

The Buncefield Incident

A Review and the Path Forward



©KENEXIS 2010

Presenter Introduction



- Peter Herena
- Senior Engineer, Kenexis Consulting
- 12 Years Petrochemical Industry Experience
 - 9 Years Control and Safety Systems
- BSCHE, BSEnvE, Northwestern University
- PE, ISA-84 SFS/SSS

Buncefield Background

- Major pipeline transfer crossroad
- 5th largest fuel storage depot in UK
- 40km north of London



Source: Buncefield Final Report

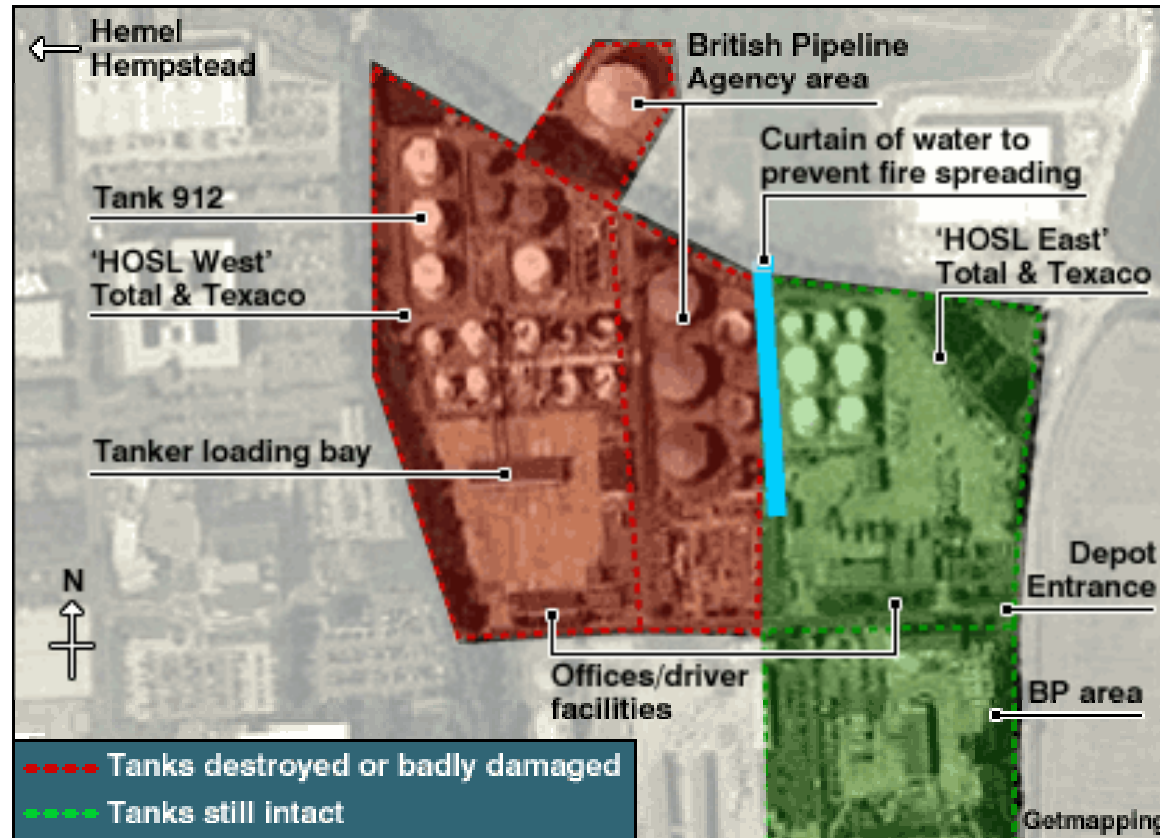
Buncefield Surroundings

- Maylands Industrial Estate
 - 630 businesses
 - 16,500 people
- Residential areas
- Town of Hemel Hempstead



Source:
Buncefield
Final Report

Map of Affected Area



Source: BBC

Local Incident Effects

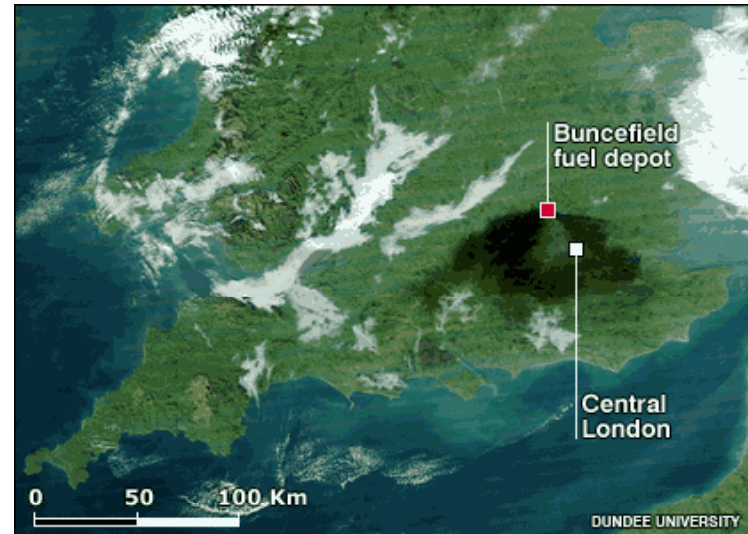
- 43 injuries
- 2,000 evacuated
- Damage estimate:
*£*1 billion



Source: Buncefield Final Report

Regional Effects

- Disruption to fuel supply
- Environmental Damage
- Negligible DW Contamination
- Possible MTBE/BTEX threat



