Safety Systems 101

Understanding Safety Instrumented Systems

Bob Stahl

Honeywell

Today's Topics

- Functional Safety
- Safety Instrumented Systems
- Safety Instrumented Functions
- Layers of Protection Analysis
- Safety Integrity Level
- Risk Reduction Factor

What is Safety?

- Freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly as a result of damage to property or the environment

Functional Safety

Honeywell

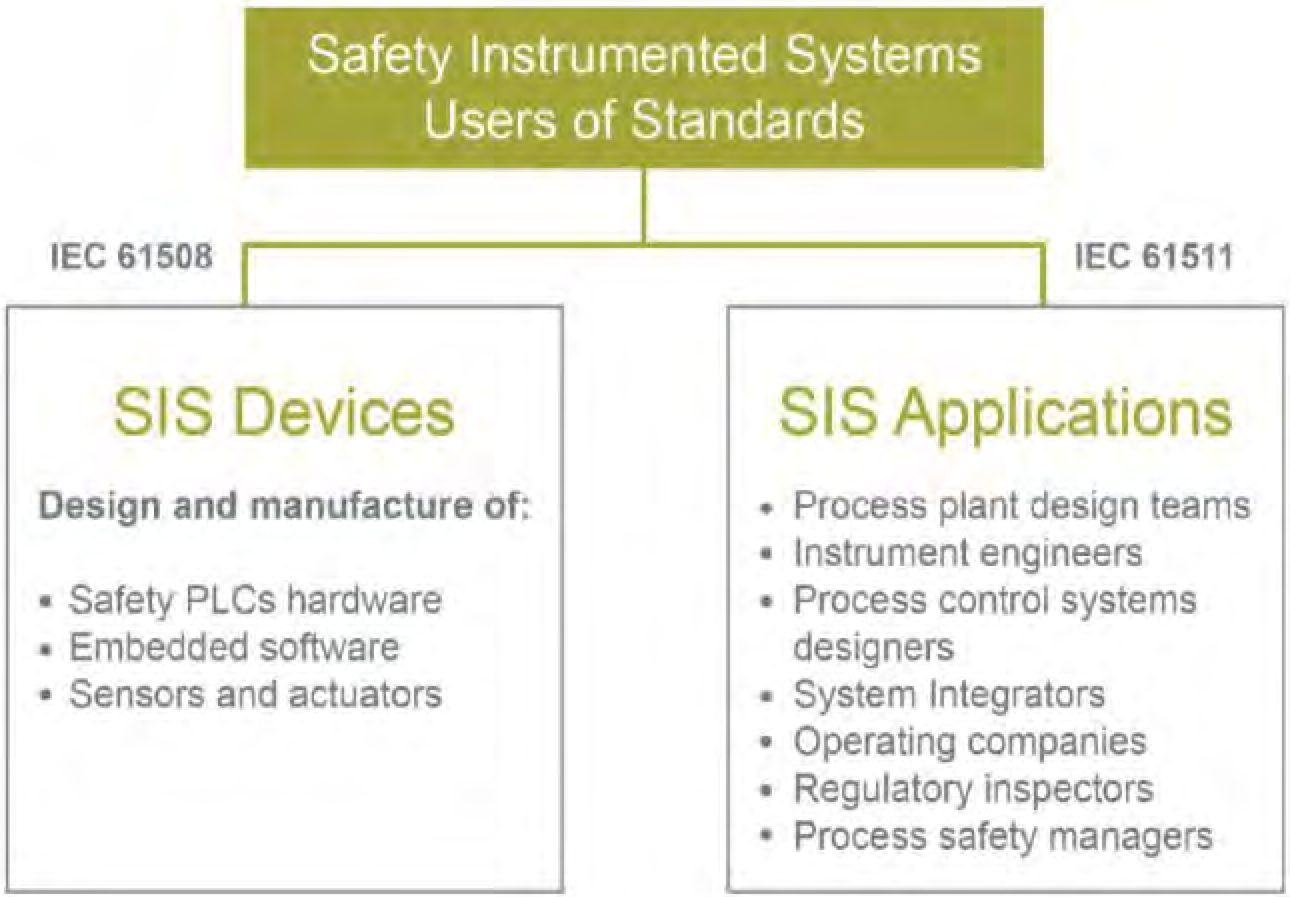
- Functional Safety is part of the overall safety of the equipment under control that depends on a system or equipment operating correctly in response to its inputs
- Functional Safety relies on active systems

Functional Safety Standards

- IEC 61508 is a standard written with an intent to help design and develop products which are SIL rated for any industry
- IEC 61511 and ISA84.01 are almost identical standards which have been written to help analyze, design, realize, install, commission and maintain SIL loops for the process industry

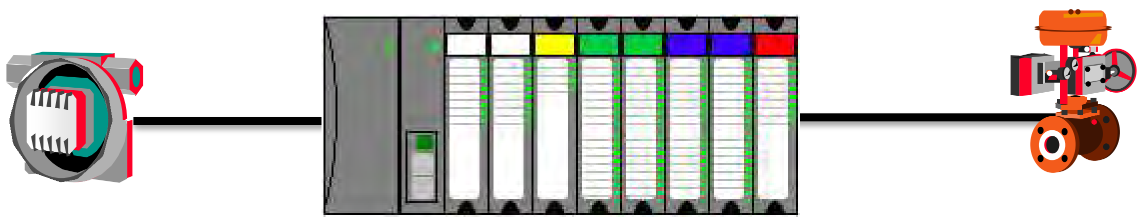
Which Standard to Use?

