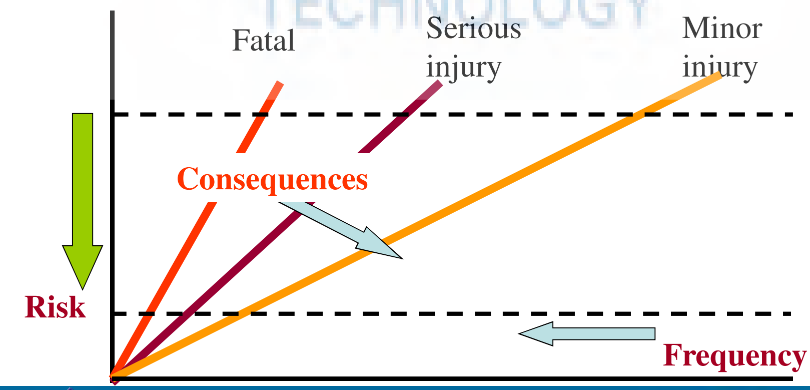
www.idc-online.com www.eit.edu.au

Risk = Frequency of Event x Consequence



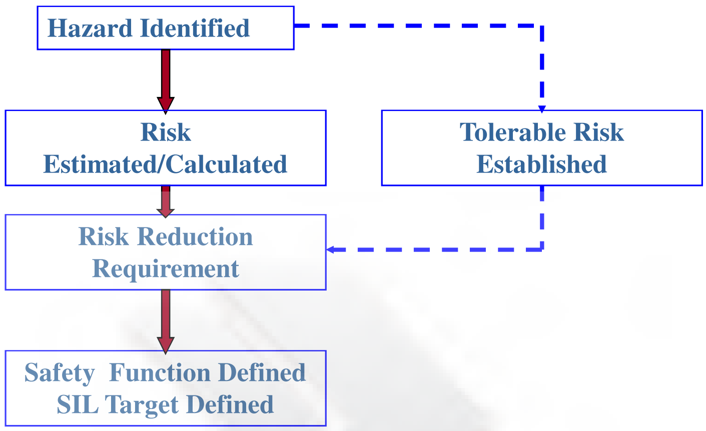
www.idc-online.com www.eit.edu.au

To Reduce Risk:
Reduce Frequency or Consequence or do both



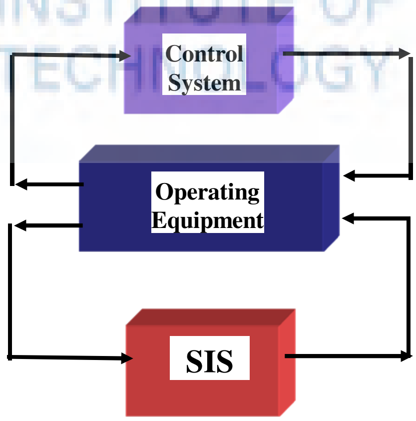
www.idc-online.com www.eit.edu.au

Risk Reduction: Design Principles



www.idc-online.com www.eit.edu.au

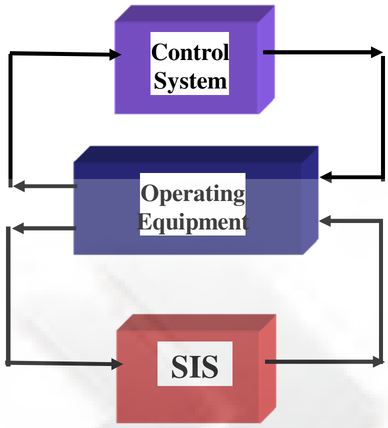
Safety Control systems act independently of the process or its control system to try to prevent a hazardous event.



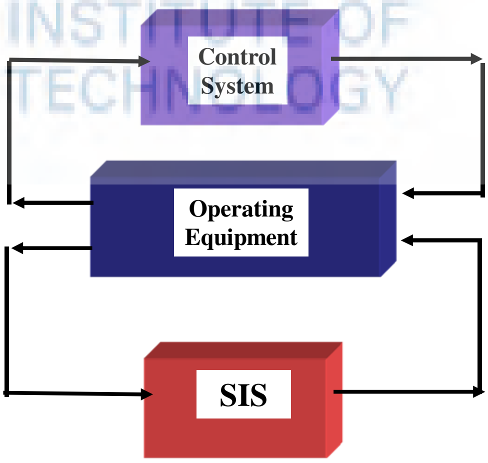
www.idc-online.com www.eit.edu.au

The SIS achieves risk reduction by reducing the frequency (likelihood) of the hazardous event

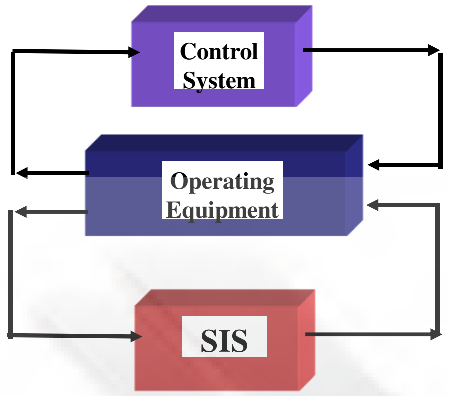
Fig 17



The amount of risk reduction achieved is indicated by the risk reduction factor: RRF



The amount of risk reduction allocated to the SIS determines its "target Safety Integrity Level" i.e. SIL



www.idc-online.com www.eit.edu.au

Fig 1.8

Safety Integrity Levels

SIL	RRF	Probability of Failure on Demand
4	>10 000 to < 100 000	$>10^{-5}$ to $<10^{-4}$
3	>1000 to < 10 000	$>10^{-4}$ to $<10^{-3}$
2	>100 to < 1 000	$>10^{-3}$ to $<10^{-2}$
1	>10 to < 100	$>10^{-2}$ to $<10^{-1}$

Safety Integrity Level defines the degree of confidence placed in the ability of a system to provide functional safety. SIL values also indicate the quality of care and attention taken to avoid systematic errors in design and maintenance.

www.idc-online.com www.eit.edu.au

Intuitively what does SIL mean?

- Statistical representations of integrity of SIS
- For example: SIL 1….
  - SIS with availability of 90% is acceptable
  - High level trip in a liquid tank
  - Availability of 90% (10% chance of failure)
  - One out of every 10 times the high level was reached, there would be a failure
  - Subsequent overflow 1 out of every 10 times.

www.idc-online.com www.eit.edu.au

Thank You For Your Interest

If you are interested in further training, please visit:

The Engineering Institute of Technologies
Online Certificate and
Advanced Diploma programs:

www.eit.edu.au

IDC Technologies
1, 2 & 3 day practical workshops, technical manuals,
onsite training & International conferences:

www.idc-online.com