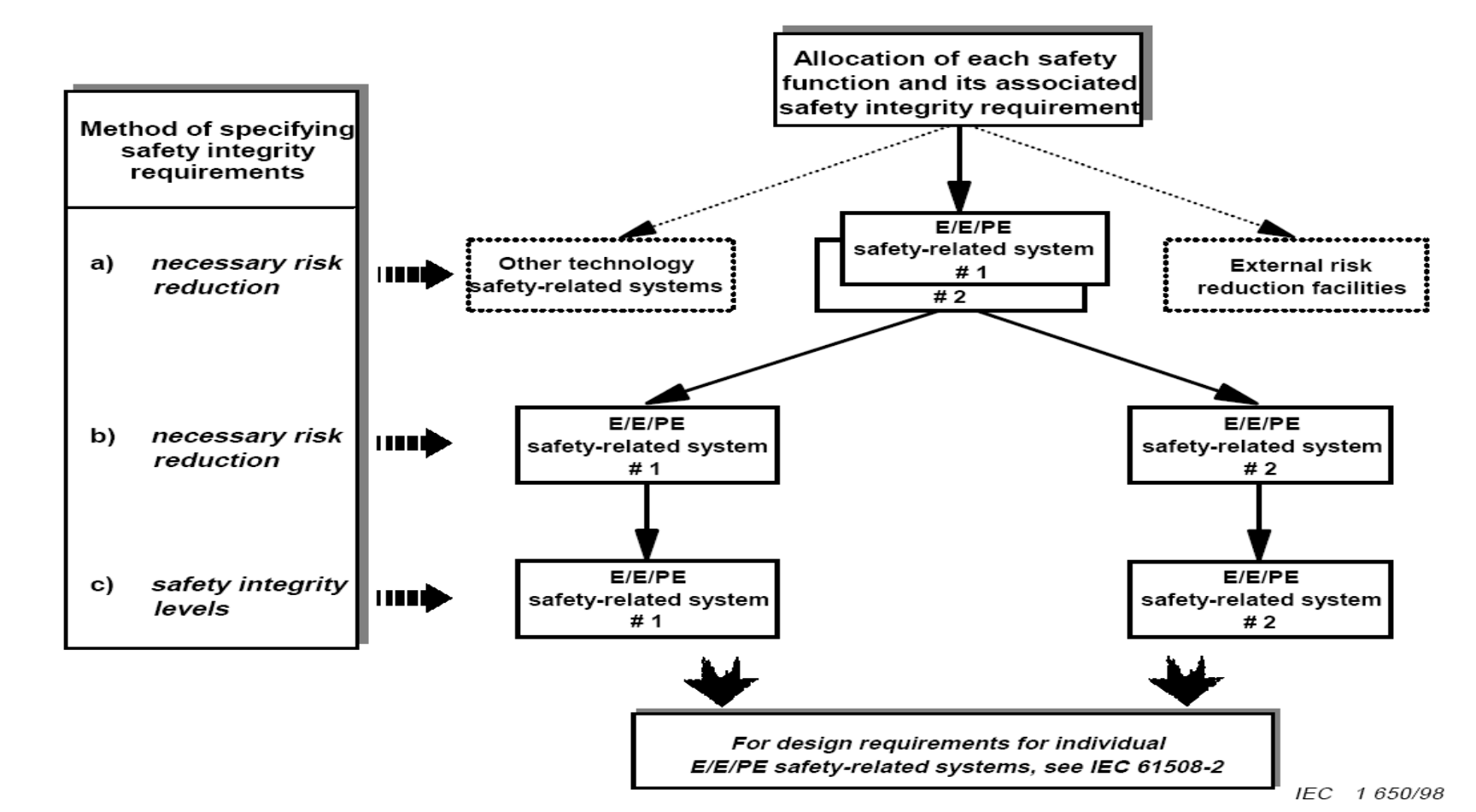
Controlling Risks
Selecting a Safety Integrity Level

IEC 61508

- The IEC 61508 specifies 4 levels of safety performance for a safety function.
- These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity
- safety integrity level 4 (SIL4) is the highest level.
- The standard details the requirements necessary to achieve each safety integrity level.
- These requirements are more rigorous at higher levels of safety integrity in order to achieve the required lower likelihood of dangerous failure.