Honeywell

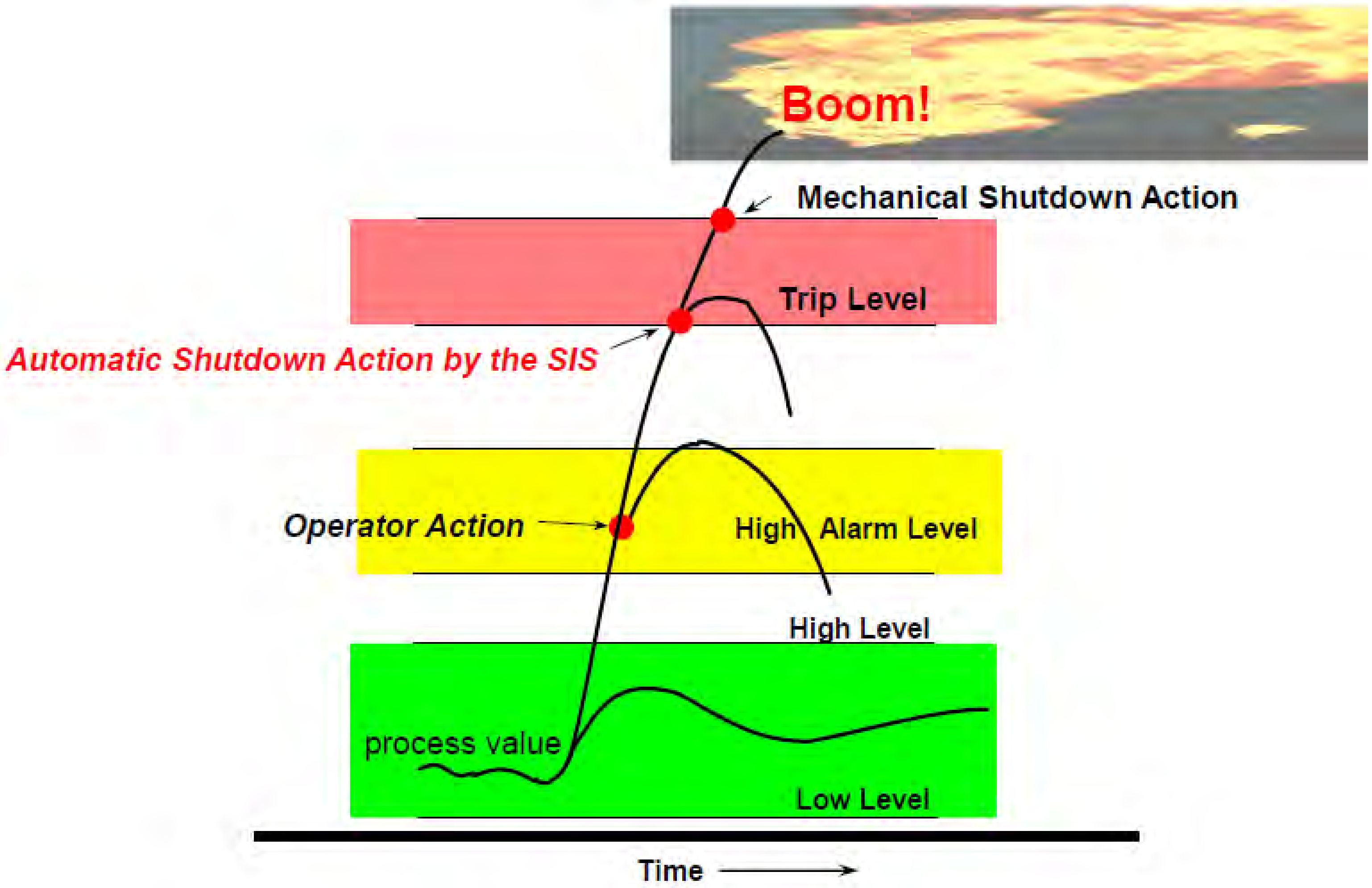


What is a Safety Instrumented System?

- An SIS is composed of any combination of
  - Sensors
  - Logic Solvers
  - Final Elements



