The Risk of Using Risk Matrix in Assessing Safety Risk

Joint Seminar of HKARMS, HKIE-MMNC, CILTHK, and IMechE

16 November 2010

Vincent Ho

HAKRMS

Safety Engineering Lecture Series 2.2

Is your risk management regime working?

- How do you know your risk management methods/tools/techniques work or not?
- Would any organisation know if their risk management methods/tools/ techniques didn't work?
- What about the process itself?
- What would be the consequences if they didn't work
- Have you done a risk assessment of your risk management process?

The biggest single risk for any organization is the risk that its risk management doesn't really work – it is the ultimate "common mode failure"

Skepticism

- In defense of using some popular methods for safety and decision analysis, you may have heard (or said) the following:
  - "Our method is structured and formal"
  - "It helps us build consensus"
  - "It can be done quickly and within budget."
  - "It's easily understood by senior management"
  - "It's a proven method" (proven meaning somebody else did it this way and said they liked it)
  - "This is the best (or only practical) tool we have used"
- If someone can be an expert of a risk analysis method after a one-day workshop, then you should be suspicious of its applicability

3

Takeaways

- Risk management methods vary widely among industries but the most popular risk assessment methods are/may be the least effective
- There is a strong “placebo effect” in analysis - even a completely ineffective method would *feel* like it worked, particular when it is easy to master
- Even in organizations with extensive performance metrics, one of the most important measures is almost always ignored – the effectiveness of its risk management process

We will not complete a risk assessment of using risk matrix tonight but I hope this talk will stimulate your thinking in the effectiveness of using risk matrix and the associated risks

Topics to be Covered

- Understanding Risk
- Background of the Risk Matrix Application
- Types of Risk Matrices
- Issues in Using Risk Matrices

Power Point will be available at www.hkarms.org

Understanding Risk

Definitions of Risk

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}}$$

- Risk is never zero by increasing safeguards, as long as hazard is present
- Conceptually good but difficult to use in assessing risk

$$\text{Risk} = \text{Likelihood} \times \text{Consequence}$$

- Classical, most popular but most misleading
- More useful in hazard analyses

Definitions of Risk

- From Wikipedia
  - A risk is the ***total*** of each of the hazards that contribute to it.
  - The risk of any particular hazard, H, can be defined as its probability, P, multiplied by its consequence, C. In layman's terms: how likely it is to happen and how bad it would be if it happened.

$$H = P \times C$$

Same as last page

  - Therefore the total risk, R, of an event, e, is the sum of the *n* potential hazards that would result in that event:

$$R_e = \sum_{i=1}^{n} H_i$$

Have you ever added up the risks of individual hazards?

Definitions of Risk

$$\text{Risk} = \text{Uncertainty} \times \text{Consequence}$$

- Risk is usually associated with uncertainty and undesirability of a potential situation or event
- Without uncertainty or damage, there is no risk
- In order to have a risk situation, both elements must be present
- Anybody can guess extent of damage/Consequence but with different levels of uncertainties

This definition has been my favorite

Definitions of Risk

- From ISO 31000:2009 *Risk Management — Principles and Guidelines on Implementation;* ISO 73: *Risk Management - Vocabulary*
  - Published as a standard on the 13th of November 2009 for the implementation of risk management
  - Risk is defined as the "effect of ***uncertainty*** on objectives“
  - …to be applicable and adaptable for "any public, private or community enterprise, association, group or individual."

How often does your risk management system mention the word “uncertainty”?

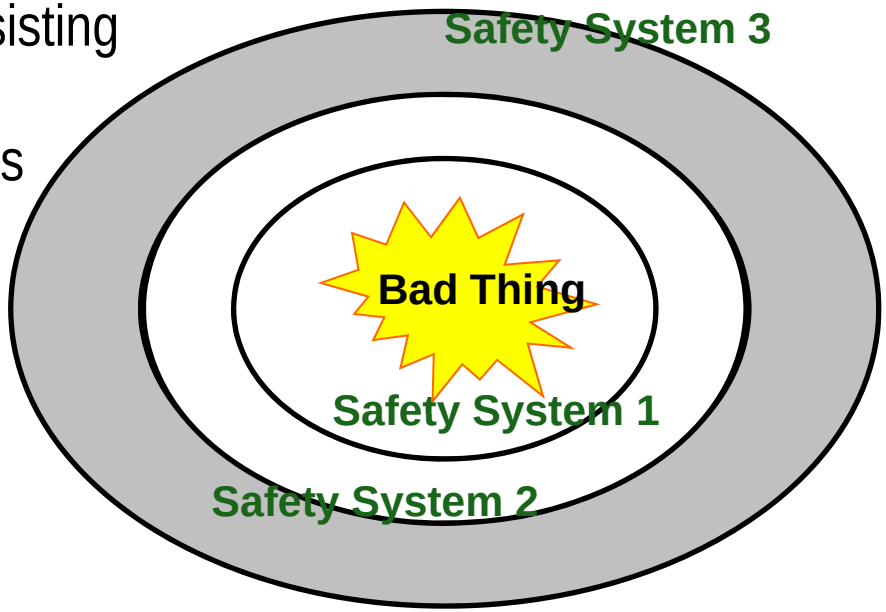
Sources of Uncertainties

- Stochastic uncertainties, parameter uncertainties, modeling uncertainties
  - No access to the whole truth (e.g., failure rates, consequence)
  - Impossible to explicitly specify all conditions
  - Inadequate or incorrect information on conditions
  - Inconsistent interpretation and classification of events
  - Lack of success data (for number of demands and exposure/mission time)
  - Limited data sample size; realised risk and unrealised risk
  - Imperfect mathematical and computer modelling of reality

In probabilistic (or quantitative) risk assessments, uncertainty is measured by level of belief; i.e., probability

