2015 SOEHK Symposium

The Do's and Don'ts in Risk Management – A Safety Practitioner's Perspective

5 June 2015

Vincent Ho, PhD

HKARMS
香港風險管理與安全協會
Hong Kong Association of
Risk Management and Safety

Contents

- What is risk management?
- How to apply risk management?
- What works and what doesn't?
- How to avoid the avoidable?

Have You Heard These Before?

- …this is how we do our business, there is no risk…
- …we don't need risk management, we have a small operation…
- …my managers are too busy to do risk management…
- …we don't have the money nor the time to apply risk management…
- …our business partner does not believe in risk management…
- …we have a low injury rate, we have no risk…
- …let's do a risk assessment to show we have low risk …
- …let's not make this a Level-A risk, be careful in what we report …
- ….you are the risk manager so you own the risk, I have no risk....
- …give me your risk report. If it works for you, it will work for us…
- My long time favorite:

…do not go that direction, what if you identify a hazard that we cannot control....

Why do we need Risk Management? – The Purpose

- Identify risk exposure/ levels/ profile
  – to see how big the bag is
- Rank hazards and risk control measures
  – to optimise resources, decide what to do and their cost-effectiveness
- Document decisions and due process
  – to address liability, what you have done to prevent the accident
- And do the above systematically
  – to minimise uncertainty and surprises

Making the right decision can reduce harm to individuals, risk management helps you to choose the optimal decision

What is Risk Management?

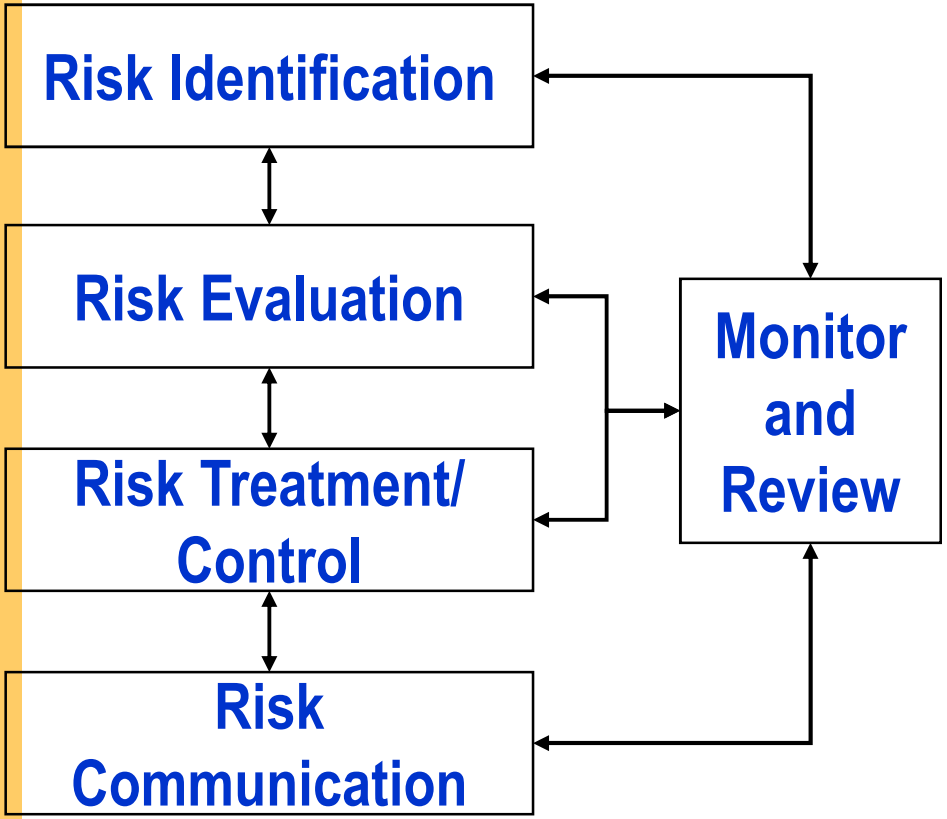
- Risk Management: coordinated activities to direct and control the organization with regard to risk
- Risk Management Framework: set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation
- Risk Management Process: systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk
- Risk Management should be embedded in all organisation's practices and processes in a way that it is relevant, effective and efficient. The risk management should become part of, and not separate from, those organisational processes

But What Does That Mean?