What an SIS Does

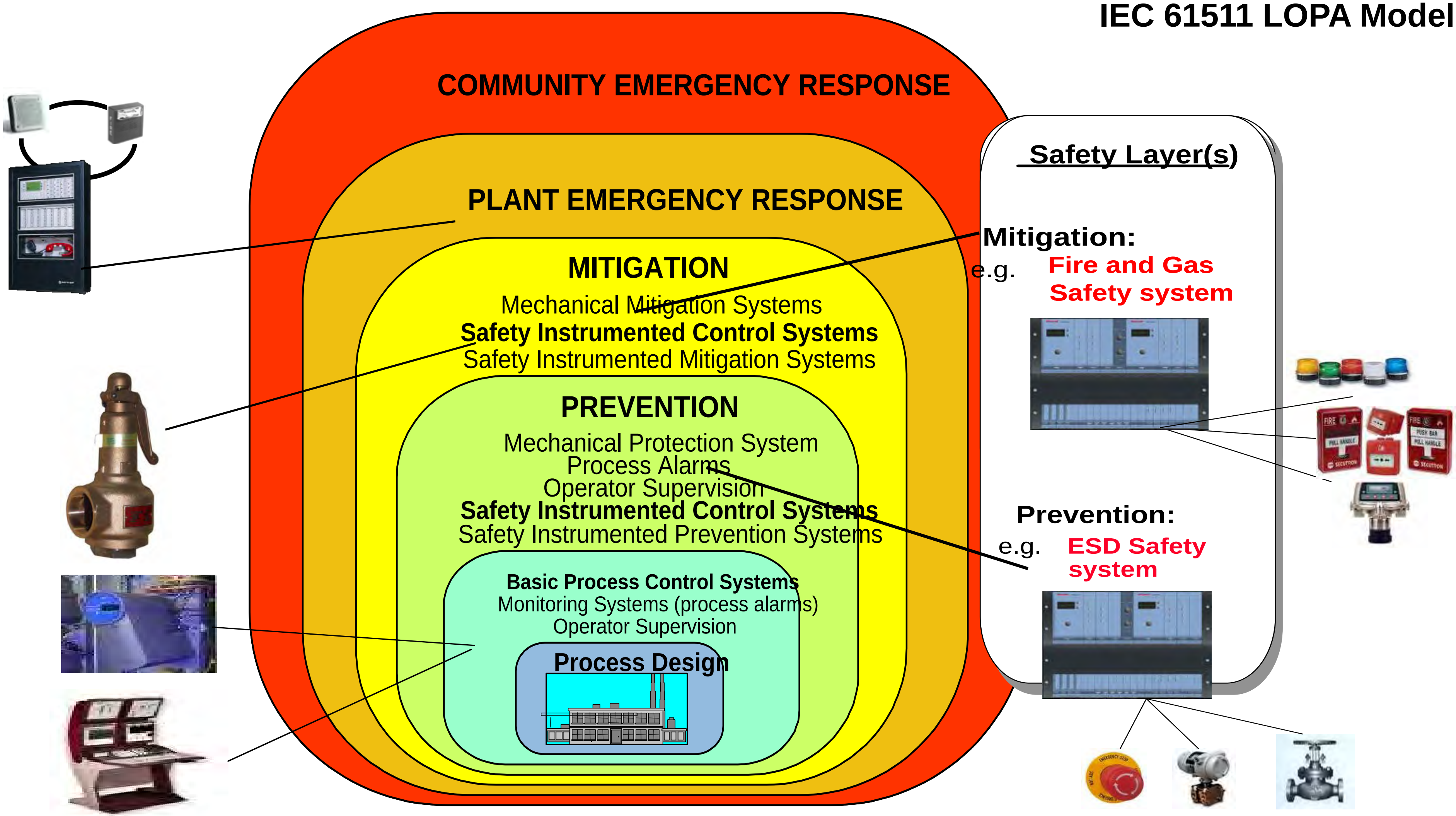


Types of SIS

- Safety Related Systems
- Safety Interlocks
- Emergency Shutdown Systems (ESD)
- Fire & Gas Systems (F&G)
- Instrumented Protective Systems (IPS)
- Burner Management Systems (BMS)
- High Integrity Pressure Protection System (HIPPS)

Layers of Protection

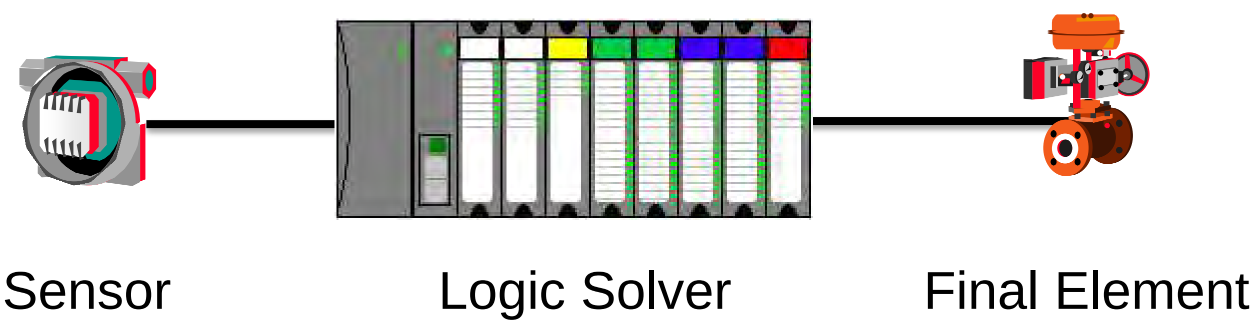
IEC 61511 LOPA Model



What is a SIF?