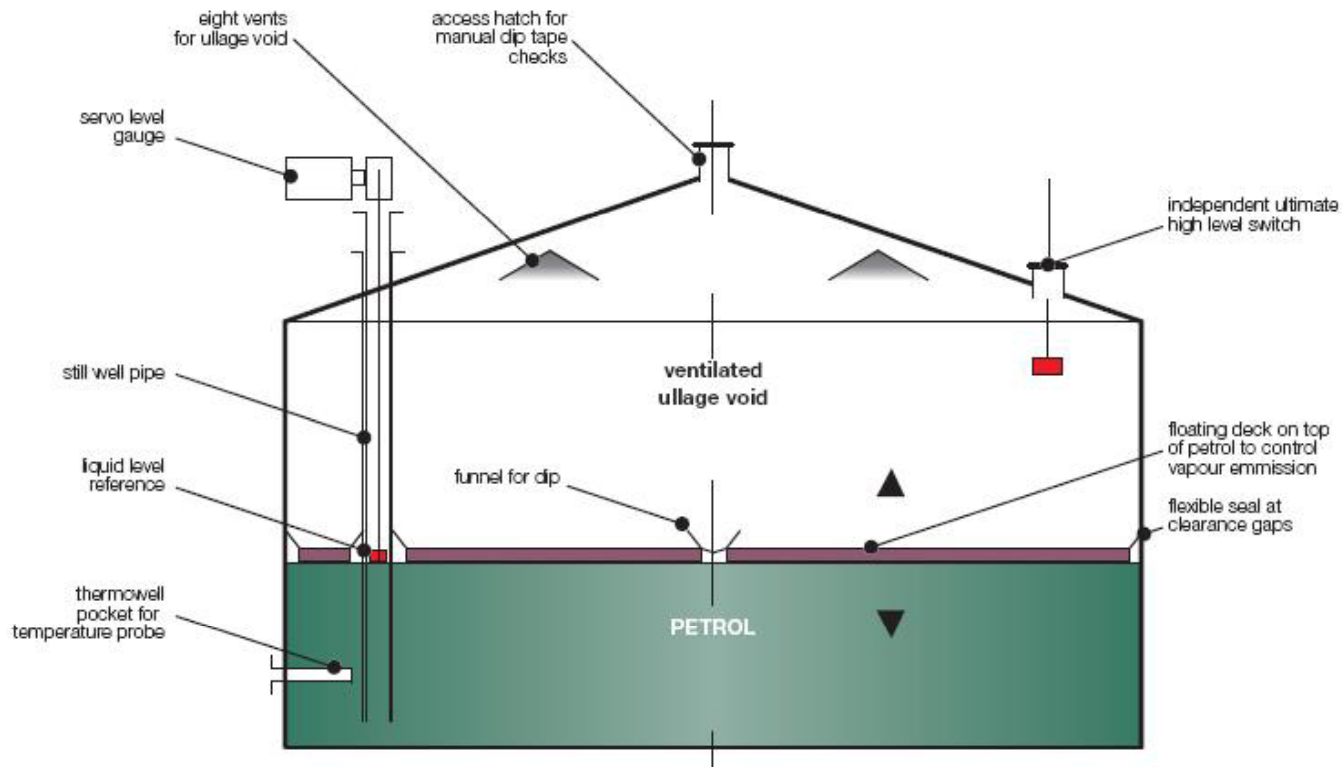
Cost & Litigation

- Recent High Court Ruling, Total liable for civil damages
- HOSL Claims: £ 625 million
- Criminal investigation ongoing

Timeline: Initial Events

- Pipeline transfer to load Tank 912 at HOSL with petrol began night of Sat, 10 Dec '05
- Tank level indication unchanged
- No operator intervention
- Ultimate high level sensor failed to function

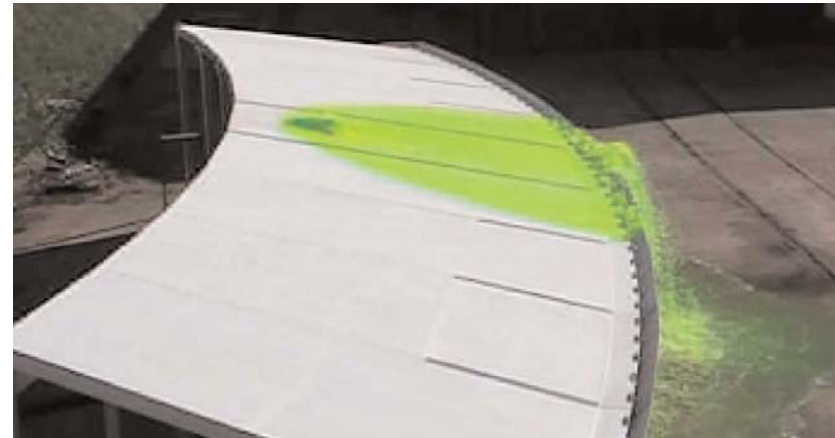
Tank 912 Schematic



Source: Buncefield Final Report

Timeline: Tank Overflow

- Overflow from ~0520 onwards
- Pump rate increased at 0550



Source: Buncefield Final Report

Timeline: Tank Overflow

- Vapor cloud flowed from Bund A in all directions
- Between 0530 and 0600 observed by witnesses



Source: Buncefield Final Report

Timeline: Tank Overflow

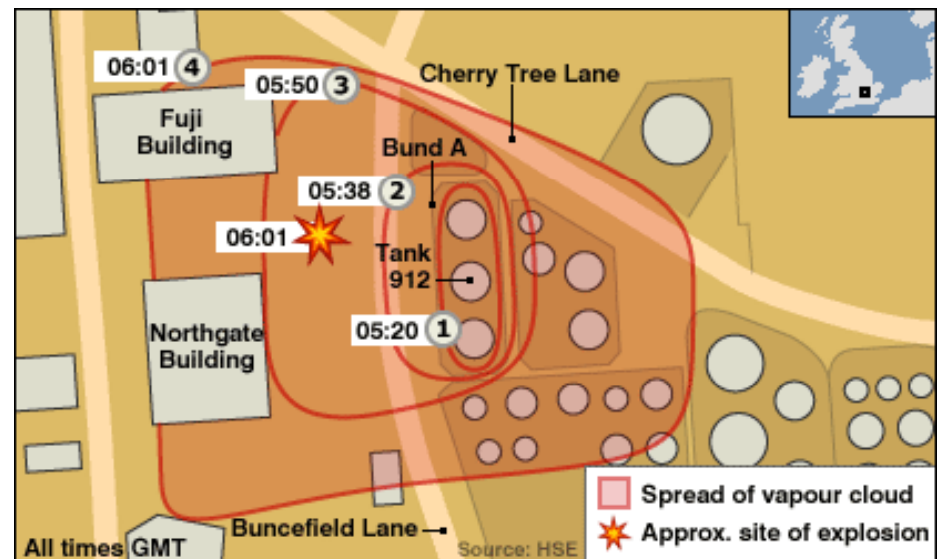
- “White Mist” Extended to far ends of some Maylands bldgs



Source: Buncefield Final Report

Timeline: Explosions

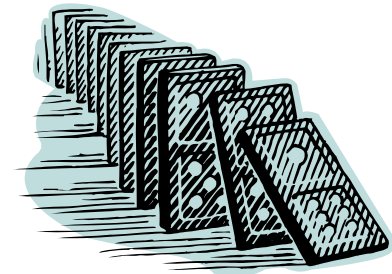
- Occurred at 0601
- A series of explosions that started massive fire
- Burned for 4 days



Source: HSE

Timeline Overview

- Initiating event:
 - Misoperation during loading
- Propagating events/conditions:
 - Poor administrative controls
 - Failure of primary level & alarm
 - Failure of operations to recognize
 - Failure of safety system to act
 - Poor maintenance practices



MIIB Board Recommendations

- Intended for “Buncefield-type” sites
- 78 Recommendations in 5 key areas
 - Off-site hazard mitigation
 - Emergency response preparedness
 - Land use planning
 - Regulation for inspection enforcement
 - Risk-based application of prevention measures

Recommendation #3

- Application of high integrity automatic overfill prevention systems
- Physically and electrically separate and independent from tank gauging system

Recommendation #8

- Called for consideration of alternate sensors
 - Easier to test
 - More reliable
 - Better diagnostics
 - Do not require components internal to tank