- A risk management programme includes a set of practices that lead to minimising possible harm to individuals
- While it may not be possible to totally protect every individual, a risk management system seeks to identify factors that may increase those risks and actively promote practices that will keep the risk at an acceptable level
- Risk management is the identification, assessment, and prioritisation of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximise the realisation of opportunities
- Risk management helps prioritise your resources in applying optimal control measures to reduce harm to individuals

"…my managers are too busy to do risk management…" ☹

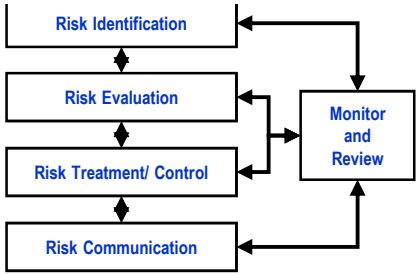
How to do it?
– Steps in a Risk Management Programme

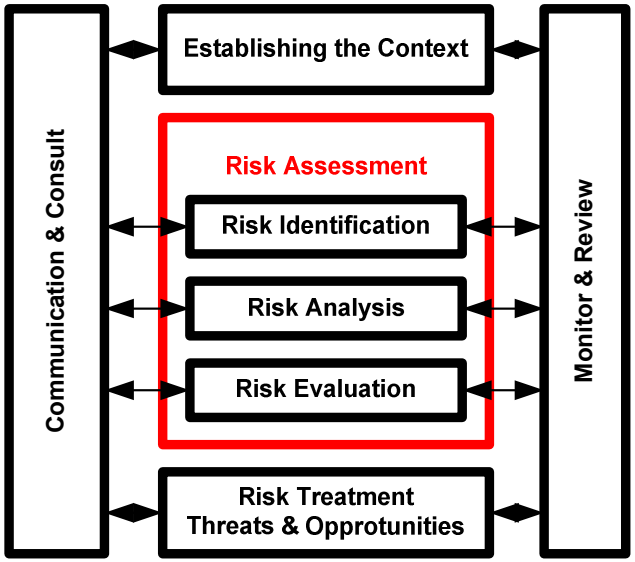


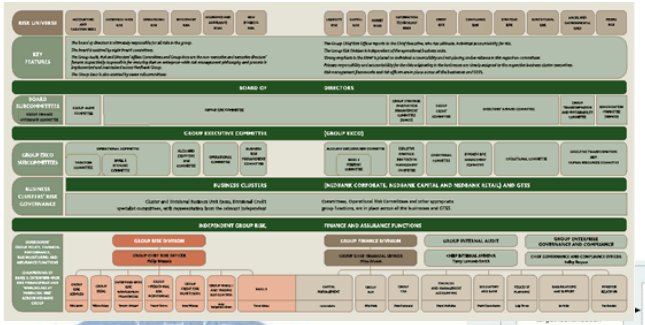
- Risk management programme is not a one-off activity
- These steps are often iteratively applied in phases, and are applicable to ALL businesses/ disciplines/ industries continually

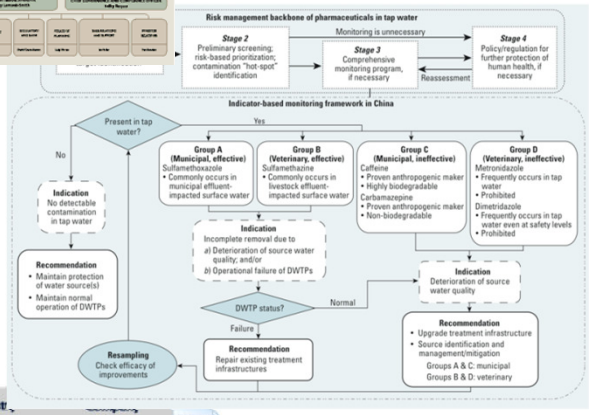
Which one is the most important step?