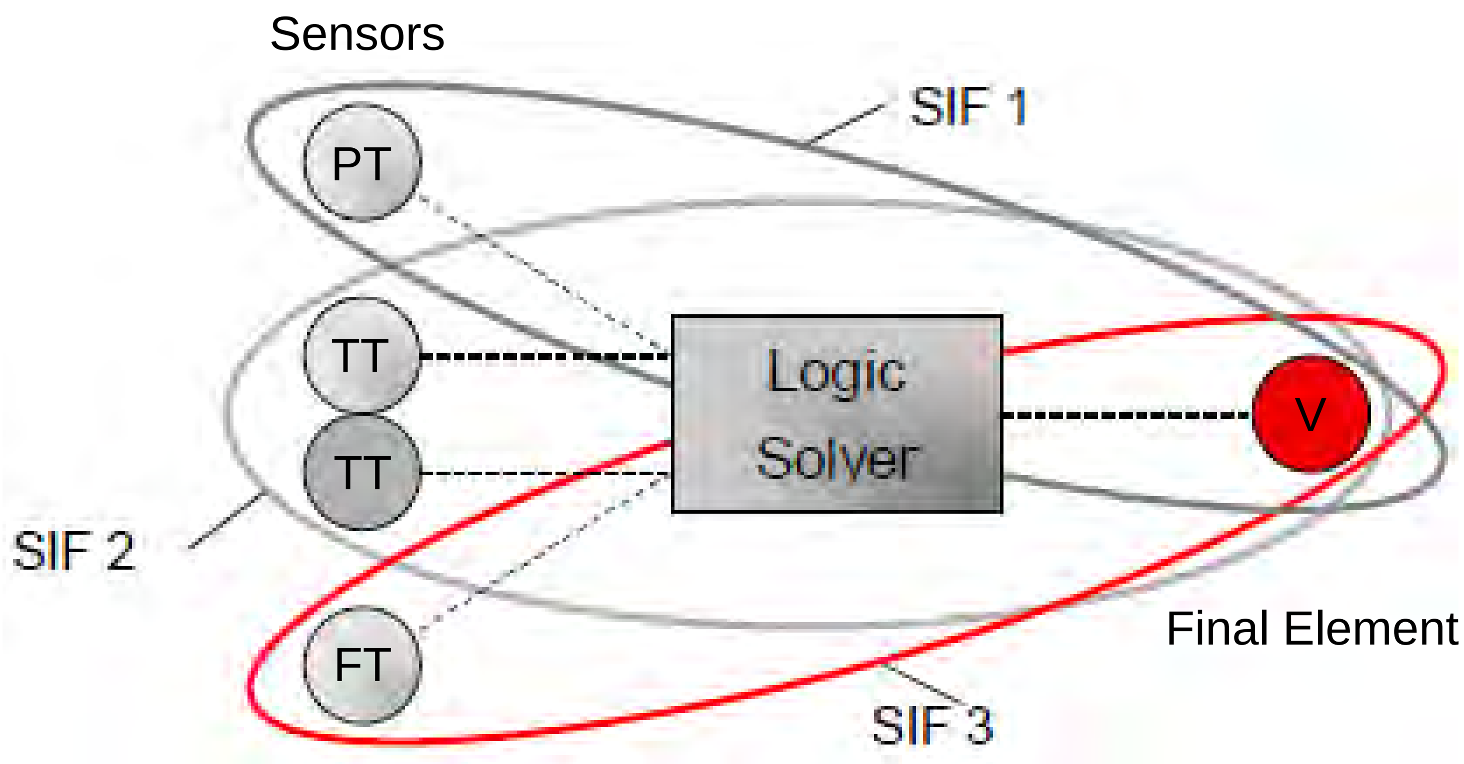
Honeywell

- Stands for Safety Instrumented Function
  - Sensor
  - Logic Solver
  - Final Element



SIS Consists of Multiple SIFs

Honeywell



Safety Instrumented System

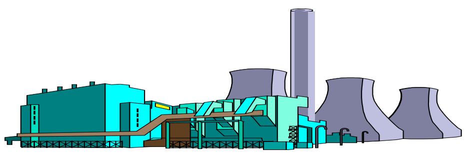
What is SIL?

Honeywell

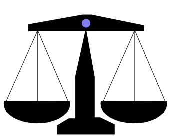
- Stands for Safety Integrity Level
- Quantifiable measurement of risk
- SIL applies only to a SIF
- IEC 61508 standard specifies 4 levels