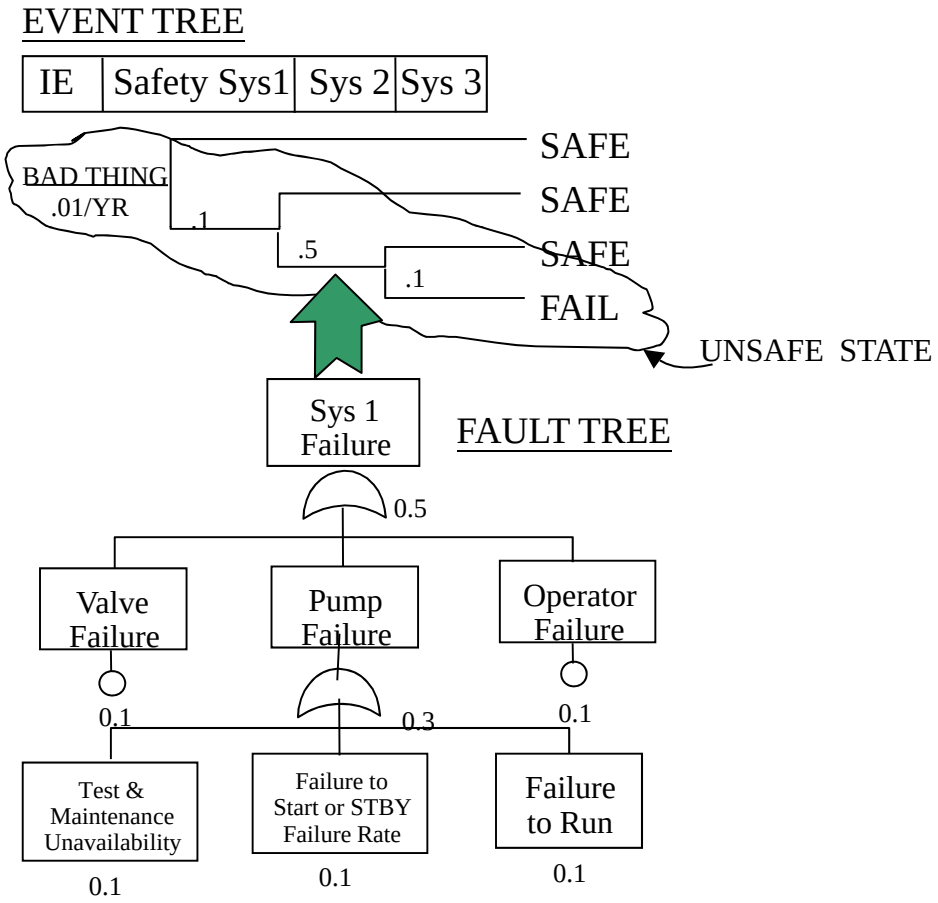
Quantitative Definition of Risk

- In general, risk is used to answer:
  - What can go wrong?
  - What are the damage effects?
  - How likely is it that this will happen?
  - What are the uncertainties?
- Thus, risk can be thought to be consisting of four elements:
  - Scenarios or accident sequences
  - Consequence
  - Likelihood
  - Uncertainties



Use of Probabilities in Risk Assessments

- In a QRA, we know what the Consequences (damage effects) and their contributing factors are, we want to know the Likelihood of these contributing factors
- Typically, you would first model the accident sequences using event tress and fault trees, then apply probability to assess the risk of reaching end states by each accident sequence



Total Risk is the sum of all paths leading to Unsafe State

Quantitative Definition of Risk

Scenario	Likelihood	Consequence
s_1	L_1	C_1
s_2	L_2	C_2
s_3	L_3	C_3
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
s_N	L_N	C_N

- Risk = $\{<S_i, L_i, C_i>\}$
- For each S_i, $Risk_i = L_i \times C_i$
- Total risk of the system is $R = \Sigma_i L_i \times C_i$
- L is expressed by probability of frequency in handling uncertainties

Background of the Risk Matrix Application

The Beginning of The Risk Matrix Era

- The arm race in the 1950s and 1960s generated a large number of systems that must meet mission objectives and safe to operate
- A System Safety Program grew out of the US aerospace and military programs to improve safety and system survivability
- This proactive system-level approach replaced the reactive, fly-fix-fly approach

- 1962: System Safety Engineering for the Development of Air Force Ballistic Missiles
- 1969: MIL-STD-882A, System Safety Program Requirements (882D is now being revised)

Mid-Std-882 System Safety Program Requirements

- To achieve acceptable risk through a systematic approach of hazard analyses, risk assessments, and risk management program throughout the life cycle of a project or activity
- The Mid-Std-882 series have introduced
  - RAMS criteria for system design
  - hazard analysis tools
  - Hazard logging system
  - Requirements for contractors
  - Documentation to satisfy approval authority

Hazard Evaluation

- The complexity of a hazard analysis depends on the scope, application and industry
- MIL-STD-882 suggests the use of worksheets with look up table or risk matrices to characterise the risk impact of hazards in terms of the likelihood and consequence mainly as preliminary screening analysis
- The application of the worksheet/ risk matrix approach to evaluate hazards has since become very popular in almost everywhere including safety analysis, terrorism risk analysis, project risk management, traffic safety, climate impact, ERM, etc.

Worksheet Method

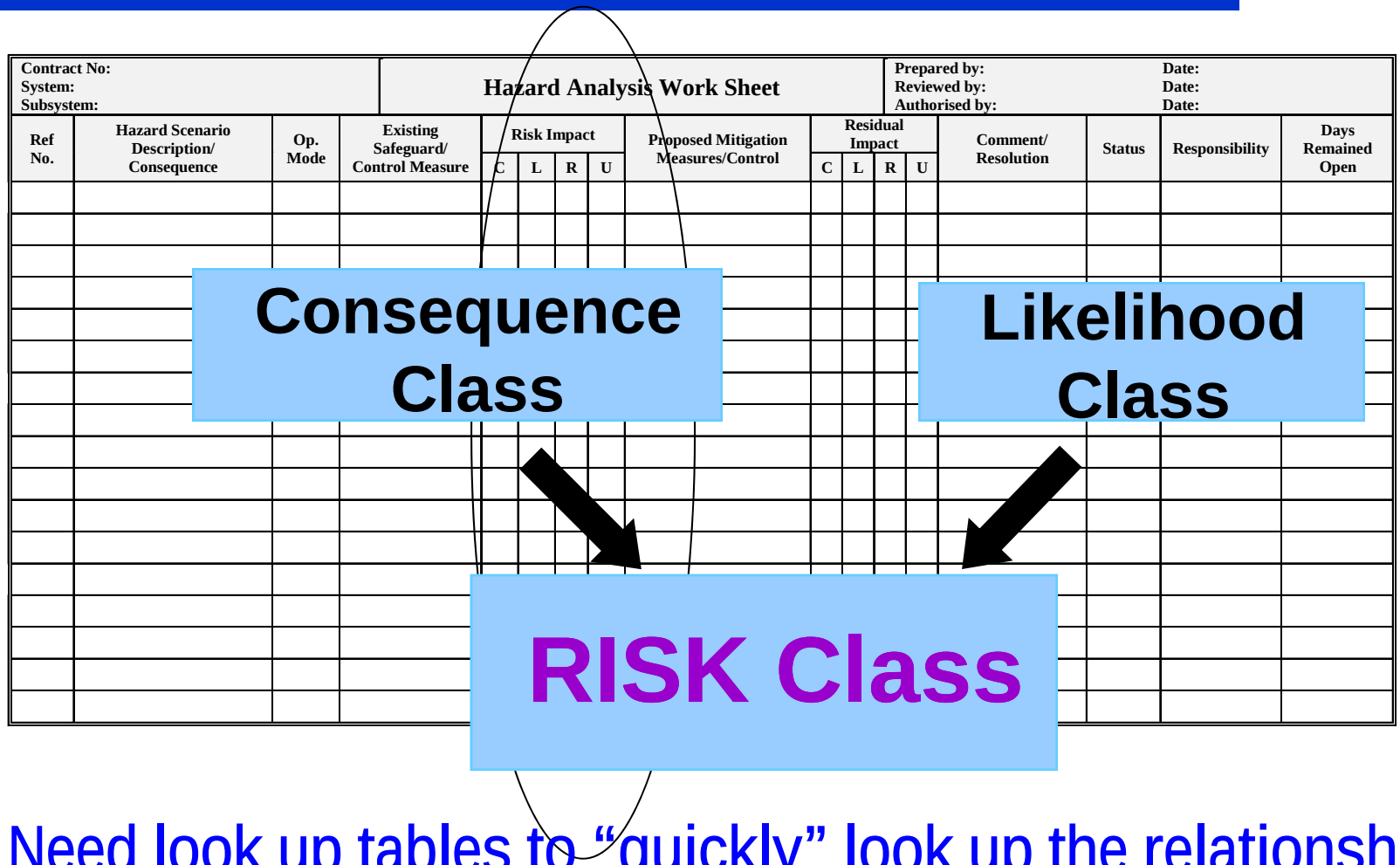
- For qualitative screening purposes or rank-ordering of hazard scenarios
- Each row is one hazard scenario *(almost an accident sequence!)* that gives one unique set of likelihood/ consequence /risk, which are then expressed as bins or classes
- Information contained must be adequate and concise – different analysts should be able to arrive the same set of likelihood/consequence/risk classes, today, and years later