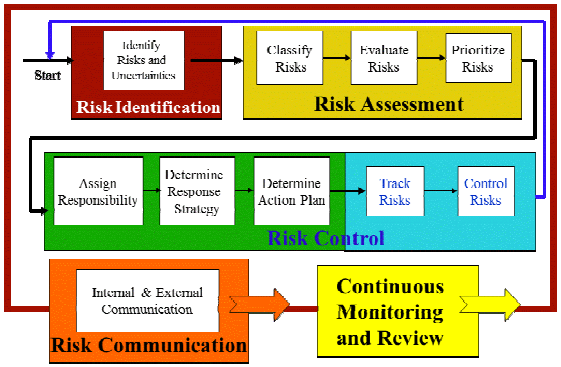
Risk Management Frameworks

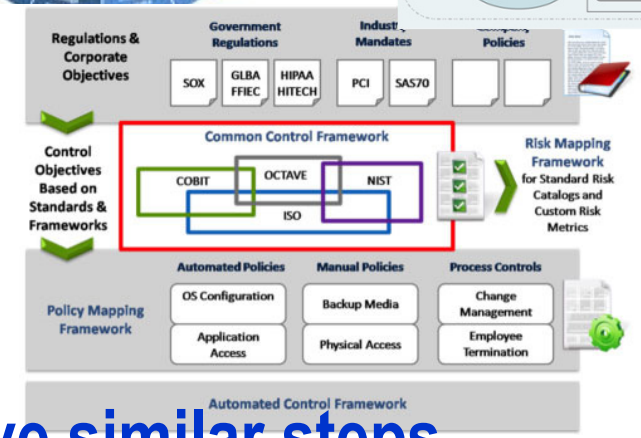






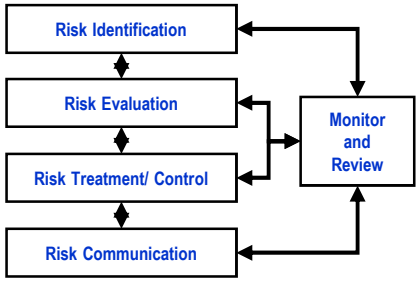






They all have similar steps

Risk Management Programme



DO

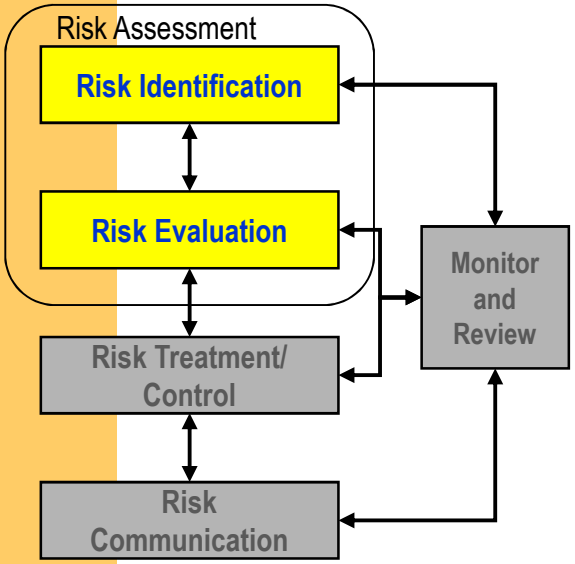
- Keep a simple programme to ease communication
- Involve all staff and relevant parties
- Allow sufficient and adequate resources to implement the programme

DON'T

- Treat risk management programme as an ad hoc one-off process but monitor regularly
- Compartmentalise information but share information between stakeholders
- Underestimate the complexity of risk management but seek external review and look for continuous improvement

Risk management is a life long process and needs to be fit-for-purpose

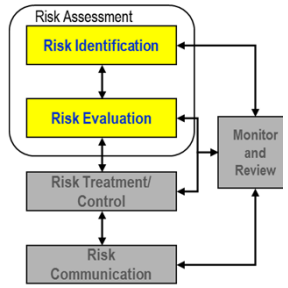
What Can Go Wrong in These Steps?