Recommendation #11

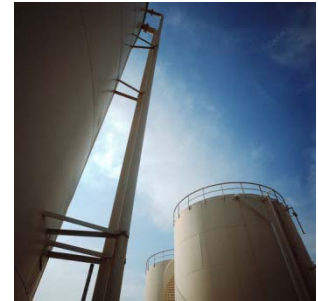
- Consider employing measures to detect hazardous conditions upon loss of containment
 - Flammable gas detectors in bunds
 - Connect flammable gas detectors to overfill protection system
 - Apply CCTV equipment that can detect and respond to condition changes

ISA-84 (IEC-61511) Application

- Recommendations 1-5 directly or indirectly references ISA-84 (IEC-61511)
 - Select a SIL using its methodology
 - Verify OPS (new/existing) achieves SIL
 - Design OPS using its methodology
 - Proof test per its methodology
 - Procedures for maintenance and testing, keep test records

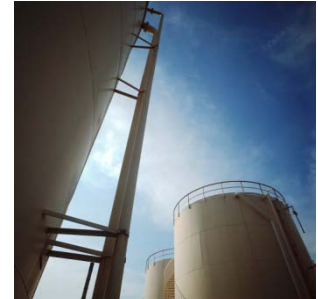
Challenges in Tank Measurement

- Density/Temperature fluctuations
- Corrosion
- Foreign material buildup
- Foaming
- Testing/Diagnostics
- COST



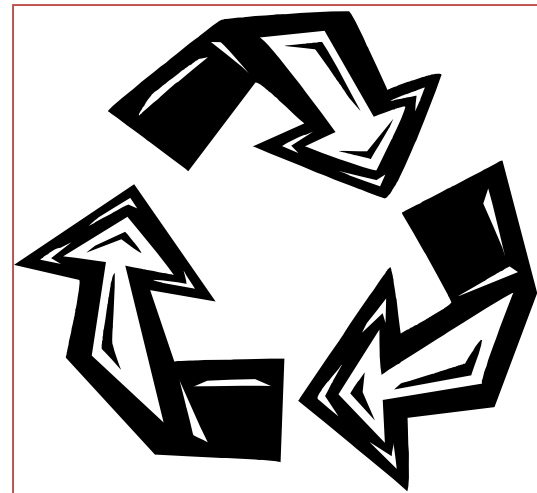
Tank Level Instrumentation

- Radar/Microwave
- Float/Servo Gauge
- RF Cap, Admit or Imp
- Conductivity
- Hydrostatic
- Ultrasonic
- Tuning Fork



ISA-84 Standard Safety Lifecycle

- International Society of Automation (ISA)
- ISA-84, “Safety Instrumented Systems for the Process Industry Sector”
- Provide a complete safety lifecycle to address all root causes of failure
 - Identification of systems
 - Design
 - Testing
 - Maintenance
 - Management of Change

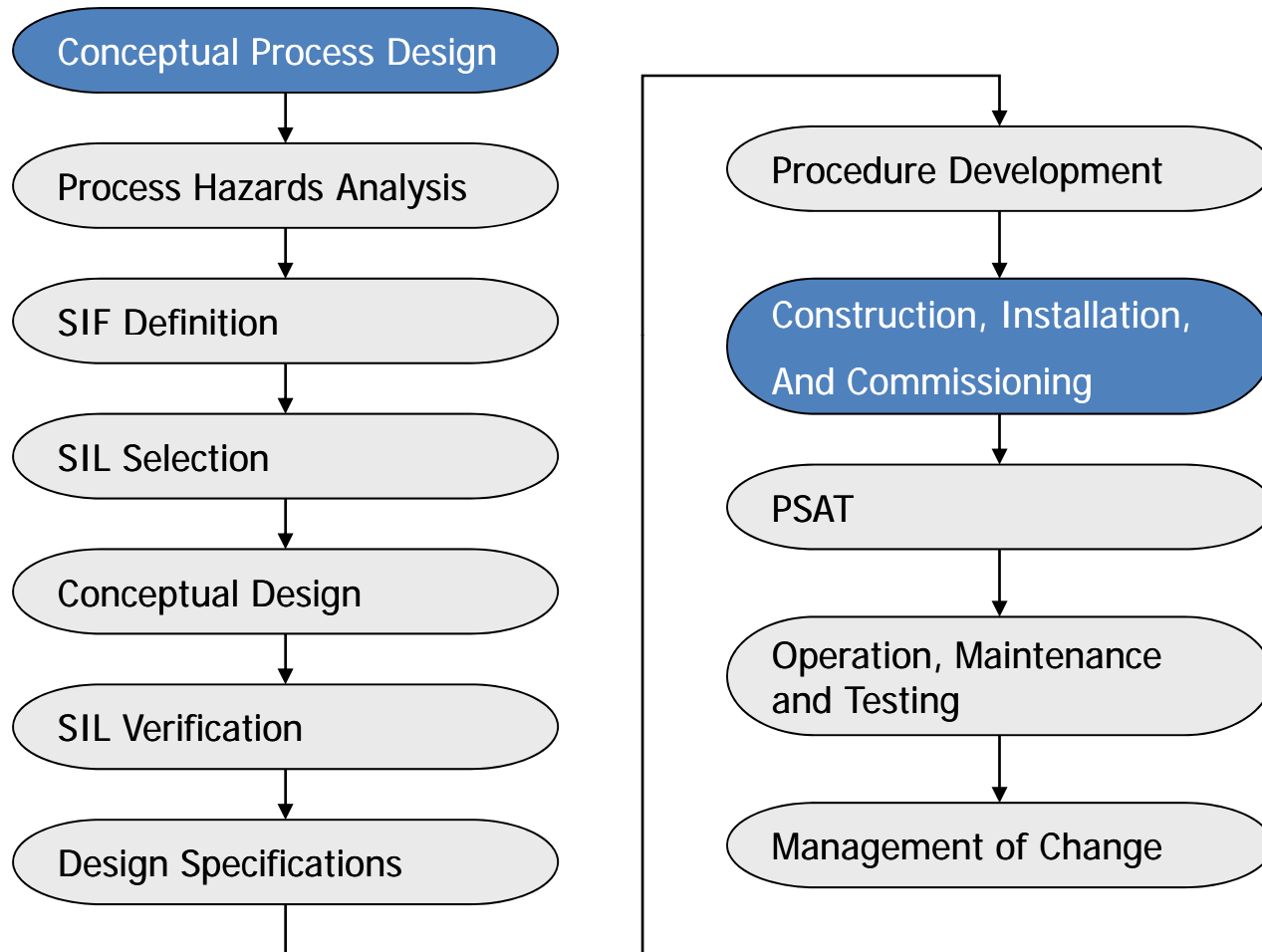


What does ISA-84 require?