- Allocation of safety functions to specific protection layers for the purpose of prevention, control, or mitigation of hazards from the accelerator and its associated equipment;
- The allocation of risk reduction targets to safety instrumented functions.

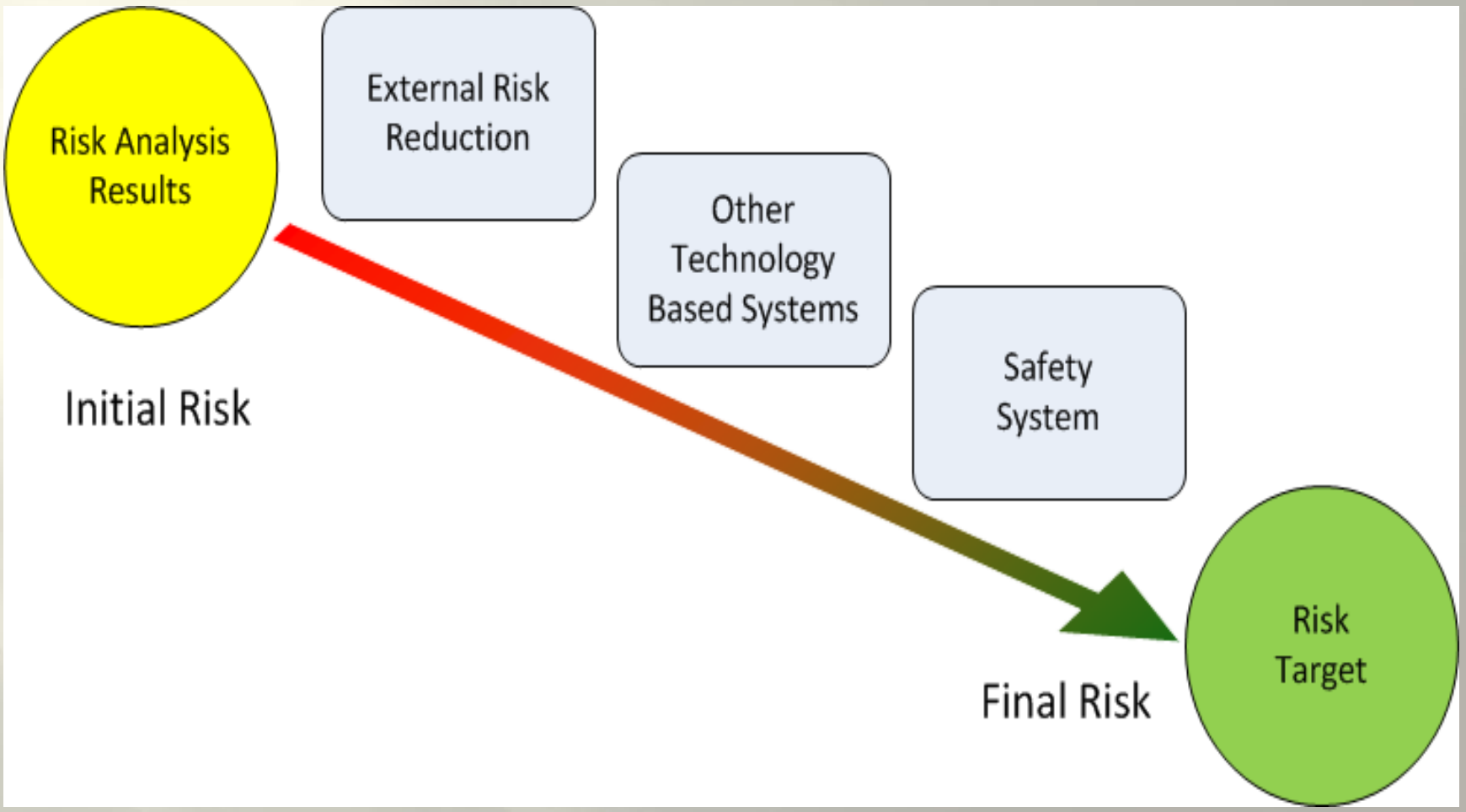
Method for Specifying SIL Requirements



Guide Lines for Determining Necessary Risk Reduction

- Guidelines from the appropriate safety regulatory authority;
- Discussions and agreements with the different parties involved in the application;
- Industry standards and guidelines;
- International discussions and agreements; the role of national and international standards are becoming increasingly important in arriving at tolerable risk criteria for specific applications;
- The best independent industrial, expert and scientific advice from advisory bodies;
- Legal requirements, both general and those directly relevant to the specific application.