Division:		**Hazard Scenario Summary Worksheet**						Prepared by:		Date:	
System:		**Study Title**						Reviewed by:		Date:	
Subsystem:								Authorised by:		Date:	

Ref No	Hazard Scenario Description	Potential Cause	Consequence	G	Existing Control Measure	Original Risk F	S	R	Respon-sibility	Proposed Control Measure	Proposed Risk F	S	R	Comment
	A concise description of the hazard shall be provided here. The description should describe the source of danger (hazard), or a failure condition. Not the consequence of exposure to a hazard; e.g., collision/ derailment are consequence and should not be included here in most cases.	A concise list of potential causes that can lead to the exposure of the hazard. Human errors should normally be listed here.	A reasonable worst-case consequence of the exposure of the hazard to the exposed group. List type of injuries and/or type of accident.		List existing operational measure or current design. "None" if no existing measure	This should consider existing measure or existing design.			Hazard owner or contractor	List proposed measures or design.	This should consider both proposed measures and existing measure if still present			

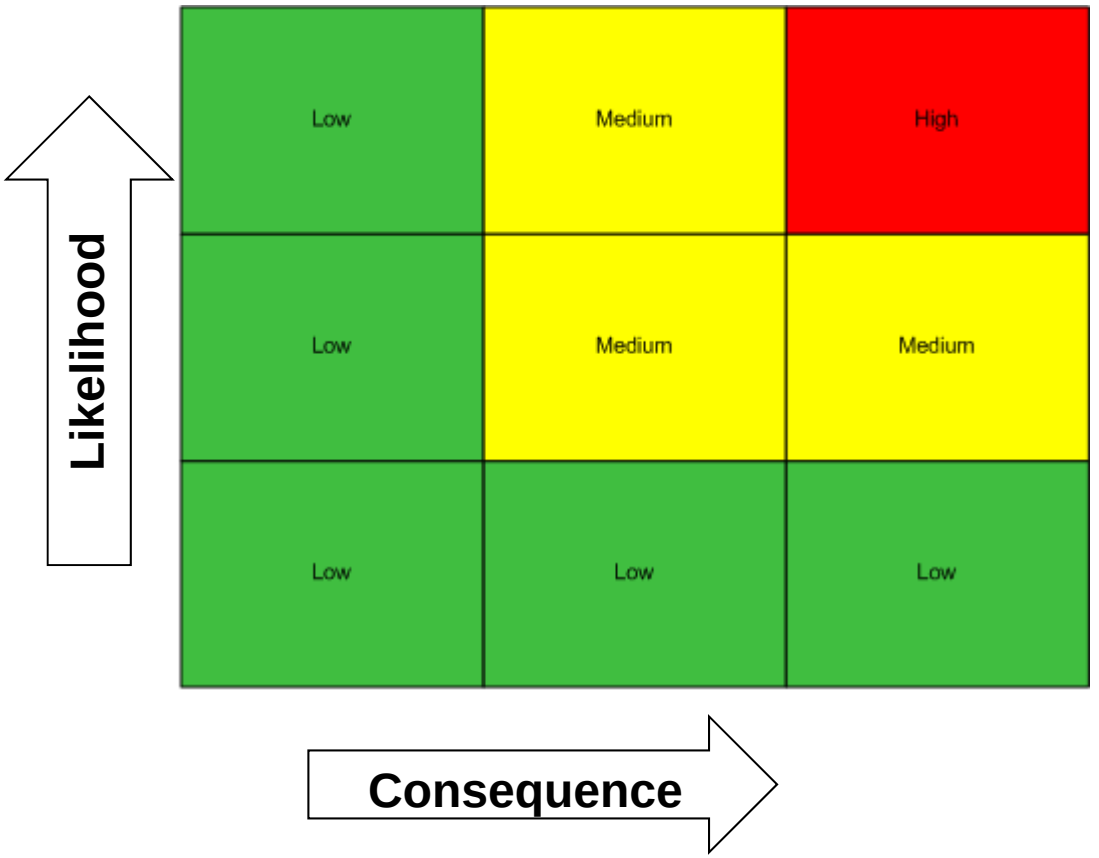
Strictly speaking, a worksheet type analysis is a Hazard Analysis, not a Risk Analysis