- Almost everyone under the sun is conducting risk assessment, from spilling water to Mars landing mission
- Check the box "Hazard X present or not" → is it a risk assessment?
- Risk assessment methods vary widely among industries but the most popular methods are usually 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

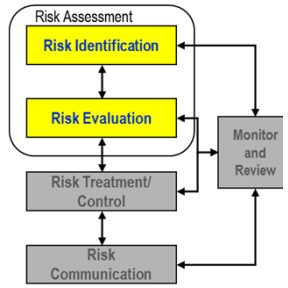
"…Let's not make this a Level-A risk, be careful in what we report …" ☹

Let's be Positive, so What *Does* Work in Risk Identification?



- Project and operational risks are effectively identified and managed holistically
- Risks are identified, studied and managed, not only in isolation but as an integral part of the business
- Embed risk identification in work process and promote active reporting of hazards
- Risk related to changes are carefully identified, assessed and managed
- Continually seek to reduce uncertainty by systematically acquiring additional knowledge and sharing good practice
- Employ audit and review to ensure relevant procedures are complied and effective
- Apply a structured method to leave no stone unturned
- Identify site-specific hazards
- Capture near-misses and precursors
- Document findings
- Centralise knowledge base

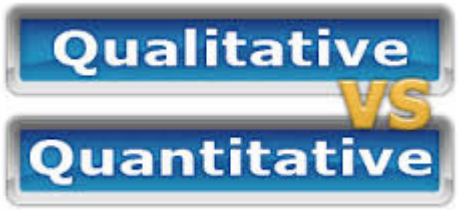
"…do not go that direction, what if you identify a hazard that we cannot control..." ☹



Statistics = Risk?

- Accident statistics are past events. They may not capture "unrealised risks" or rare events
- Can be biased due to limited data
- Cannot support new systems or those with little operating experience
- Often lead to ineffective allocation of resources in Cost/Risk-Benefit Analysis

"…we have a low injury rate, we have no risk…" ☹



Qualitative or Quantitative?

Qualitative Risk Analysis

- Prioritize the identified risks using a pre-defined rating scale or aspects
- Risks may be scored and ranked based on their likelihood of occurrence and the impact on objectives
- Relatively quick and simple to apply
- Can be subjective and difficult to trace the basis and findings
- Typically used in the preliminary analysis phase of a detailed risk assessment to screen out negligible risks

Quantitative Risk Analysis

- Typically used in the detailed analysis phase of a risk assessment to quantify the possible outcomes of accident scenarios and the probability of such occurrence
- Need high-quality data that may be hard to find
- Well-developed models are readily available but must be applied by trained users
- Findings are relative easy to trace and review

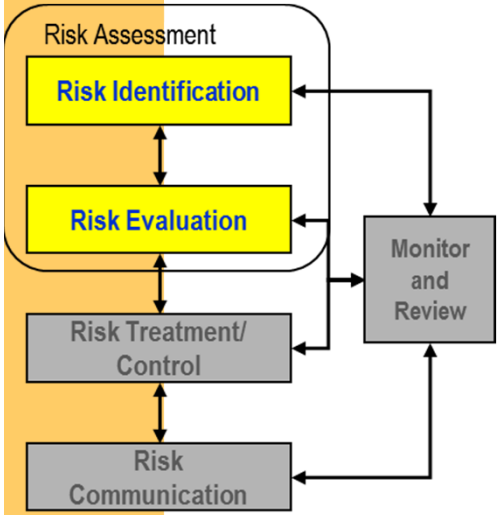
If you cannot quantify it, you cannot improve it

Skepticism to using Quantitative Tools

- "We don't trust the numbers."
- "It can't be done quickly."
- "We don't have all the data."
- "Something is always bothering me and it can't be expressed as numbers"
- "Our senior management does not understand the numbers."
- "Our current tool was developed by a senior manager years ago"
- "Our method is the best tool we have used (because it is the easiest)"

If you don't have the data, how can you assess the risk?