Risk Reduction



Other Technology Safety-Related Systems

IEC 61508:

Safety related system* based on technology other than electrical/electronic/programmable electronic (E/E/PE) technology

Example:

Relief valve, disaster monitor, creditable control system functions

*Warning! DOE has a very specific use of the term “Safety Related System”, a.k.a. “Safety Significant System.” The IEC definition and the DOE definition are not necessarily the same.

External Risk Reduction Facility

IEC 61508:

Measure to reduce or mitigate the risks which are separate and distinct from, and do not use, E/E/PE safety-related systems or other technology safety-related systems*.

Example:

Shielding, emergency management, activated water containment system

*Warning! DOE has a very specific use of the term “Safety Related System”, a.k.a. “Safety Significant System.” The IEC definition and the DOE definition are not necessarily the same.

Independent Protection Layers

- Each ‘Other Technology’ and ‘External Risk Reduction’ can be credited with risk reduction if:
  - They are effective in preventing the consequence
  - They are independent of the initiating event
  - They are independent of other credited IPLs for a given scenario
  - They are auditable

Safety Function

- Derived from the hazard analysis
- Described as an action taken by the safety system
- Specific to each hazardous event
- Implemented through a combination of:
  - A safety instrumented system (SIS)
  - Other technology safety related system
  - External risk reduction facilities

Safety Functions

Function ID	Safety Function
SF1	Prevent beam transport from exclusion to occupied areas
SF2	Shut off interlocked devices when physical barriers between personnel and hazards are unsecured.
SF3	Shut off interlocked devices upon activation of an ESTOP
SF4	Shut off interlocked devices in support of administrative access to a secure beam enclosure.
SF5	Support search and secure operations prior to facility operations.
SF6	Inhibit operation of radiation generating devices when a high radiation dose rate associated with the device is detected in an occupied area
SF7	Deter unauthorized entry to exclusion areas
SF8	Provide visual indications of unsecured safe, secure safe, and unsafe radiological enclosure status.
SF9	Provide audible warnings of pending unsafe status of a beam enclosure
SF10	Activate audible and visual alarms when the indicated oxygen level in monitored areas drops below 19.5% by volume.

Safety Functions and SIS

- The safety functions allocated to a safety instrumented system (SIS) become performance requirements for the safety system.
  - Effectiveness
  - Timing
  - Sustainability
- Captured in a requirements document

Requirements Specification

- Scope, Context, Assumptions, References
- Mandatory requirements
  - DOE orders, Statutes, Facility Policy
- Safety Functions
- SIL assignments
- Generalized requirements
  - Apply to whole lifecycle
  - Objective based
- Specific requirements
  - May apply to specific parts of the lifecycle
  - Performance
  - Systems/architecture
  - Software
  - Operations and Maintenance
  - Management and Staffing

Identification of Requirements

10.3 SIS safety requirements

10.3.1 These requirements shall be sufficient to design the SIS and shall include the following:

- A description of all the safety instrumented functions
- Requirements to identify and take account of common cause failures
- A definition of the safe state of the process for each function
- A definition of any individually safe process states which, when occurring concurrently, create a separate hazard
- Assumed sources of demand and demand rate
- Required proof test intervals
- The response time for the SIS to bring the process to a safe state
- The safety integrity level and mode of operation for each safety function
- A description of SIS process measurements and their trip points
- A description of SIS process output actions and criteria for successful operations
- …

Identification of Requirements

10.3 SIS safety requirements

10.3.1 These requirements shall be sufficient to design the SIS and shall include the following:

- …The functional relationship between inputs and outputs (Logic)
- Requirements for manual shutdown (ESTOP)
- Requirements relating to energize or de-energize to trip
- Requirements for resetting the SIS after shutdown
- Maximum allowable trip rate
- (SIS) Failure modes and desired response of the SIS
- Startup procedures
- All interfaces between the SIS and any other system
- A description of the modes of operation of the (Accelerator) and identification of safety instrumented functions required in each mode
- The application software requirements
- …