Risk is a Function of Scenario, Likelihood, Consequence

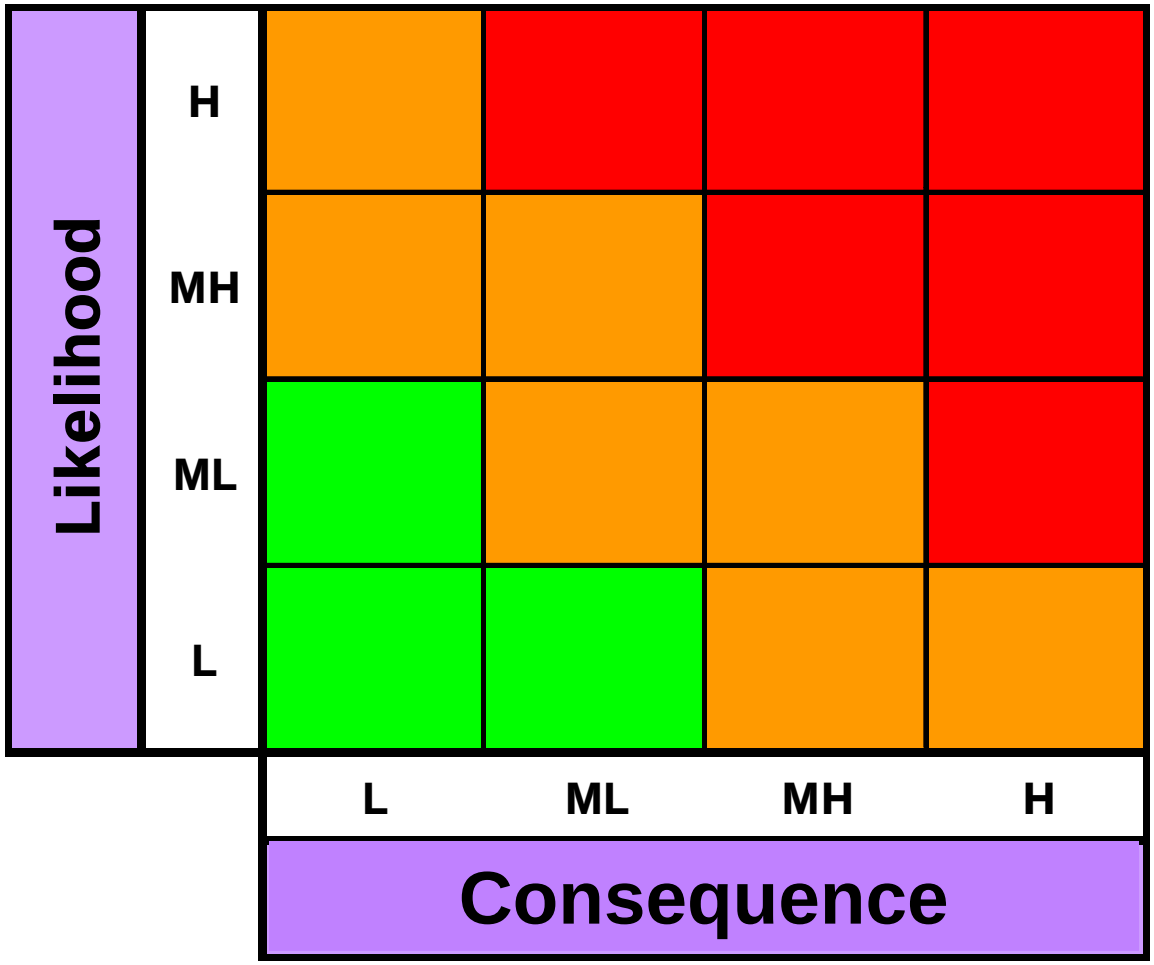


Need look up tables to “quickly” look up the relationship

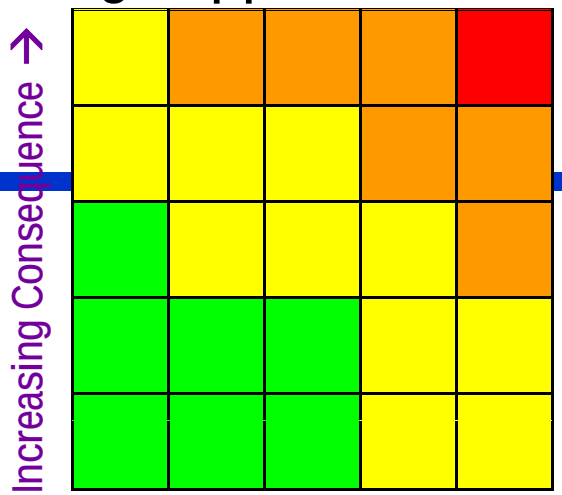
Orientation of a Risk Matrix



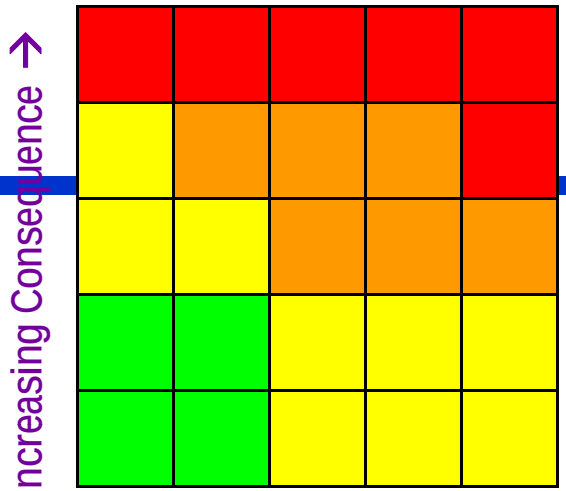
Risk Matrix Defines Your "Risk Appetite"