- Performance based
- Defines a “safety lifecycle”
- Requires selection of performance target
- Requires confirmation of target achievement, quantitatively



Typical SIS Design Lifecycle



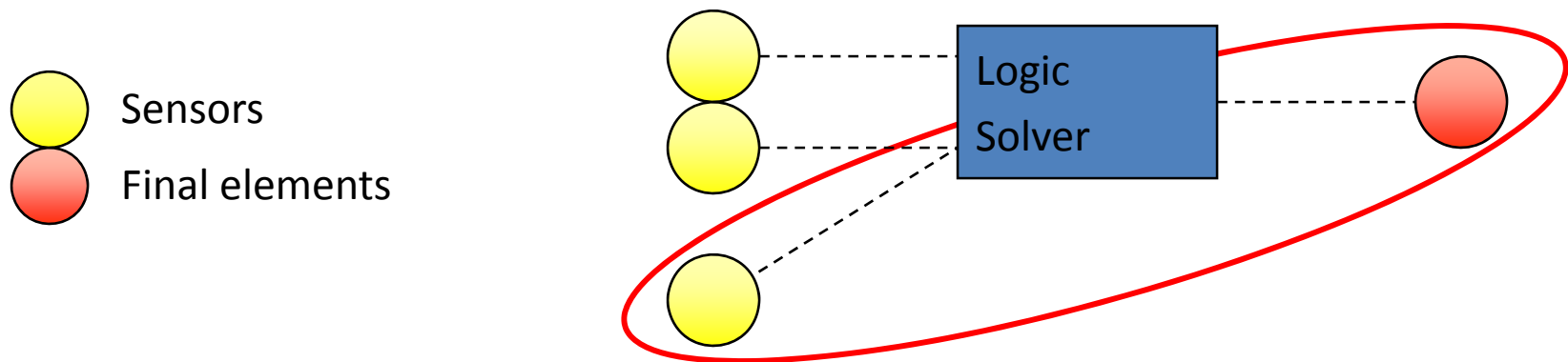
Principals of Risk Management

- Definitions
- Layers of Protection Concepts
- Different Philosophical approaches
- Risk Management Criteria



Safety Instrumented Function – Practical Definition

- Safety Instrumented Function(SIF) is
 - Specific actions to be taken under specific circumstances, which will automatically move the process from a potentially unsafe state to a safe state



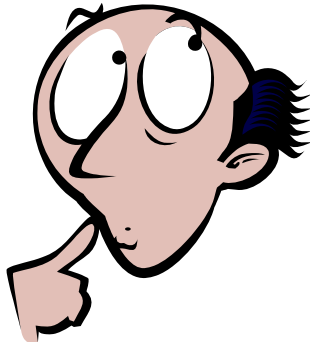
What is a Safety Integrity Level (SIL)?

A measure of the amount of risk reduction provided by a Safety Instrumented Function (SIF)

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> 99.99%	0.001% to 0.01%	100,000 to 10,000
SIL 3	99.9% to 99.99%	0.01% to 0.1%	10,000 to 1,000
SIL 2	99% to 99.9%	0.1% to 1%	1,000 to 100
SIL 1	90% to 99%	1% to 10%	100 to 10

How do I assign SIL?

“What is the Safety Integrity Level for my Safety Function ?”



Assign SIL that reduces risk to tolerable level

- Numerous techniques
 - Layer of Protection Analysis
 - Risk Graph
 - Quantitative
 - Others
- Be consistent!

What is risk?

Risk is a measure of the *likelihood* of occurrence of an unwanted event



and the *consequence* of adverse effects;



How often can it happen, and what will be lost if it does?

Types of Risk

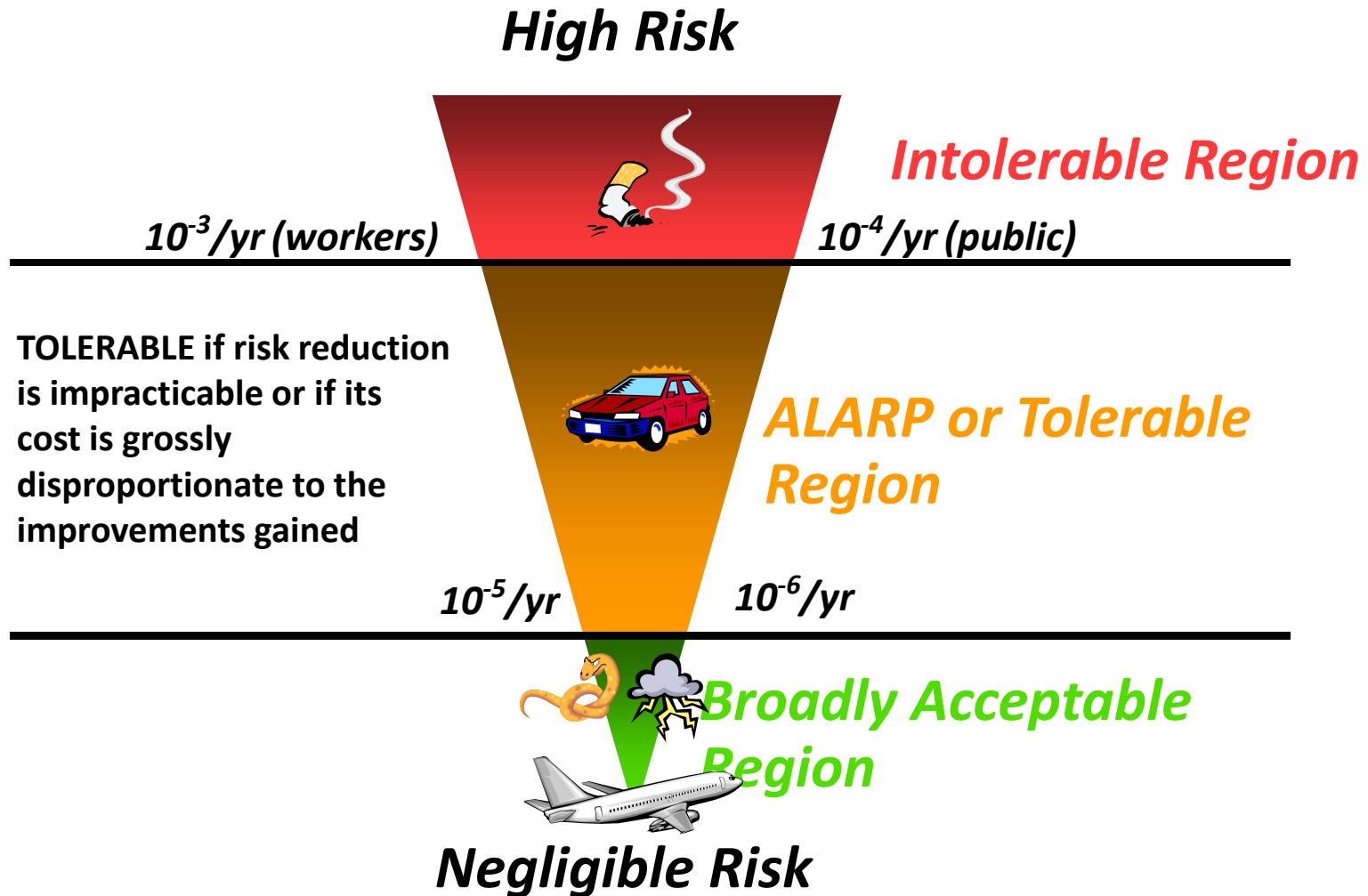
- Safety
 - Workers
 - Public
- Environment
- Property Damage
- Business Interruption
- Loss of Market Share