Identification of Requirements

10.3 SIS safety requirements

10.3.1 These requirements shall be sufficient to design the SIS and shall include the following:

- …Requirements for overrides, inhibits, bypasses including how they will be cleared
- Any action necessary to achieve or maintain a safe state in the event of faults being detected in the SIS (Including human factors)
- The mean time to repair taking in to account travel time, location, spares, …etc.
- The extremes of all environmental conditions likely to be encountered
- Identification of normal and abnormal modes for both the (Accelerator) and (Accelerator) operational procedures
- Definition of the requirements for any safety function necessary to survive a major accident event (e.g. beam stopper survival)
- …

Attributes of Specific Requirements – The ‘ables

- Requirements must be;
  - Uniquely identifiable
  - Testable
  - Verifiable
  - Traceable

SIL Ranges

DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	Average Probability of Failure on Demand	Risk Reduction
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to $\leq$ 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to $\leq$ 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to $\leq$ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to $\leq$ 100

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	Frequency of Dangerous Failures Per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

SIL Allocation

- Performance requirement
- For each safety instrumented function
- Qualitative or quantitative
- Based on:
  - Average probability of dangerous failure per demand (PFD_{avg})

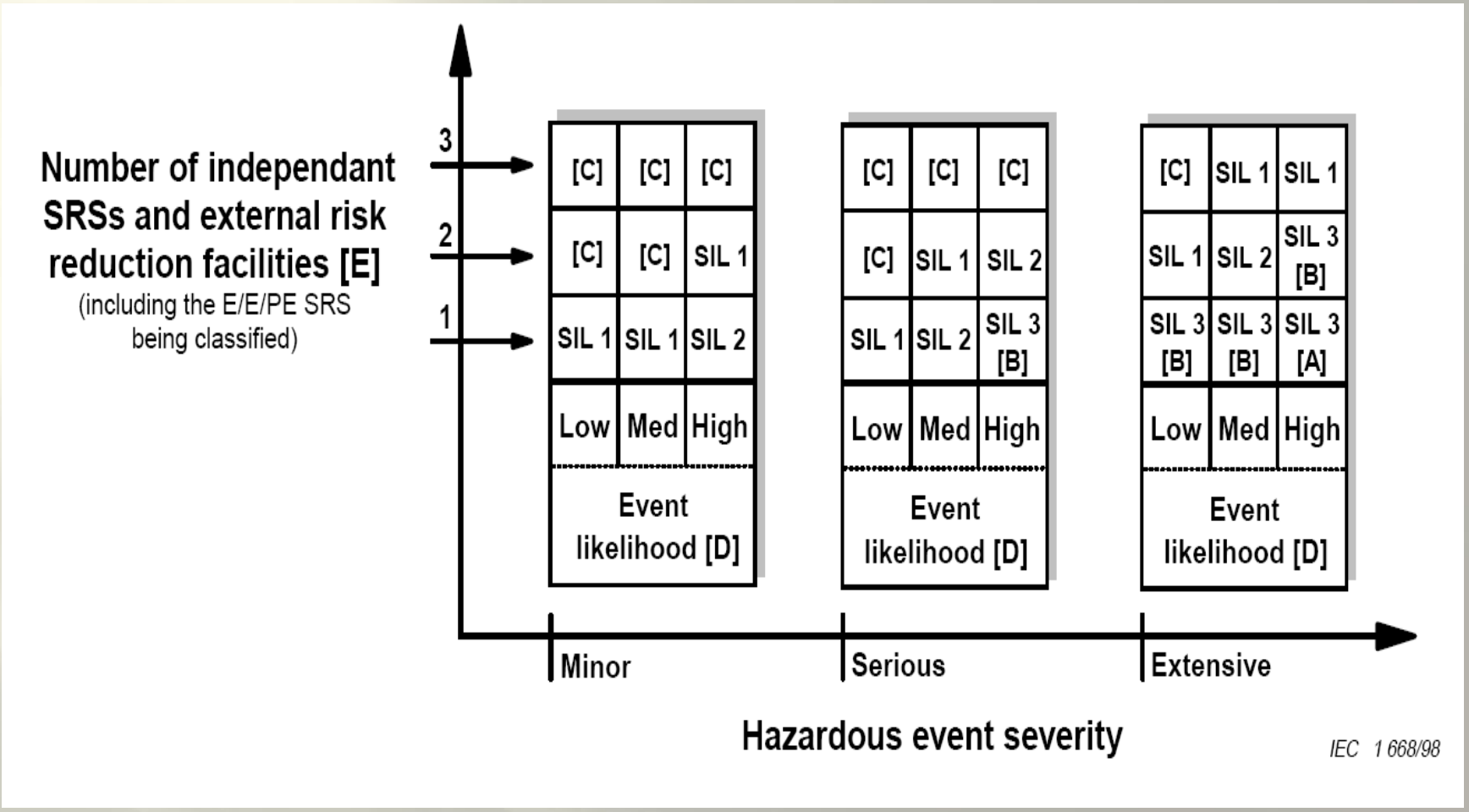
  OR

  - Failure rate, per hour

Latte

- Qualitative data:
  - robust aroma
  - frothy appearance
  - strong taste
  - burgundy cup
- Quantitative data:
  - 12 ounces of latte
  - serving temperature 150º F.
  - serving cup 7 inches in height
  - cost $4.95

Risk Matrix Approach



Risk Matrix Use

- Calibrate risk classifications of the unmitigated accident