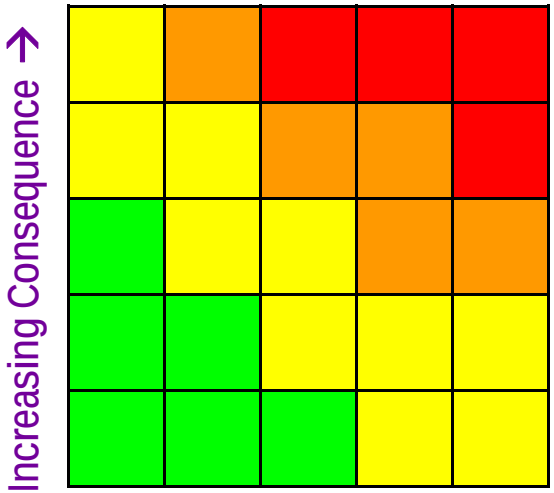
Large Appetite for Risk



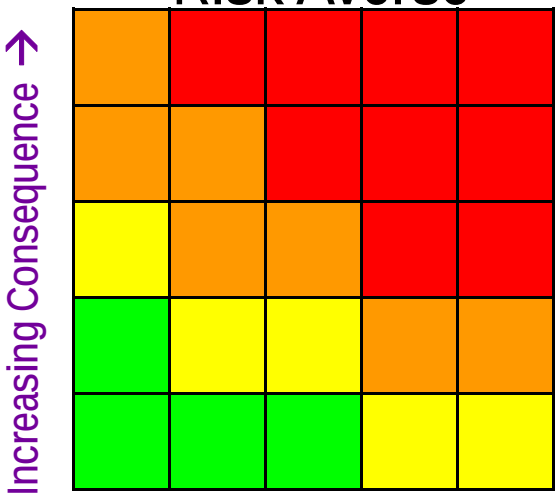
Plan for All Extreme Risks



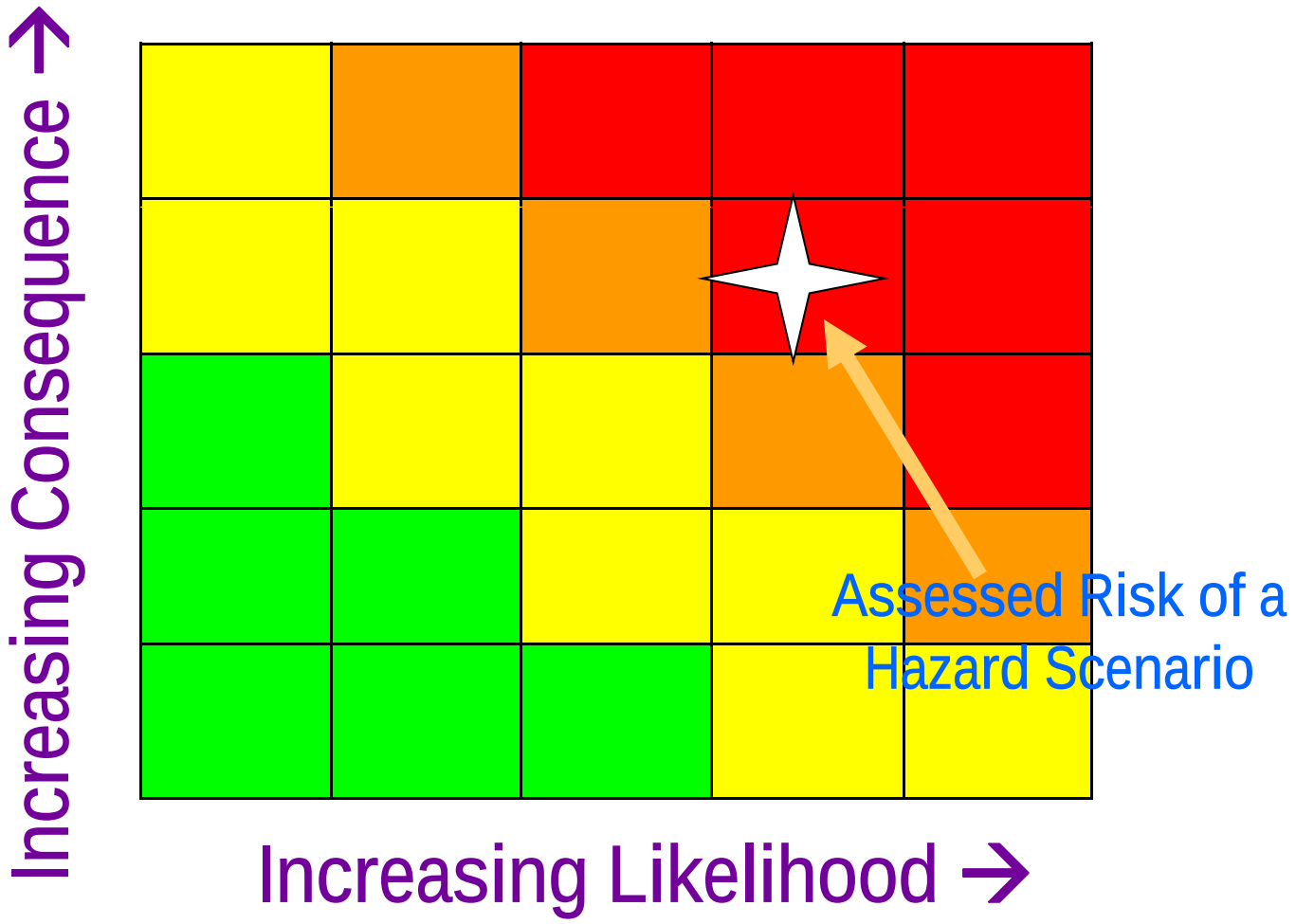
Standard



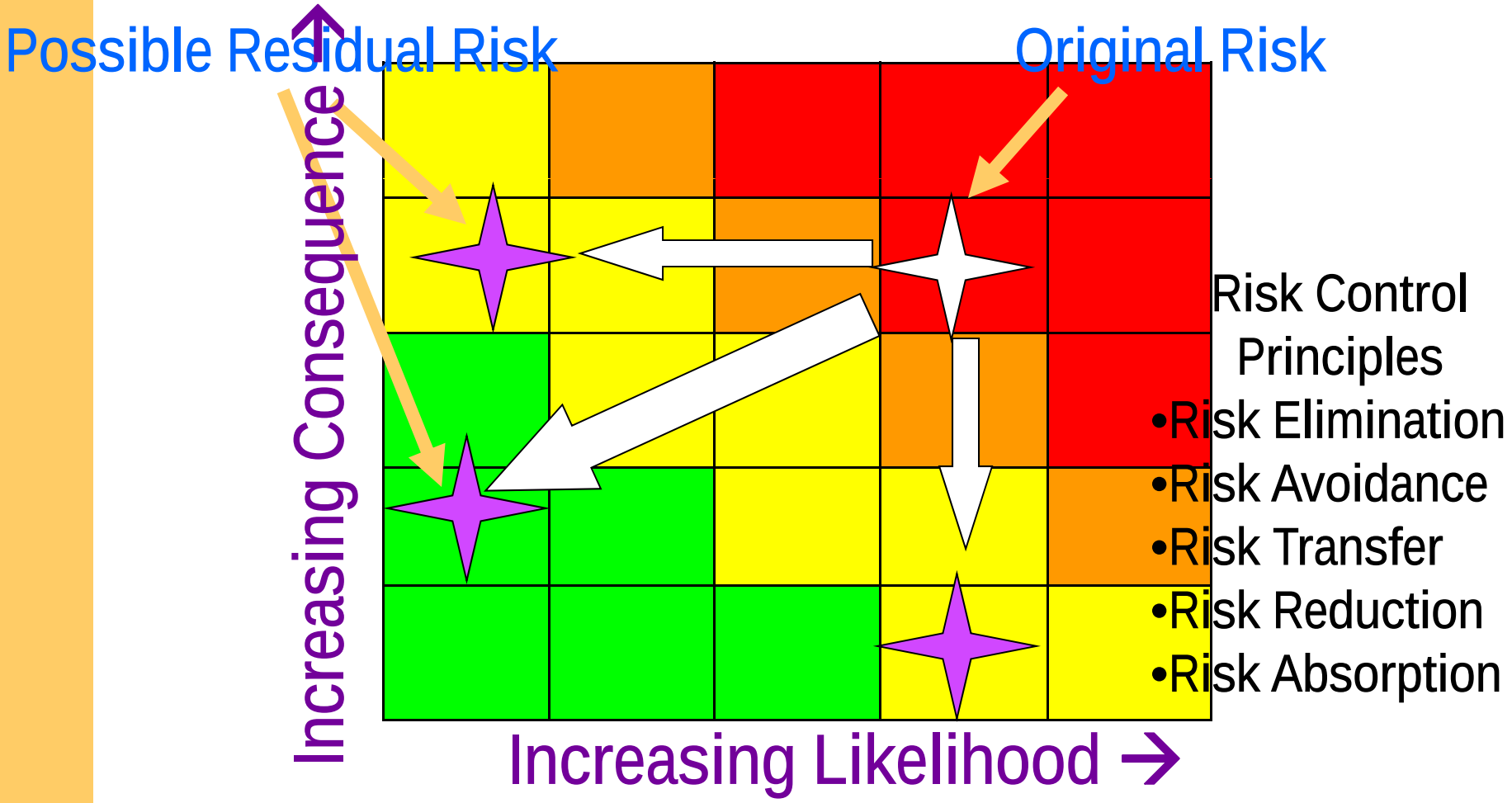
Risk Averse



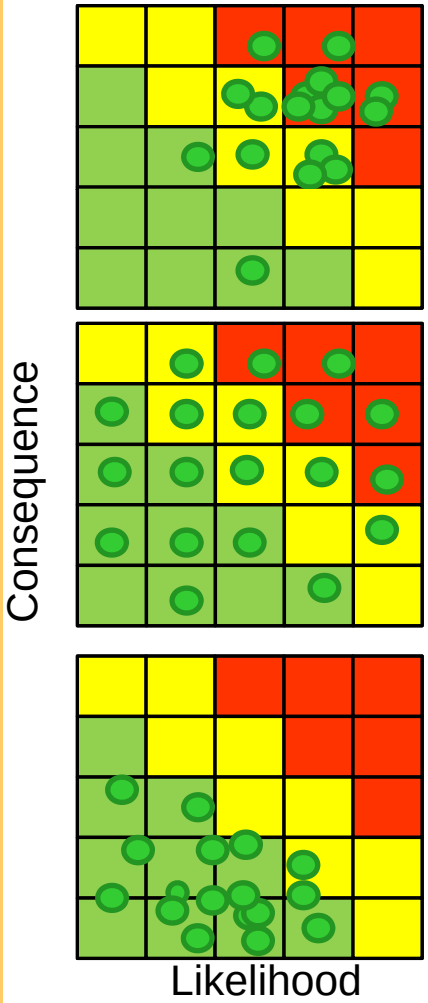
Application in Risk Control



Demonstrate Reduction in Risk Ranking



Pattern of Your Risk Profile



- Does your “Risk Map” look more like one of these charts?
  - Clustering or equally-spread risk mapping means that the risk matrix may not suit your operation
  - Risk profile changes as safety and risk management program mature, why not your risk matrix?

When was the last time your organisation updated its risk matrix?

Types of Risk Matrices

Risk Matrix Can be Simple

Risk Level	Description
High Risk	The hazard may cause fatal or multiple serious injuries, for all ranges of frequency
Medium Risk	The hazard may cause single serious injuries, and the likelihood of having these kinds of injuries is quite probable
Low Risk	Other risk which is neither high nor medium

MIL-STD-882 Mishap Severity Categories

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

MIL-STD-882 Mishap Mishap Probability Levels

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

MIL-STD-882 Mishap Risk Assessment Values

SEVERITY PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

Responsibility-Based

Typical Risk Matrix

Consequence / Likelihood		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain	A	S	S	H	H	H
Likely	B	M	S	S	H	H
Moderate	C	L	M	S	H	H
Unlikely	D	L	L	M	S	H
Rare	E	L	L	M	S	S

H = High risk - detailed research and management planning required at senior levels
S = Significant risk - senior management attention needed
M = Moderate risk - management responsibility must be specified
L = Low risk - manage by routine procedures

Action-Based

Typical Risk Matrix

		Consequence Class					
		R – Service-Related	C1 – Trivial	C2 – Minor	C3 – Serious	C4 – Critical	C5 – Disastrous
Frequency Class	F1 – Frequent (>10/yr)	R	B	A	A	A	A
	F2 – Common (1/yr to 10/yr)	R	B	B	A	A	A
	F3 – Likely (0.1/yr to 1/yr)	R	C	B	A	A	A
	F4 – Rare (0.01/yr to 0.1/yr)	R	C	C	B	A	A
	F5 – Unlikely (10^{-3}/yr to 0.01/yr)	R	D	C	C	B	A
	F6 – Improbable (10^{-4}/yr to 10^{-3}/yr)	R	D	D	C	C	B
	F7 – Incredible (<10^{-4}/yr)	R	D	D	D	C	C

Risk Class	Description
A	**High Risk** – Risk control measures should be implemented to mitigate the risk to a level that is ALARP with a top priority.
B	**Medium Risk** – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP within a reasonable time.
C	**Low Risk** – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP with a low priority.
D	**Negligible Risk** – Risk is considered acceptable; no additional risk control action is normally required. Cost-effective risk control measures may be implemented to further mitigate the risk with the lowest priority.