HKARMS



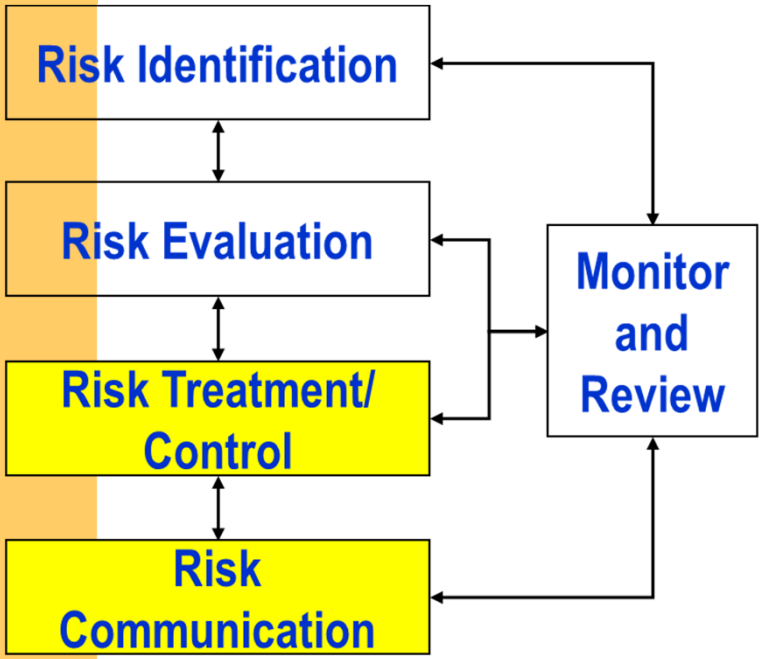
Do's

- ☺ Comprehensively include all reasonably foreseeable scenarios
- ☺ Adhere to evidence
- ☺ Apply logical and technically sound methods
- ☺ Be practical and reasonable
- ☺ Open to evaluation through peer professional review
- ☺ Base on explicit assumptions and premises
- ☺ Specialise to the system being analysed
- ☺ Conducive to learning as a living document
- ☺ Attune to risk communication to stakeholders

Don'ts

- ☹ Focus narrowly with unclear scope
- ☹ Conduct unsystematic and unclear scenario generation
- ☹ Underestimate the complexity of the system and data available
- ☹ Be overly subjective with no supporting evidence
- ☹ Apply only generic data without system-specific input
- ☹ Apply process that is difficult to understand with no open review
- ☹ Apply incorrect tools and techniques
- ☹ Present inconclusive outcome
- ☹ Be too deterministic with no account for uncertainties
- ☹ Be overconfident in applying expert judgment without any calibration

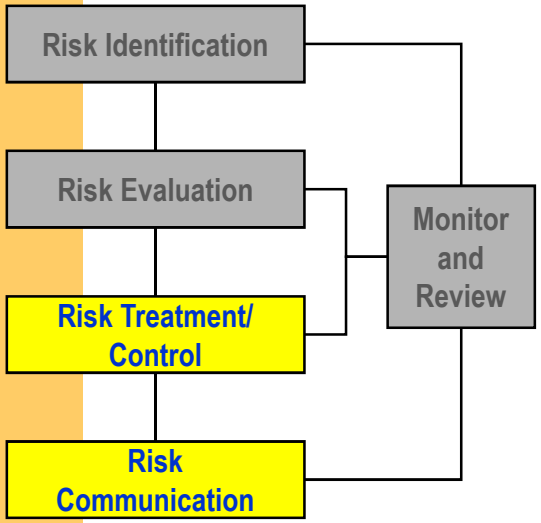
What to Do After You Have assessed the Risk?



- How safe is safe?
- What level and how much can you afford safety?
- What to do with the risk reports?
- How to communicate with stakeholders?

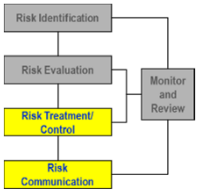
"…give me your risk report. If it works for you, it will work for us…" ☹

What Can Go Wrong in These Steps?