Objectives of SIL Analysis

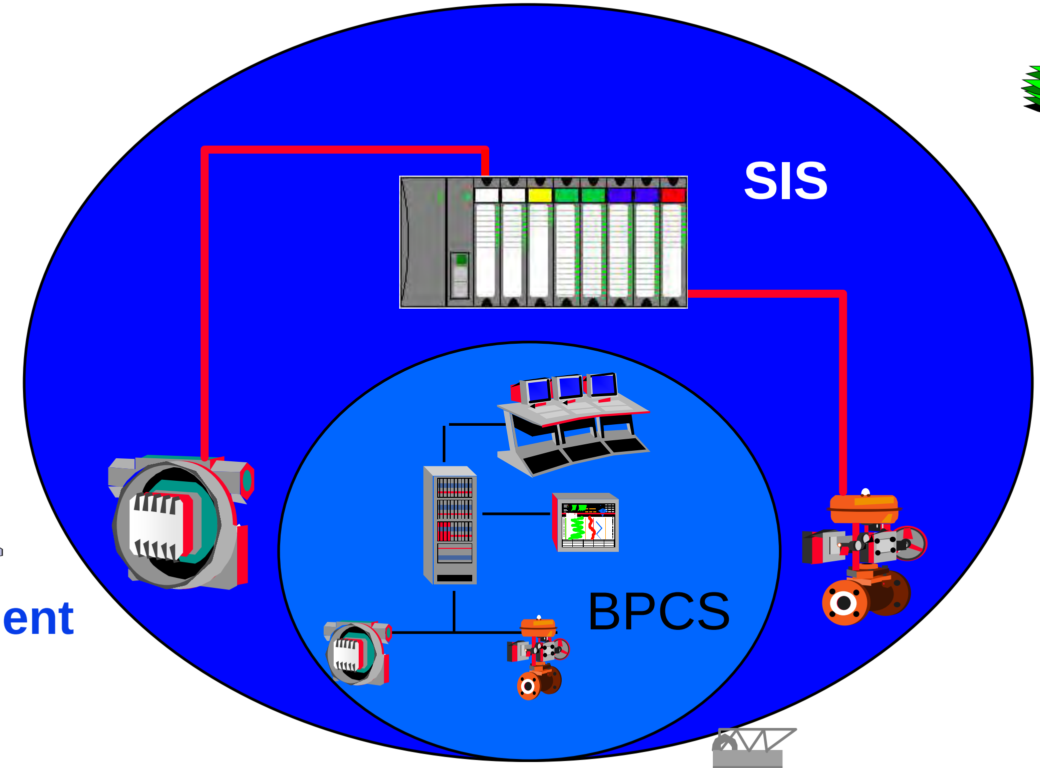
Personnel Safety

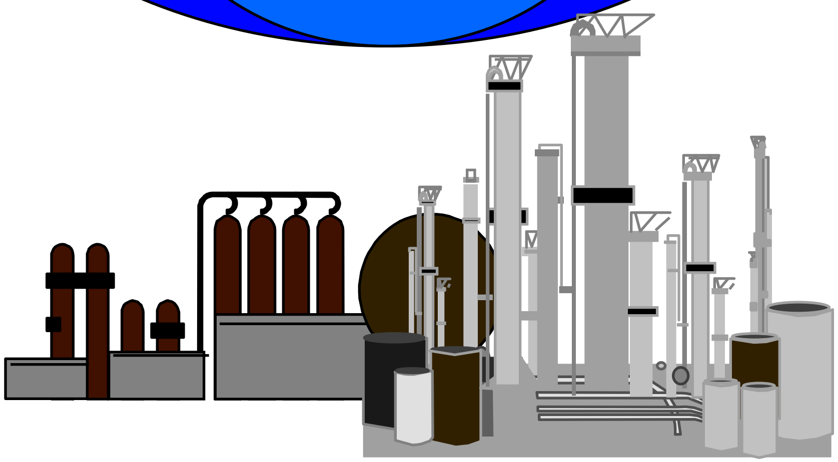


Protection of Equipment

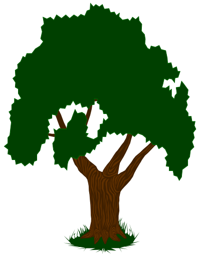


Protection from Litigation





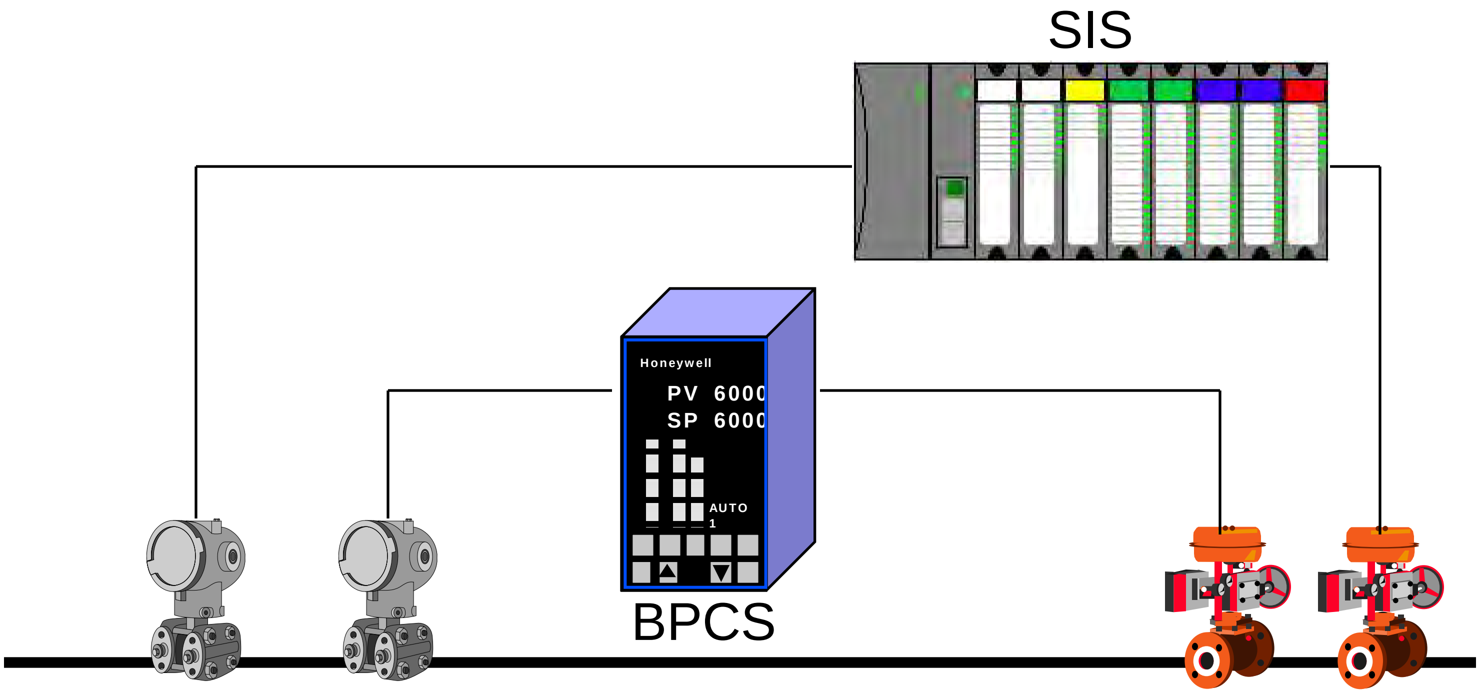
Profit



Environmental Safety

BPCS and ESD (SIS) Separated Solution

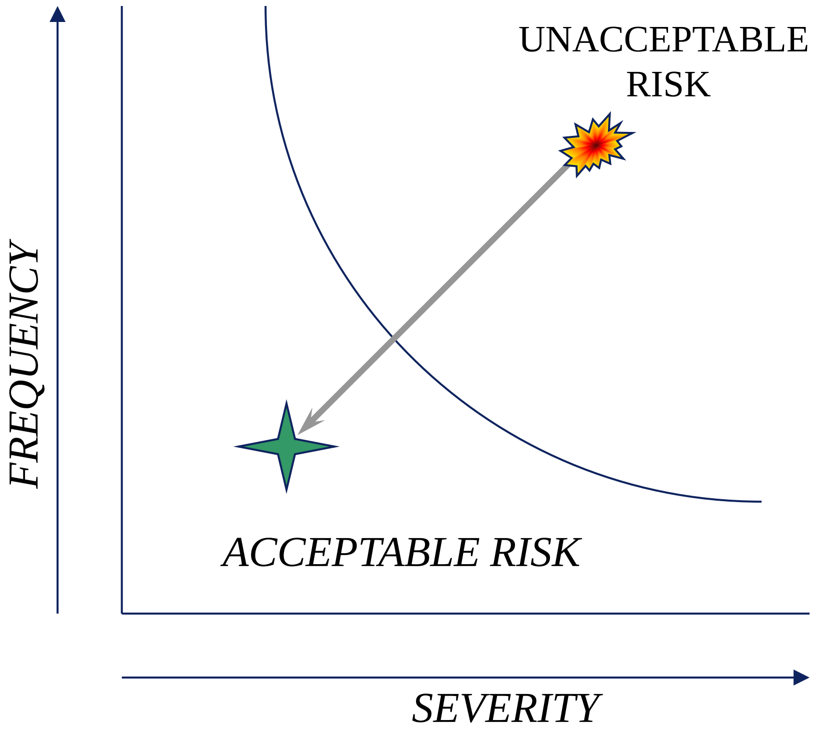
Honeywell



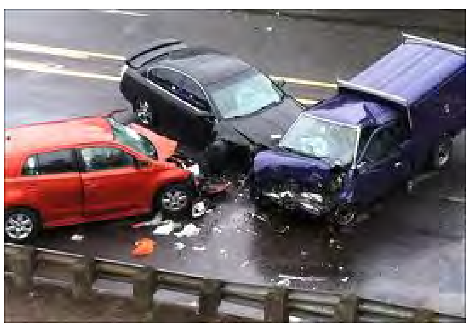
What Is Risk?

Honeywell