Priority-Based

Likelihood	Consequences				
	Severe (1)	Major (2)	Medium (3)	Minor (4)	Negligible (5)
Almost certain (A)	E	H	H	M	M
Likely (B)	H	H	M	M	L
Possible (C)	H	M	M	L	L
Unlikely (D)	M	M	L	L	T
Rare (E)	M	L	L	T	T

Hybrid Approach

- E — Extreme risk — Immediate action required; this level of risk needs detailed research and planning by senior management.
- H — High risk — Action plan is required as soon as practicable by senior management.
- M — Moderate risk — Action plan is required by Area/Department Manager within reasonable time
- L — Low risk — Managed by routine procedures and employees under supervision.
- T — Trivial risk — Unlikely to need specific application of resources.

THERE IS NO STANDARD RISK MATRIX

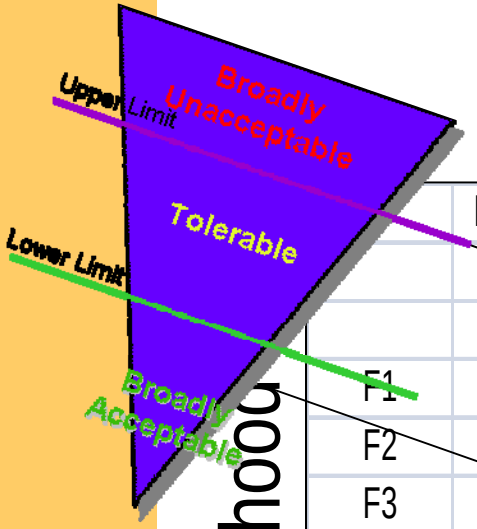
Risk Matrix using Scores

		Risk Levels				
Likelihood	High (0.9)	9	18	36	54	90
	Medium/High (0.7)	7	14	28	42	70
	Medium (0.5)	5	10	20	30	50
	Medium/Low (0.3)	3	6	12	18	30
	Low (0.1)	1	2	4	6	10
		Negligible (10)	Low (20)	Medium (40)	High (60)	Extreme (100)
		Impact				

This type of scoring matrix allows adding up of hazard risks

Issues in Using Risk Matrices (What Can Go Wrong?)

Risk Matrix Should be Designed by Quantitative Input



Consequence

Likelihood

Eqv Fatality		0	0.005	0.07	1	15
		C1	C2	C3	C4	C5
	Freq	0.00	0.02	0.26	3.87	38.73
F1	31.62	0.05	0.59	8.37	122.38	1224.75
F2	3.16	5.00E-03	0.06	0.84	12.24	122.48
F3	0.32	5.00E-04	5.92E-03	0.08	1.22	12.25
F4	3.16E-02	5.00E-05	5.92E-04	8.37E-03	0.12	1.22
F5	3.16E-03	5.00E-06	5.92E-05	8.37E-04	0.012	0.12
F6	3.16E-04	5.00E-07	5.92E-06	8.37E-05	1.22E-03	0.012
F7	0.00	5.00E-08	5.92E-07	8.37E-06	1.22E-04	1.22E-03

Is the design of your risk matrix based on Risk Acceptability Limits?

Issues in Designing Risk Matrix

Risk Assessment Matrix

SEVERITY	CONSEQUENCES				INCREASING LIKELIHOOD				
	People	Assets	Environment	Reputation	A	B	C	D	E
					Never heard of in the Industry	Heard of in the Industry	Has happened in our Organisation or more than once per year in the Industry	Has happened at the Location or more than once per year in our Organisation	Has happened more than once per year at the Location
0	No injury or health effect	No damage	No effect	No impact					
1	Slight injury or health effect	Slight damage	Slight effect	Slight impact					
2	Minor injury or health effect	Minor damage	Minor effect	Minor impact					
3	Major injury or health effect	Moderate damage	Moderate effect	Moderate impact					
4	PTD* or up to 3 fatalities	Major damage	Major effect	Major impact					
5	More than 3 fatalities	Massive damage	Massive effect	Massive impact					

Infer Risk and Value Equivalence

* Permanent Total Disability

MIL-STD-882 Mishap Severity Categories

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Introducing value of life, or cost of preventing fatality, etc.