  - e.g. “Intolerable, Unacceptable, Tolerable, Acceptable”
  - Apply external safety layers and ‘other technology’ systems
  - Increase SIL Level until objective met

    OR

    Apparent additional risk reduction required

Risk Matrix

Risk matrix
set up for hazard type

External Risk Reduction	0						
Other Technology Based Systems	0						
SIL	0					User Defined	Range
Risk Matrix		Color code	Intolerable		0	4	
			Undesirable		4	5	
			Tolerable		5	7	
			Acceptable		7	>	
User Defined Likelihood							
Immanent	0	Frequent	3	2	1	0	
1day-1year	1	Probable	4	3	2	1	
1-10 years	2	Occasional	5	4	3	2	
Over life of facility	3	Remote	6	5	4	3	
100-1000 years	4	Unlikely	7	6	5	4	
>1000 years	5	Impossible	8	7	6	5	
			3	2	1	0	
		Consequences	Minimal	Marginal	Critical	Catastrophic	
			First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

Risk Matrix

External Risk Reduction and Other Methods Evaluated

External Risk Reduction	2						
Other Technology Based Systems	1						
SIL	0						User Defined Range
Risk Matrix		Color code	Intolerable		0	4	
			Undesirable		4	5	
			Tolerable		5	7	
			Acceptable		7	>	
User Defined Likelihood							
Immanent	0	Frequent	6	5	4	3	
1day-1year	1	Probable	7	6	5	4	
1-10 years	2	Occasional	8	7	6	5	
Over life of facility	3	Remote	9	8	7	6	
100-1000 years	4	Unlikely	10	9	8	7	
>1000 years	5	Impossible	11	10	9	8	
			3	2	1	0	
		Consequences	Minimal	Marginal	Critical	Catastrophic	
			First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

Risk Matrix

Effect of SIL Levels Evaluated

External Risk Reduction	2						
Other Technology Based Systems	1						
SIL	3					User Defined Range	
Risk Matrix		Color code	Intolerable		0	4	
			Undesirable		4	5	
			Tolerable		5	7	
			Acceptable		7	>	
User Defined Likelihood							
Immanent	0	Frequent	9	8	7	6	
1day-1year	1	Probable	10	9	8	7	
1-10 years	2	Occasional	11	10	9	8	
Over life of facility	3	Remote	12	11	10	9	
100-1000 years	4	Unlikely	13	12	11	10	
>1000 years	5	Impossible	14	13	12	11	
			3	2	1	0	
		Consequences	Minimal	Marginal	Critical	Catastrophic	
			First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