Risk is defined as the combination of the frequency of occurrence of harm and the severity of that harm



Risk Based on Frequency & Severity of Consequences

Severity	Frequency	Safety Risk
 **Plane crash – 200 deaths**	**Once in 20 million flights globally per year, i.e. 5 x 10E-8**	1 x 10E-5 LOWER
 **Car crash – 2 deaths**	**1 times in 1000 road incidents per year in a large city, i.e. 1 x 10E-3**	2 x 10E-3 HIGHER

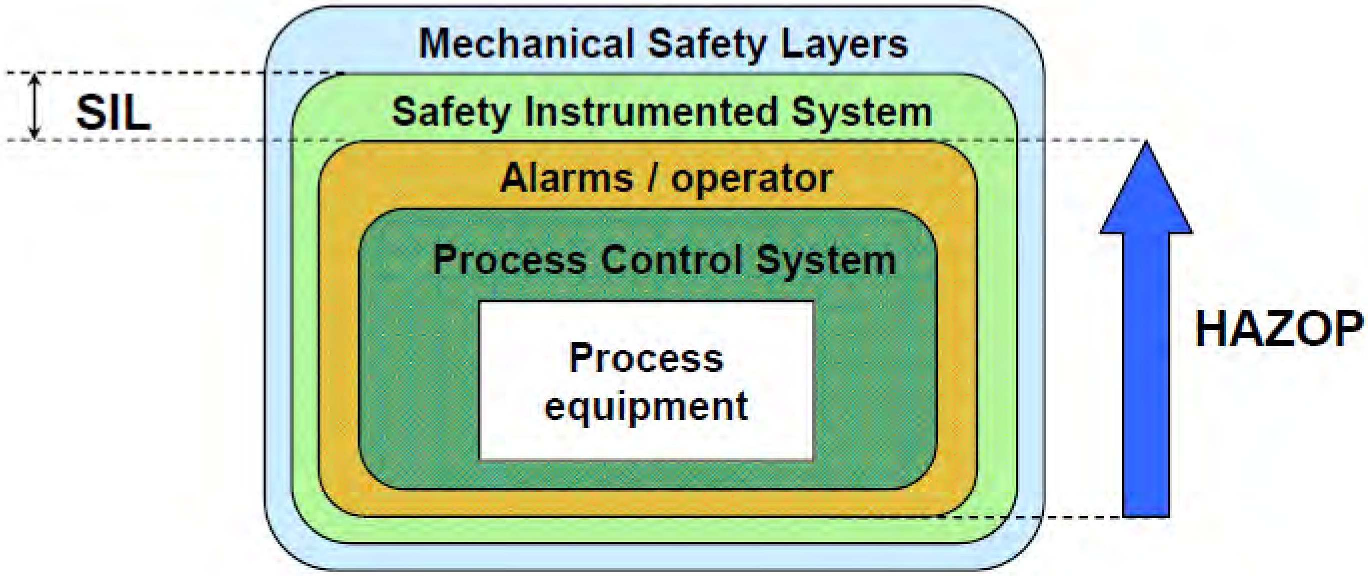
Hazard and Operability Study (HAZOP)