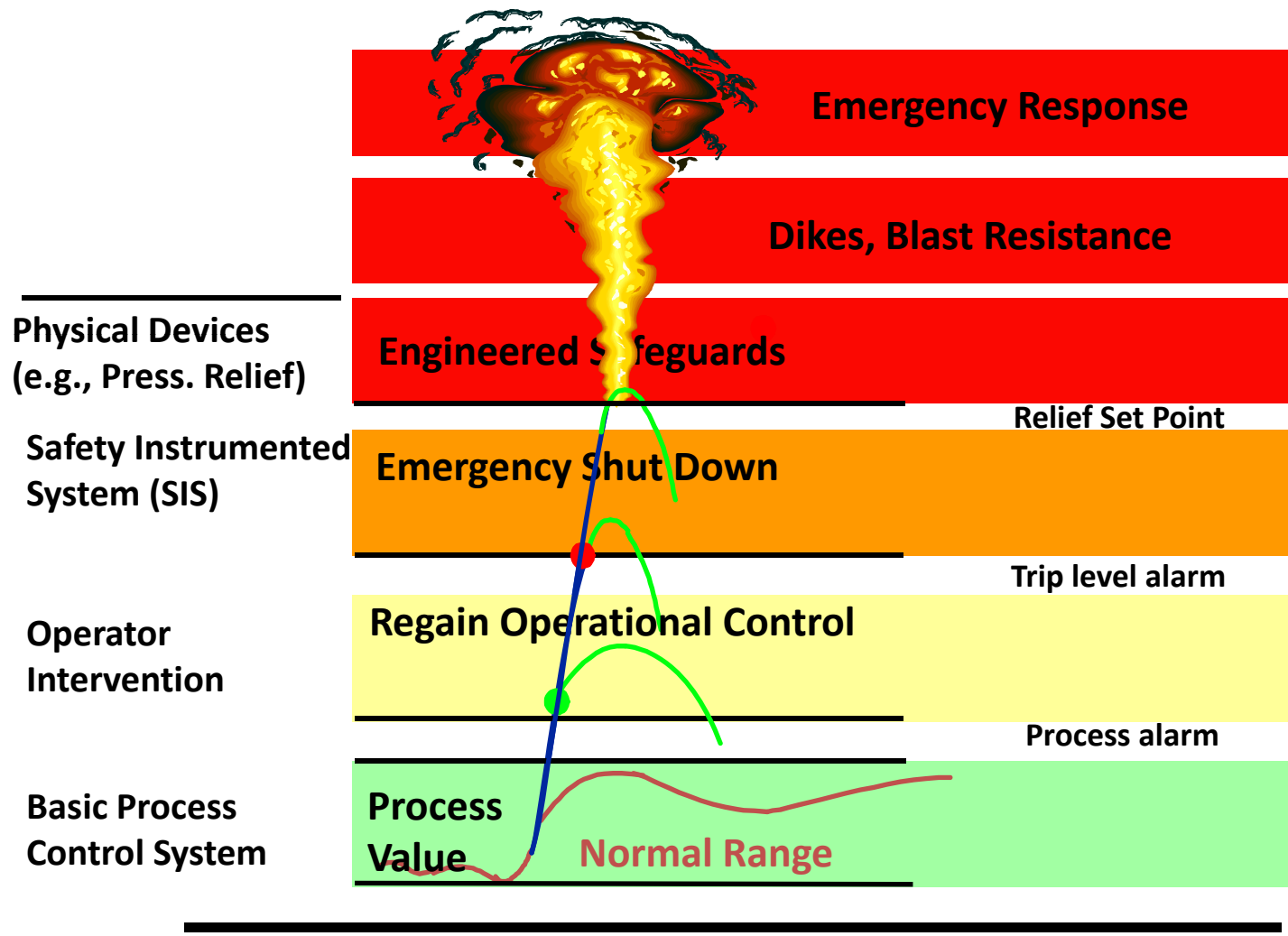
How ISA-84 Relates to Concept of “Risk”

- Decisions about when to use and SIS and the SIL should be based on *Risk*
- Don't prescribe how much risk to tolerate
- Most standards do not directly use risk, they have prescriptive requirements that provide an appropriate degree of safety