Risk Graph

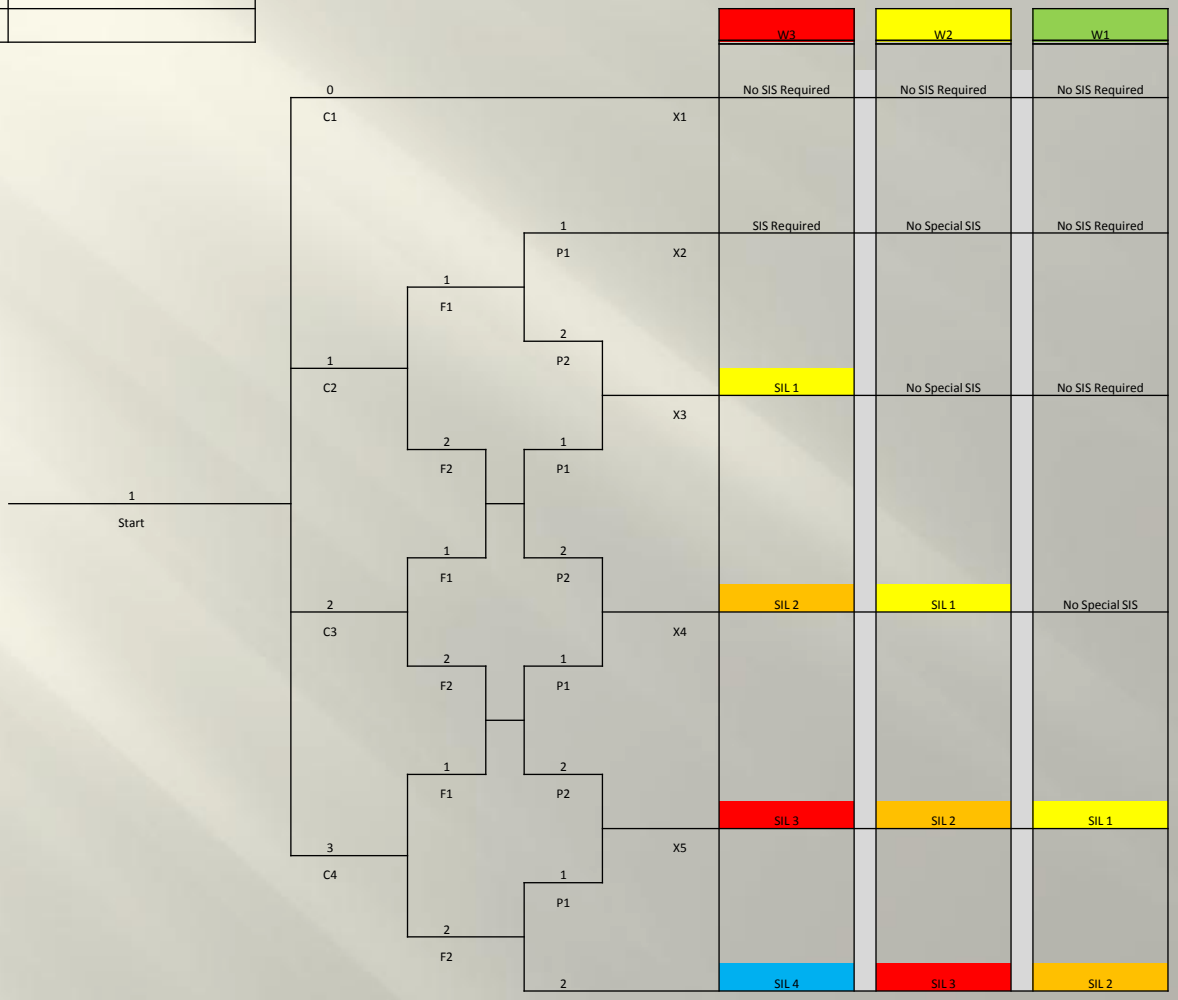
- Developed in Germany, used widely
- Incorporates exposure and possibility of avoidance
- Intuitive decision path
- Direct reading of SIL

Risk Graph Use

- Calibrate categories of the graph
  - Consequence
  - Frequency/Exposure
  - Avoidance
  - Demand/Outcome
- Trace each safety instrumented function through to the appropriate box in the “W” columns.