- We have the lowest accident rate, why are we doing more?
- Nothing will be done until there is an accident
- The residual risk is in the same risk class as the original risk, there is no need to do more
- Technical risk is difficult to understand, what if you find something we cannot manage
- The cheapest way to reduce the risk is usually useless, but the expensive way does not mean it is useful. Not common to see a robust cost/risk-benefit analysis being done

"…this is how we do our business, there is no risk… " ☹



Principles of Risk Control

- Risk Elimination
- Risk Avoidance
- Risk Transfer
- Risk Reduction
- Risk Absorption

Hierarchy of Risk Control – in Descending Order of Priority

- Elimination – remove the hazards all together
- Substitution – e.g., substituting with a less hazardous substance
- Isolation – e.g., isolate the hazards from any person exposed to it
- Engineering control – e.g., guard around machinery
- Administration control – e.g., training and work process
- Personal protective equipment (PPE)

Do not jump into issuing PPE until you have thought of other control measures

Barriers to Effective Risk Communication

- Lack of ownership
- "Bring me the solution, never the problem"
- Every department wants to do it their own way
- Lack of a common, agreed language or terminology
- Lack of a clear and consistent Risk Management champion
- Unclear or non-existent decision authority structure
- Silos of analyses and reporting of different risk types
- Maturity, governance, technology, process and people
- Inadequate resource allocation, ambiguous inputs and outputs
- Perception of a risk manager and roles/responsibilities
- Culture (How does the organisation operate?)
- Internal and external communication to stakeholders

"…our business partner does not believe in risk management..." ☹

Do's – What *Does* Work?

- Have a clear and consistent organisation-wide approach supported by leadership and stakeholders in managing and communicating risks across business units
- Tackle the most important risks first, and that the safety budgets will be spent in the most effective way
- Give risk management appropriate visibility in organisations with open communication engaging users and stakeholders
- Communicate lessons learnt between business units
- Document risk management process with maturity tracking
- Involve the front line staff in the risk control process
- Provide training to all involved in the risk management process
- Report incidents and near-misses timely and accurately

Last Words

- The biggest single risk for any organization may be the risk that their approach in applying risk management doesn't really work for them - it is the ultimate "common mode failure"
- Risk management methods vary widely among industries and the most popular are usually the least effective
- There is a strong "placebo effect" in analysis - even a completely ineffective method would feel like it worked
- Your perception of risks and your risk aversion changes daily due to irrelevant, random external influences
- Risks ultimately should be filtered to the lowest level possible for ownership and mitigation

Risk is the effect of uncertainty on objectives, whether positive or negative

Takeaway –
Do the Do's and Don't do the Don'ts

"….you are the risk manager
so you own the risk, I have no risk..." ☹

Thank You

End

Safety Corner: What are the Criteria for an "Acceptable" Risk Assessment?
(as appeared in Hong Kong Engineers, July 2010)

The objective of a risk assessment for a system is to find out what can go wrong (the scenarios) so that their impact can be prioritized (typically, by their likelihood and consequence). Effective measures can then be implemented to control the risks; thus, rendering the system safer to operate. Because the "true" total risk of a system will never be known without accepting a certain level of uncertainties, philosophically, there is no such thing as a "perfect" risk assessment. To make a risk assessment acceptable or being a "good" risk assessment, care must be taken in every step to ensure the process is done according to criteria. The following list of criteria or factors that lead to a "good" risk assessment is by no mean exhaustive but forms the general characteristics that you would expect to find in a "good" risk assessment:

1. Comprehensive to include all reasonably foreseeable scenarios
2. Adherent to evidence
3. Logical and technically sound
4. Practical and reasonable
5. Open to evaluation through peer professional review
6. Based on explicit assumptions and premises
7. Compatible and specialised to the system being analysed
8. Conducive to learning as a living document
9. Attuned to risk communication to stakeholders
10. Innovative but does not reinvent the wheel

So, what are the characteristics of a "bad" risk assessment? These are the common symptoms:

1. Narrowly focused with unclear scope
2. Unsystematic and unclear scenario generation
3. Underestimate of the complexity of the system and data available
4. Overly subjective with no supporting evidence
5. Only generic data used without system-specific input
6. Difficult to understand with no open review
7. Incorrect application of tools and techniques
8. Inconclusive outcome
9. Too deterministic with no account for uncertainties
10. Overconfidence in applying expert judgment without any calibration

==========

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho@UCLA.edu

Safety Corner: What are the Seven Sins of a Risk Assessment?
(as appeared in Hong Kong Engineers, August 2010)

In the last issue we have discussed the general characteristics one can find in a "good" and a "bad" risk assessment. In this issue, we will highlight some of the more egregious errors found in quantitative risk assessments (QRA). These deadly sins are to be avoided at all costs before laymen losing respect to the application of QRA.

1. Lack of a clear defined scope. A clear defined scope can dictate the complexity and details, and also set the course of a QRA.
2. Calling a hazard assessment a quantitative risk assessment. Analyses using risk matrix to assign risk classes to hazard scenarios, or analyses that do not provide summation of risks are not QRA and should only be called hazard assessments. A QRA must be able to provide the total risk of a situation.
3. Using generic data without data specialisation. A QRA uses generic data without any system specific data can only reflect the risk of a generic situation but never the risk of the systems being analysed.
4. Terminology confusion. We are often bombarded with terms used by analysts who insist they mean different things, and have also seen many practitioners start to make up their own terms and methods, although they are merely a slightly modification over exiting methods.
5. Overly complex (or simplistic) risk assessment. If you can assess the risk with proven methods, there is really no need to make things too complicated. On the other hand, one must also not to conduct an overly simplistic assessment of a complex situation.
6. Incorrect application of tools and techniques. One general mistake is the misuse of tools due to the lack of an understanding of the fundamentals. For instance, fault tree is based on probability theory and therefore, one cannot propagate frequency terms (which have units) in a fault tree without special treatment.
7. Making QRA the end game. A QRA is a snap shot of a situation, and unless conducted periodically or actively (as in the case of risk monitors), the risk may change with time and input conditions.

==========

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho@UCLA.edu

HKARMS

Safety Corner: What are the Do's and Don'ts in Risk Assessment?

(as appeared in Hong Kong Engineers, June 2015)

Risk assessment methods vary widely among industries but many popular methods are actually ineffective, let alone technically flawed. There is a strong placebo effect, even an ineffective method would feel like it worked, particular when it is easy to apply and easy to be accept by senior management. Unfortunately , the cheapest and easiest way to reduce the risk is usually useless, although the expensive way does not necessarily mean it is useful. The following general Do's and Don'ts can serve as a checklist to avoid conducting a meaningless risk assessment.

The Do's

- Apply a structured method to ensure all reasonably foreseeable accident scenarios are systematically identified
- Involve front line staff and relevant parties in the scenario identification process
- Account for incidents and near-misses when building up accident scenarios
- List explicitly key assumptions and bases
- Develop application-specific database to support the risk models
- Apply Bayesian data update in handling generic data and plant-specific data
- Apply robust tools in assessing risks
- Conduct uncertainty analysis in characterising risk
- Conduct sensitivity analysis to understand the results
- Document risk assessment process
- Open to evaluation through professional peer review
- Communicate the risks to stakeholders
- Continually seek to reduce uncertainty by systematically acquiring additional knowledge

The Don'ts

- Conduct a risk assessment using generic data unless it is a scoping study
- Leave scope narrowly focused with unclear boundary conditions
- Generate arbitrary, unsystematic and unclear scenarios
- Underestimate of the complexity of the system and data available
- Apply data with no supporting evidence
- Finalise the assessment report without going through any open review
- Apply incorrect application of tools and techniques
- Present inconclusive outcome
- Ignore the uncertainty nature in data and models
- Apply expert judgment without any calibration and evidence
- Forget toe communicate with stakeholders

==========

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho@UCLA.edu