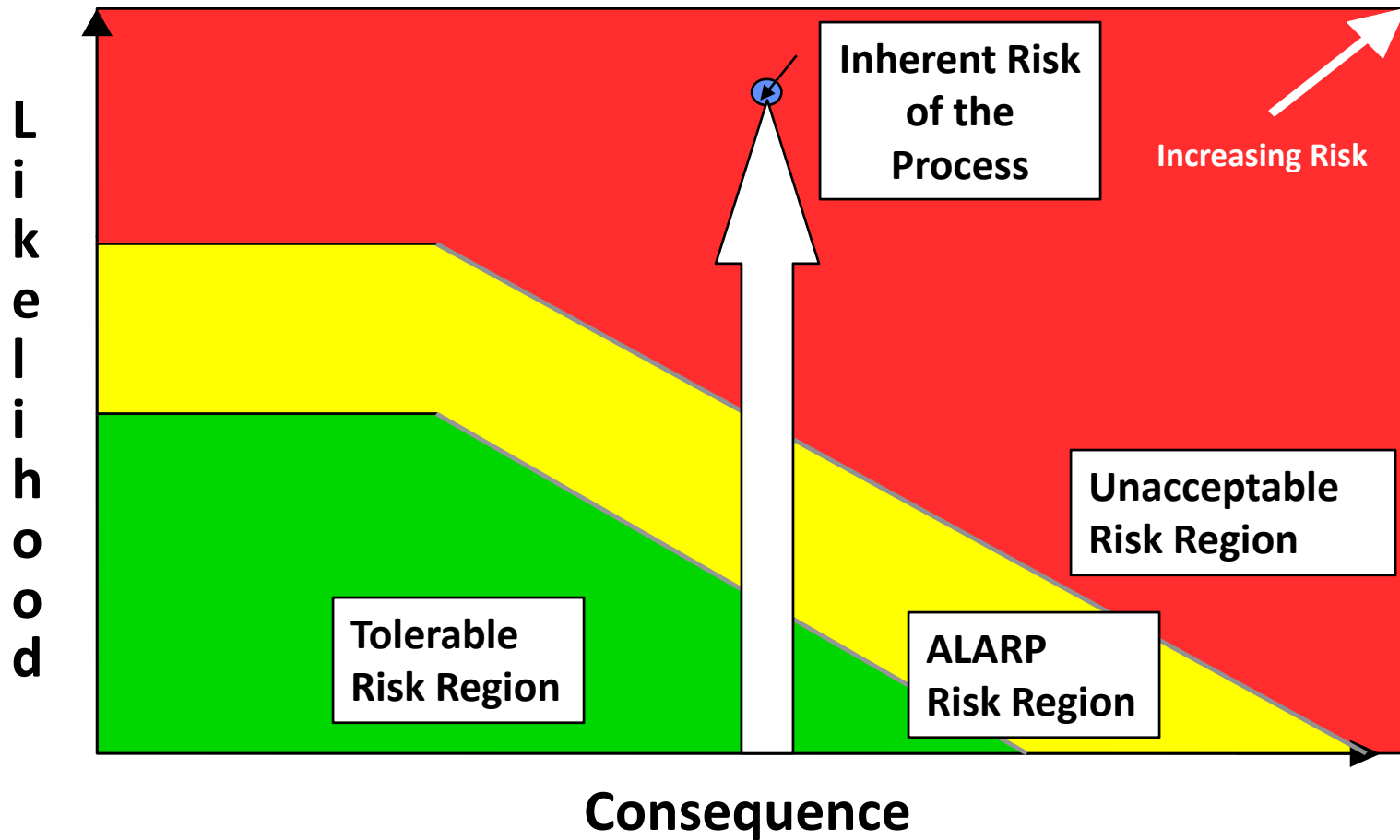
Tolerable Risk



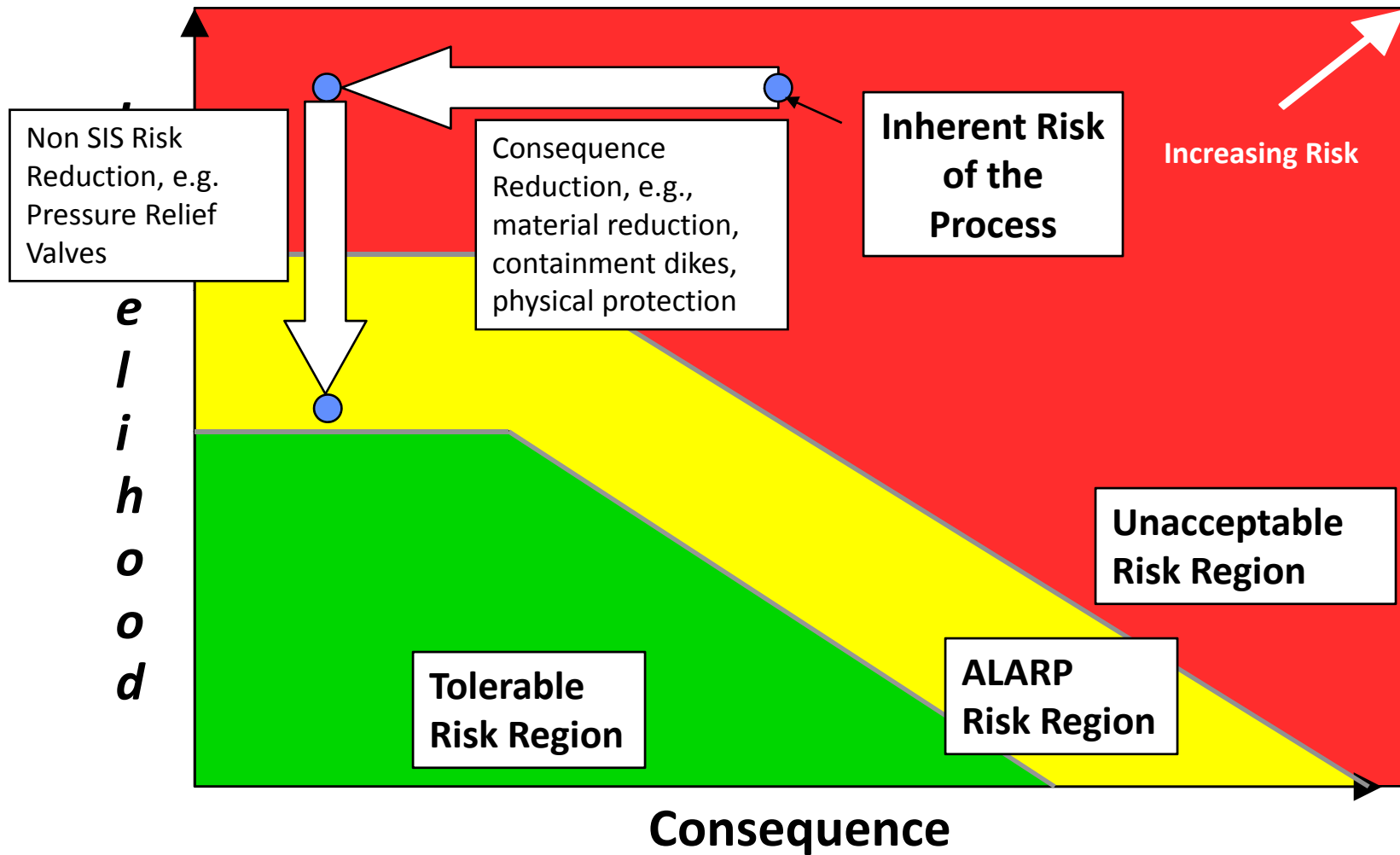
Layers of Protection



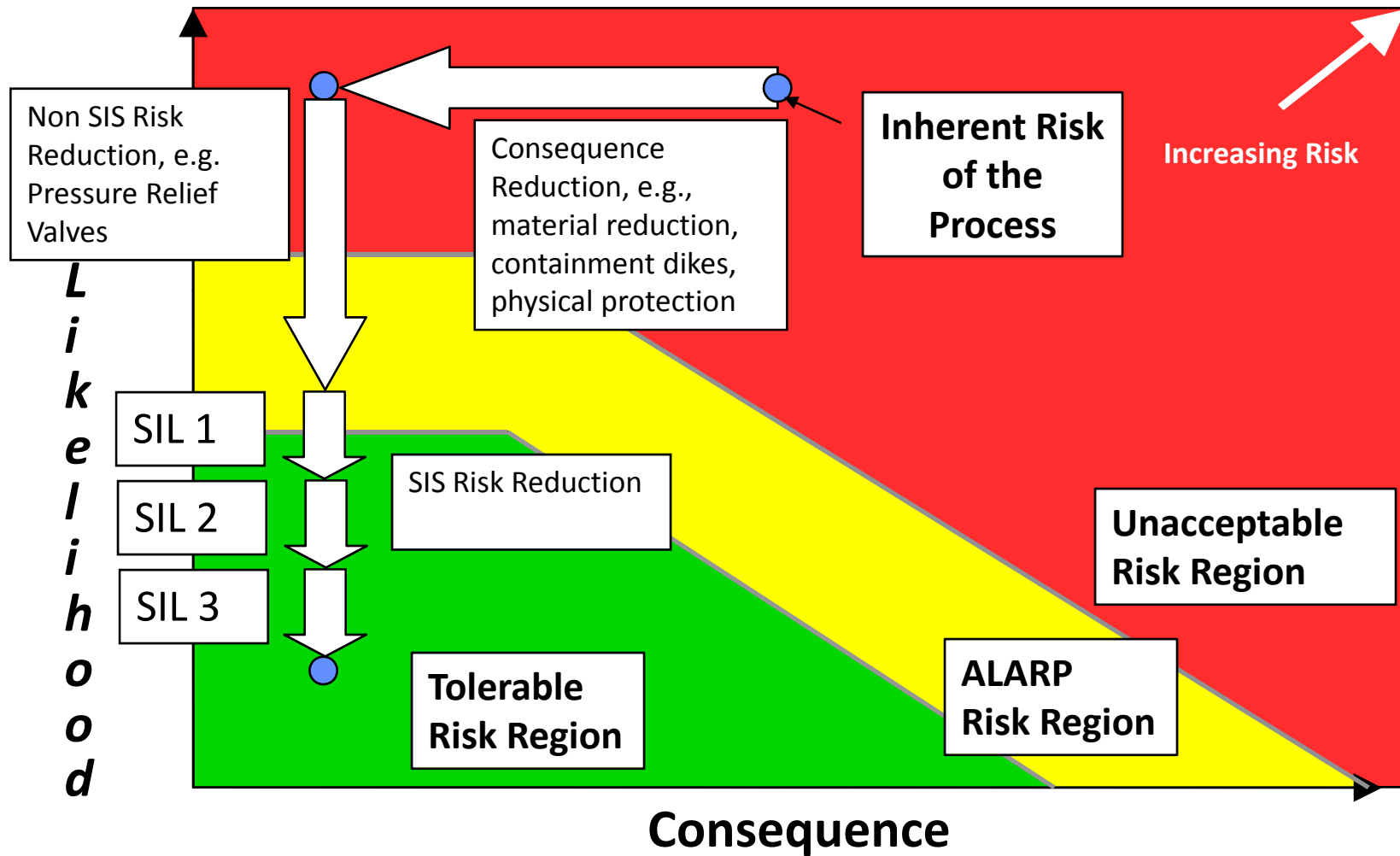
Reducing Risk



Non-SIS Risk Reduction



SIS Risk Reduction



Requirements of a Layer of Protection

- Independent protection layers have the following characteristics
 - Specificity
 - Independence
 - Dependability
 - Auditability



Commonly used IPLs

- Operator Intervention
 - Annunciated alarm
 - Continuously manned location
 - Proper training for alarm response
 - Adequate Response time
- Relief devices
- Check valves
- BPCS



Allocation of Risk