Risk Graph

Date	
Project	
Evaluator	
Hazard	
Constraints	



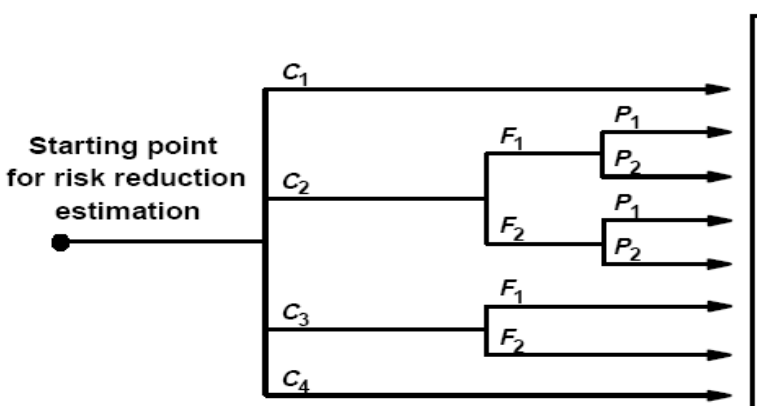
Consequence		
C1	Minor Injury	1
C2	Serious injury	2
C3	Death	3
C4	Multiple Deaths	4

Frequency and Exposure Time		
F1	Rare to Frequent	1
F2	Frequent to Continuous	2

Posibility of Avoidance		
P1	Avoidance Possible	1
P2	Avoidance not likely	2

Probability of outcome		
W1	Very Slight probability	1
W2	Slight probability, few occurances	2
W3	High probability	3

Risk Graph



W_3	W_2	W_1
a	–	–
b	a	–
c	b	a
d	c	b
e	d	c
f	e	d
g	f	e
h	g	f

a, b, c, d, e, f, g, h represent the necessary minimum risk reduction. The link between the necessary minimum risk reduction and the safety integrity level is shown in the table.

C = Consequence risk parameter

F = Frequency and exposure time risk parameter

P = Possibility of avoiding hazard risk parameter

W = Probability of the unwanted occurrence

a, **b**, **c** ... **h** = Estimates of the required risk reduction for the SRSs

Necessary minimum risk reduction	Safety integrity level
–	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS is not sufficient

IEC 1 667/98

Example Calibrations

Consequence Categories [E. Marzal, "Safety Integrity Level Selection"]		
Category	Quantitive Description	Qualitative Description
C_A	Minor Injury	Minor Injury
C_B	PLL=0.01 to 0.1	Major injury
C_C	PLL = 0.1 to 1	Death
C_D	PLL > 1	Multiple deaths and/or major impact off-site

Example Calibrations

Occupancy/Exposure Categories [E. Marzal, "Safety Integrity Level Selection"]		
Category	Quantitive Description	Qualitative Description
F_A	Occupied/Exposed < 10% of time	Rare to More Frequent
F_B	Occupied > 10%	Frequent to Continuous

Example Calibrations

Consequence Categories [E. Marzal, "Safety Integrity Level Selection"]		
Category	Description	Conditions allowing P_A
P_A	Conditions to right satisfied	P_A should only be selected if the following conditions are true: • The operator will be alerted to SIS failure • Facilities are provided for avoiding the hazard that are separate from the SIS and enable escape from the area. • The Time between the operator alert and occurrence of the event is sufficient for necessary actions.
P_B	Conditions to right not satisfied	

Demand Rate/Probability Categories

[E. Marzal, "Safety Integrity Level Selection"]

Category	Quantitive Description	Qualitative Description
W_A	< 0.02 per year	Slight
W_B	Between 1 and 0.02 per year	Occasional
W_C	> 1 per year	Frequent

Quantitative

- Calculate Initial Risk using risk analysis tools
- Calculate the residual risk using
  - Event Tree
  - LOPA
- Calculate the necessary risk reduction to reach an acceptable level
  - Requires numerical expression of acceptable risk

Quantitative Risk Reduction

$$RR = \frac{Inherent\ Risk}{Acceptable\ Risk}$$

$$Safety\ Function\ PFDavg = \frac{1}{RR}$$

Summary

SIL Allocation

Given a complete hazard analysis:

- Define Safety Functions
- Allocate functions to OTBS, ES
- Define requirements for safety instrumented functions (SIF)
- Define SIL requirements for each SIF