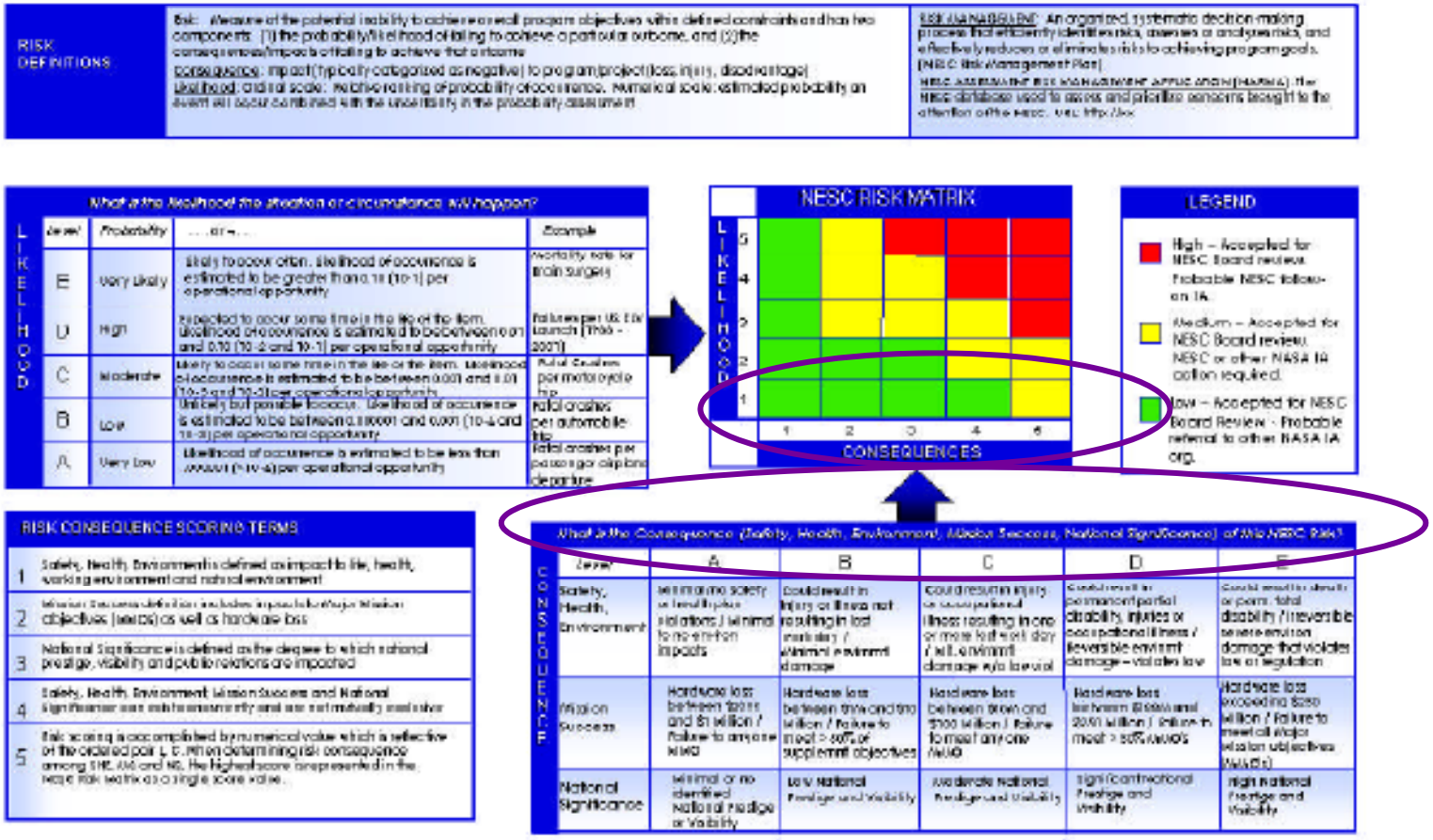
Issues in Designing Risk Matrix

Level	Descriptor	Description
1	Insignificant	Superficial injury/illness, no treatment or first aid only, low financial loss (less than $5k), requires no environmental remediation.
2	Minor	Medically treated injury/illness, medium financial loss ($5k to $50k). Short term environmental damage & minor remediation.
3	Moderate	LTI, no permanent impairment, <20 shifts lost, high financial loss ($50k to $100k), short term environmental damage & major remediation
4	Major	LTI, serious injury/illness & permanent impairment, >20 shifts lost, major financial loss ($100k -$500k), Long term environmental impact & major remediation.
5	Catastrophic	Fatality, toxic release offsite with detrimental effect, huge financial loss (More than $500k), long term environmental damage & major remediation

Are these values scalable?

For OSH use, not suitable for systems involving mass public

Issues in Designing Risk Matrix



Some typical mistakes…

Issues in Designing Risk Matrix

Rating	Likelihood	Consequence
6	Frequency greater than 10 times per year	Multiple deaths (4 or more); loss or harm of more than $100m within a financial year or forced shutdown of railway network (loss of franchise)
5	Frequency of 10 times per year	Deaths (1 to 3); loss or harm of between $10m and $100m within a financial year or extended adverse media campaign or a Judicial or Parliamentary enquiry (loss of franchise)
4	Frequency between once per month to once per year	Single death or multiple serious injuries; loss or harm of between $1m and $10m within a financial year or on-going national media coverage
3	Frequency between once per year and once every 10 years	Serious injuries; loss or harm of between $100k and $1m within a financial year or on-going State-based media coverage
2	Frequency of once per 10 years	Medical treatment; loss or harm of between $10k and $100k within a financial year or on-going local media coverage
1	Frequency less than once every 10 years	Minor injuries or nil treatment; loss or harm of less than $10k within a financial year or minimum media coverage

Are these values scalable?