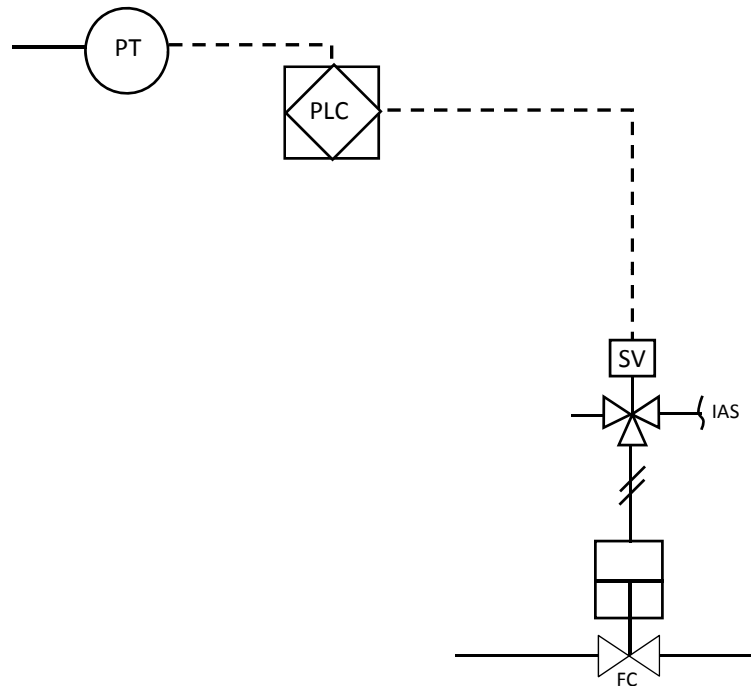
- After all protection layers are considered, the remaining risk that is in excess of what is tolerable is assigned to protection layers, usually as SIS



Principles of Risk Management Summary

- Necessary to adopt a “risk” approach to determine SIS design requirements
- Criteria for tolerable risk needs to be established
- Consistent methods for analyzing risk need to be established. No “standard” industry approach.
- Consider:
 - ✓ Consequence
 - ✓ Likelihood
 - ✓ Layers of Protection

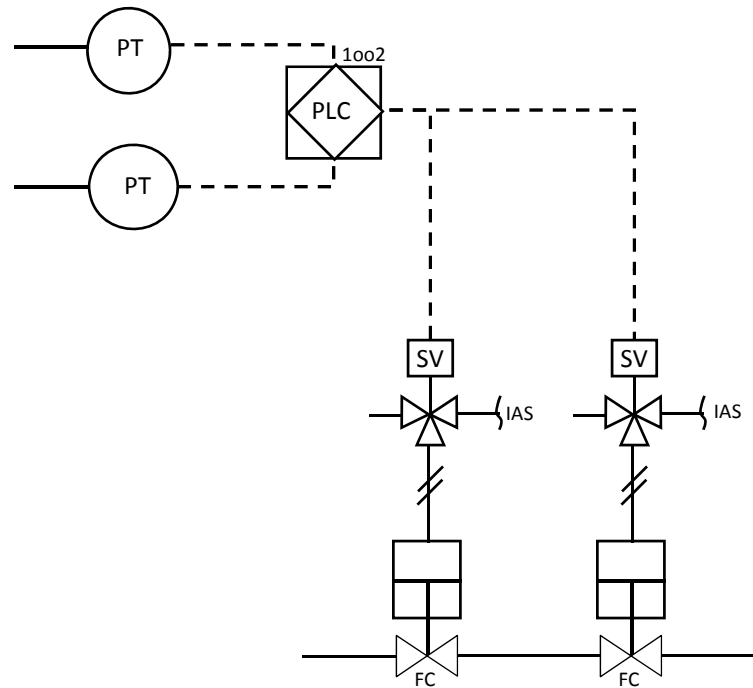
Typical SIL 1 Design



PFD(Sensors) + PFD(Logic Solver) + PFD(Final Elements)