Honeywell

- Assesses the risk associated with a hazard
- Identifies and evaluates problems with a process
  - Risks to personnel or equipment
  - Potential operability problems
  - Potential deviations from design intent
  - Examines possible causes of deviations and assessment of consequences
- Qualitative technique
- IEC 61882 Hazard and Operability Studies (HAZOP) – Application Guide

HAZOP vs SIL

Honeywell



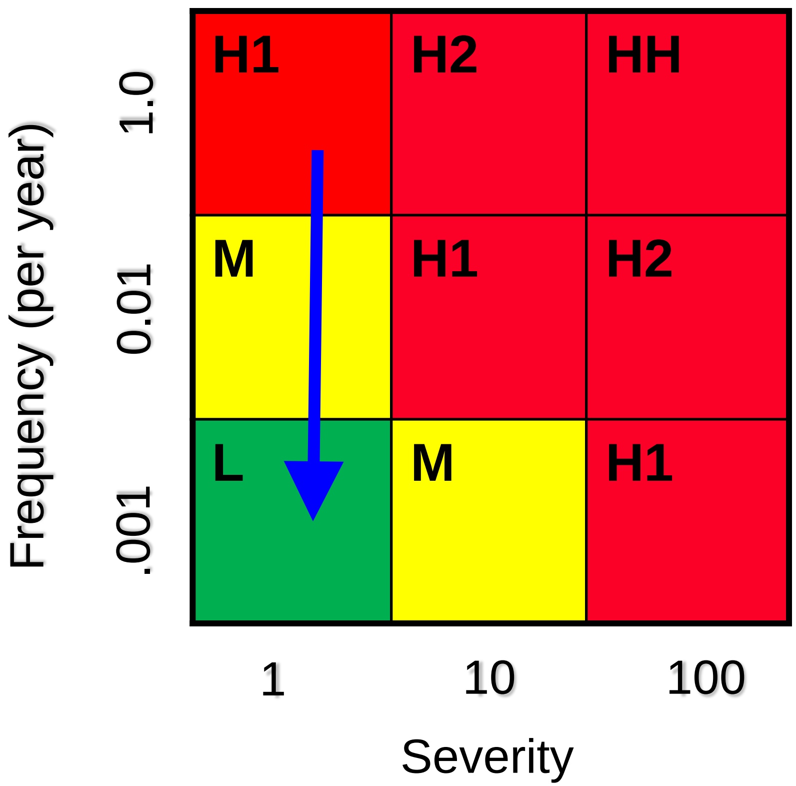
Layers of Protection Analysis (LOPA)

- Widely used risk assessment technique
- Can be viewed as an extension of HAZOP
- Semi-quantitative risk analysis tool
- Determines required Risk Reduction Factor

Required Risk Reduction - SIL determination

From the HAZOP risk matrix for this application:

1. Risk = Frequency x Severity
2. Per the indicated Risk matrix:



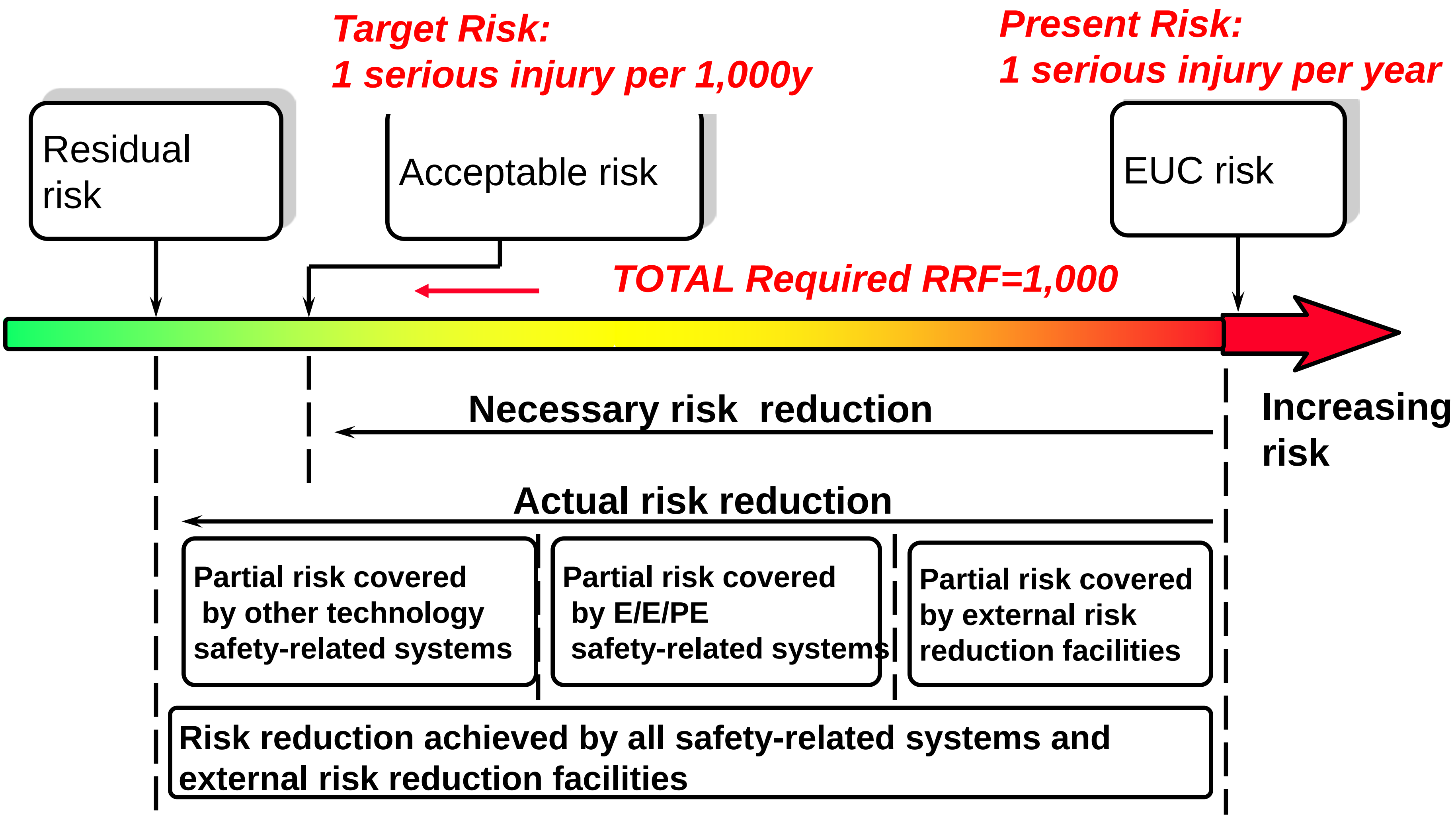
Present Risk “H1” = 1 (1 Serious injury in 1 year)

Acceptable Risk “L” = .001(1 Serious injury in 1,000 years)

Risk Reduction Factor (RRF)
=1/.001=1000

Risk and Risk Reduction

Honeywell



Safety Integrity Levels

PFD_{avg}	R in %	RRF	SIL
			4
0.0001	99.99	10,000	
			3
0.001	99.9	1,000	
			2
0.01	99	100	
			1
0.1	90	10	
			-
Probability of Failure on Demand	Reliability of Safety Functions	Risk Reduction Factor	

ISA S84.01

IEC 61508

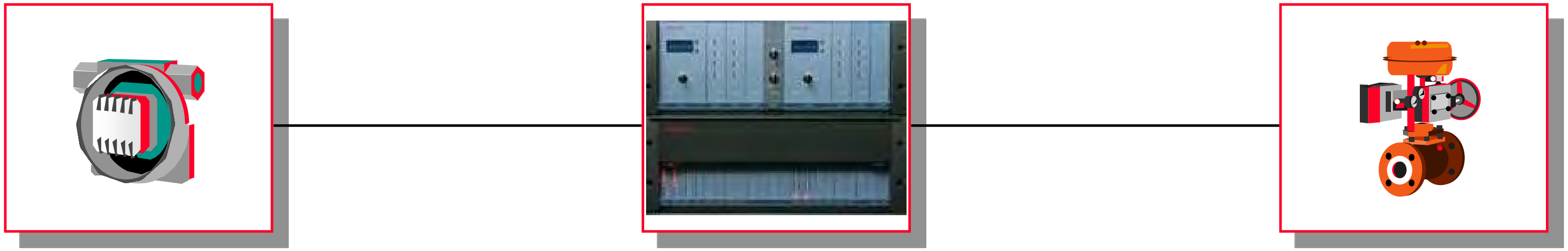
Standards Compliance

- ✓Target SIL must be specified for each SIF based on hazard and risk analysis
- ✓<u>Processes</u> for SIS throughout <u>lifecycle</u> must comply
- ✓Each SIF must meet target SIL requirements for:
  - Random failure rate (PFD_{avg})
  - Architectural constraints
  - Development process for each <u>component</u>

SIL Verification Calculation Example

$\mathbf{PFD_{avg}}$ (SIF) =

PFD_{avg}(sensor) + PFD_{avg} (logic solver) + PFD_{avg} (final element)



Example PFD_{avg} (SIF) = 0.0555 (SIL 1)

0.005 (SIL 2) + 0.0005 (SIL 3) + 0.05 (SIL 1)

SIL Verification Calculation Example

PFD_{avg} (SIF) =

PFD_{avg}(sensor) + PFD_{avg} (logic solver) + PFD_{avg} (final elements)

0.005 (SIL 2) + 0.0005 (SIL 3) + 0.0025 (SIL 2)

Example PFD_{avg} (SIF) = 0.008 (SIL 2)

Questions?