BE CAREFUL WHEN DESIGNING A RISK MATRIX

(Bad) Example of Using Risk Matrix

Hazard	Consequence	Prob	Severity	Risk Class
Pump Room fire	**Both pumps fail**	**Med**	**High**	**A**

Severity / Probability	Low	Med	High
Low	D	C	B
Medium	C	B	A
High	B	A	A

- **Pump fire is medium probability in this facility**
- **Losing both redundant pumps will lead to plant damage**

(Bad) Example of Using Risk Matrix

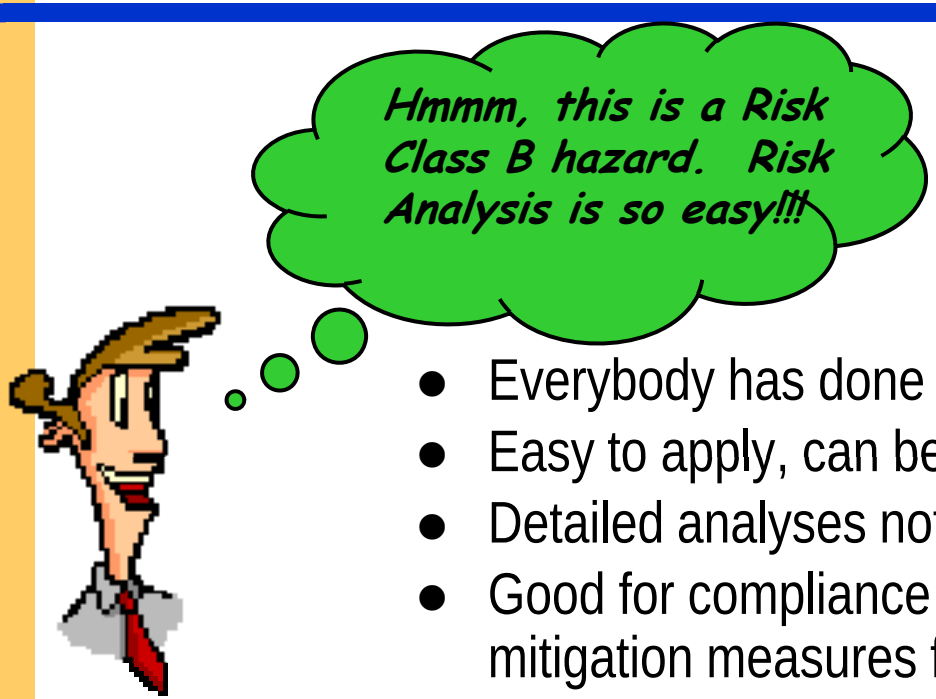
Hazard	Consequence	Prob	Severity	Risk Class
Pump A on fire	**Pump A damaged**	**Med**	**Low**	**C**

Severity / Probability	Low	Med	High
Low	D	C	B
Medium	C	B	A
High	B	A	A

A high risk location can be broken down into many sub-items (scenarios or rows in worksheet) with a lower risk for each sub-item

MIS-USE CAN CREATE FALSE SENSE OF SAFETY

Advantages of Worksheet/Risk Matrix



- Everybody has done at least one
- Easy to apply, can be used by non-experts
- Detailed analyses not required
- Good for compliance check and ensure consideration of mitigation measures for accidents/incidents
- Useful in evaluating a large number of alternatives with obvious differential risks
- Can be easily done in spreadsheet such as Excel

Disadvantages of Worksheet/Risk Matrix

- Results can be inconsistent between users
- Difficult to verify assumptions and results
- Difficult to identify common mode failures, system interactions, cascaded failures, complex situation, etc.
- Cannot compare alternatives in same risk class
- Cannot yield the total risk of a hazard, let alone for a system
- Can easily become “paper safety” and give a false sense of safety/security

DO NOT TREAT WORKSHEET/RISK MATRIX ANALYSIS AS THE END GAME

Assessing the Risk of Your Risk Management Process

- What can go wrong? (Issues, how, …)
- What are the damage effects?
- How likely is it that this will happen?
- What are the uncertainties?

"What's Wrong with Risk Matrices?"

- Source: *"What's Wrong with Risk Matrices?" T. Cox, Risk Analysis Vol 28,* suggests the following problems making risk matrix unsuitable to correctly assess risks:

☹ **Poor Resolution.** Typical risk matrices can correctly and unambiguously compare only a small fraction (e.g., less than 10%) of randomly selected pairs of hazards. They can assign identical ratings to quantitatively very different risks ("range compression")

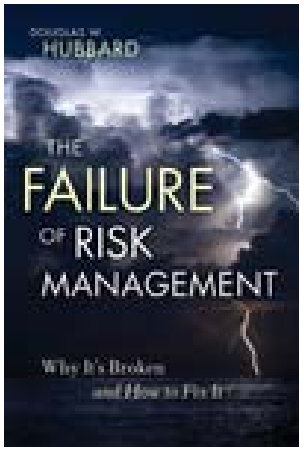
☹ **Errors.** Risk matrices can mistakenly assign higher/lower qualitative ratings to quantitatively smaller /larger risks. For risks with negatively correlated frequencies and severities, they can be "worse than useless," leading to worse-than-random decisions

☹ **Suboptimal Resource Allocation.** Effective allocation of resources to risk-reducing countermeasures cannot be based on the categories provided by risk matrices

☹ **Ambiguous Inputs and Outputs.** Categorizations of severity cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g., frequency and severity categorizations) and resulting outputs (i.e., risk ratings) require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks. These limitations suggest that risk matrices should be used with caution, and only with careful explanations of embedded judgments. Lock-on effect

Evidence of Effective Risk Management

- Source: "*The Failure of Risk Management: Why It's Broken and How to Fix It*" Douglas Hubbard suggests :



- ☺ Using calibrated probabilities to express uncertainties. risk analysis is an empirical science – it arises from experience
- ☺ Employing quantitative modelling techniques to model risks
- ☺ Developing an understanding of the basic rules of probability in quantifying risks
- ☺ Models should be built iteratively, testing each assumption against observation
- ☺ Lobbying for risk management to be given appropriate visibility in organisations
- ☺ Creating an organisation-wide approach to managing risks. This ensures that organisations will tackle the most important risks first, and that its risk management budgets will be spent in the most effective way

Evidence of Effective Risk Management

- ☺ Statistics based on large samples – the use of this depends on the availability of historical or other data that is similar to the situation at hand
- ☺ Direct evidence – this is where the risk management technique actually finds some problem that would not have been found otherwise
- ☺ Component testing – even if one isn't able to test the method end-to-end, it may be possible to test specific components that make up the method. For example, it may be possible to validate the risk matrix with known accidents or situations
- ☺ Check of completeness – organisations need to ensure that their risk management methods cover the entire spectrum of risks, else there's a danger that mitigating one risk may increase the probability of another
  - Internal completeness – covering all parts of the organisation
  - External completeness – covering all external entities that the organisation interacts with
  - Historical completeness – this involves covering worst case scenarios and historical data
  - Combinatorial completeness – this involves considering combinations of events that may occur together; those that may lead to common-mode failure discussed earlier.

Whether risk matrix is friend or a foe depends on your understanding of its limitations. It is a tool; use it well or you might be better off without it

End

Scoring Behavior & Error

- Source: "*Problems with scoring methods and ordinal scales in risk assessment*" Evan Hubbard suggests :
- ☹ Popular weighted scores add error to unaided human judgment - even if scales are "well defined" - by introducing an extreme rounding error (T. Cox)
- ☹ The use of scales simply obscures (doesn't alleviate) the lack of information and potential disagreements - it creates an "illusion of communication" (D. Budescu)
- ☹ "Partition dependence" creates an unanticipated relationship among choices on a scale. Two scales that each define a "1" in the same way (e.g. 1="impact less than $1M), will elicit different responses for a 1 depending on how many other choices there are (C. Fox)
- ☹ The anchoring effect means even the random order of assessments has an effect on judgments

Scoring methods are usually simple, but our behavior in using them is not