= 1% to 10%

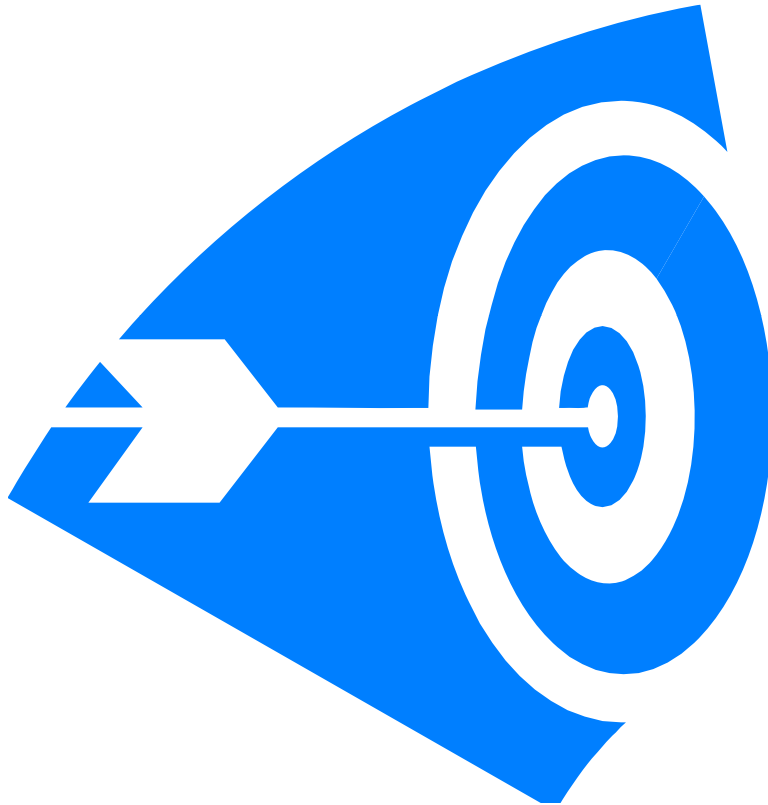
Typical SIL 2 Design



PFD(Sensors) + PFD(Logic Solver) + PFD(Final Elements)

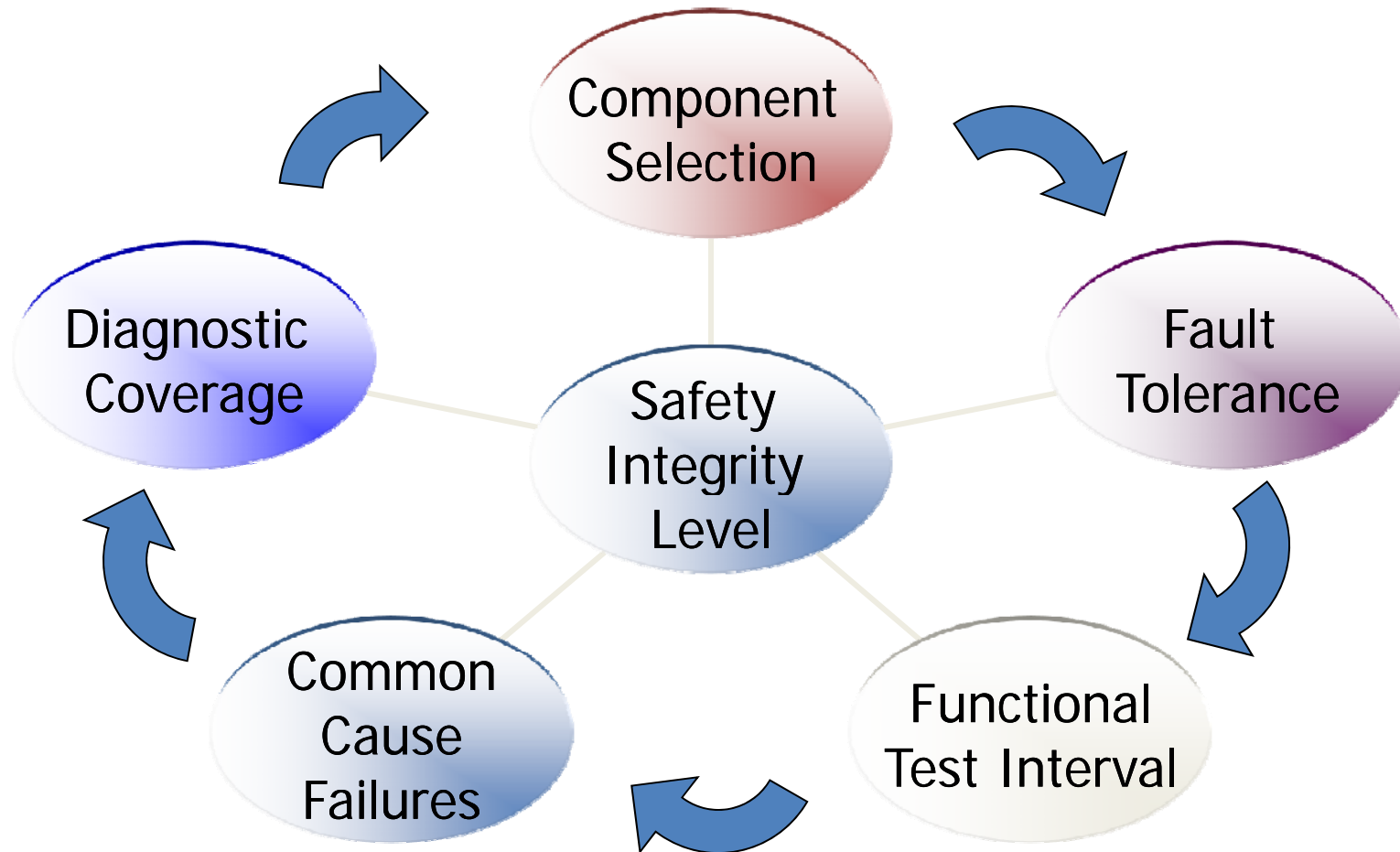
= 0.1% to 1%

SIL Verification



- Purpose is to quantitatively verify selected equipment and testing meets requirements
- Uses reliability engineering calculations

Parameters impacting SIL



Component Selection

- Device suitable application
- Device is suitable for safety
 - Proven in use
 - Mfg. in accordance w/ IEC 61508
- Technology of Device Appropriate
 - Safe Failure Fraction
 - Switches versus Transmitters
 - Relay vs. PLC vs. Safety PLC

Diversification – the Only Free Lunch?



- Sensor diversification should be strongly considered
- When multiple components are working to perform a safety function, common cause can disable similar components

Safety Requirements Specifications

- Purpose
 - Select equipment appropriate for SIL
 - Specify how the system operates
 - Basis for detailed design
 - Basis for Managing Change
- Result
 - Logic Solver Functional Specification (a.k.a, safety requirements specifications)



Test Plans

- One for each SIF
- Describes each step taken
- Matches PFD calculations
- Takes into account startup resources
 - Personnel
 - Equipment
 - Time



Recurring Nightmare



- Puerto Rico, 2009
- Two injuries
- Burned for 2 days
- Destroyed 20 tanks

Conclusions/Overview

- Challenge to meet new requirements
- Risk-based approach allows concentration on biggest hazards
- Safety Lifecycle has mutually supporting components
- Selecting instrumentation requires balancing many factors
- Some tools can streamline process

Thank You for Attending!

Peter G. Herena

Kenexis Consulting Corporation

2929 Kenny Road, Suite 225

Columbus, OH, 43221

USA

(614) 451-7031

<http://www.kenexis.com>

