MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

Engineering Curriculum Without a Common Body of Knowledge (CBoK) for Risk Based Decision-Making: A Recipe for Disaster?

Dr. M. Sam Mannan, PE, CSP, DHC, FAIChE, FIChemE, PPSE
Regents Professor and Executive Director
Holder of the T. Michael O'Connor Chair I
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University System

Uncertainty and Decision Making

Don Rumsfeld Known Known.mp4

Known Unknowns	Unknown Unknowns
Things that are known that we don't know	Things that we don't know that we don't know (Unfathomable Uncertainty)
Identified risk	***Unidentified risk***
Known Knowns	**Unknown Knowns**
Things we know that we know	We are negligent in our pursuit of knowledge. Impact is unknown but the existence is known.
Knowledge	

Hillson (2010), Exploiting future uncertainty: Creating value from risk, Surrey, UK

Risk: Common Body of Knowledge (CBoK)

1. Probability and Statistics
2. Hazard and Risk – Understanding the meaning and talk the language
3. Risk Mitigation
4. Systems Thinking: Complexity, Neutral and Engineered
5. Risk Identification and Analysis
6. Management of Change (MOC)
7. Managing Risk Across Life Cycle
8. Ethics, Culture, Values – Legal and regulatory requirements
9. Learning from Events or Incidents
10. Risk Receptors, Impacts and Multi-dimensional Uncertainty
11. Concepts of Function, and Failure (things fail)
12. Dynamic and Operational Risk Analysis
13. Humans in Engineered System

Risk: Common Body of Knowledge (CBoK)

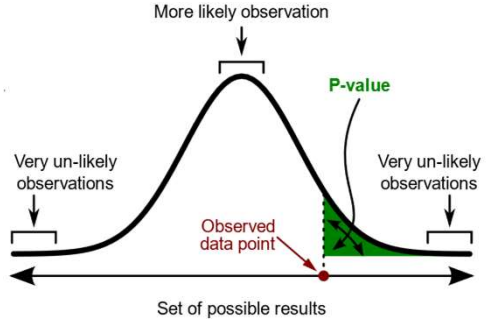
14. Data, Information, and Knowledge
15. Trade-offs : Technical, Economic
16. Perception and Awareness : Self, Situational
17. Indicators : Leading and Lagging
18. Competence, Limitations, and Roles
19. Emergency Response (ER)
20. Questioning Mentality with Professional Disposition
21. Courage and Humility
22. Diversity, Discipline, Culture and Experience
23. Safety Management System
24. Socio-Technical System
25. Resilience Engineering
26. Multidisciplinary Activity

1. Probability and Statistics

Probability

Given Model

Predict Data

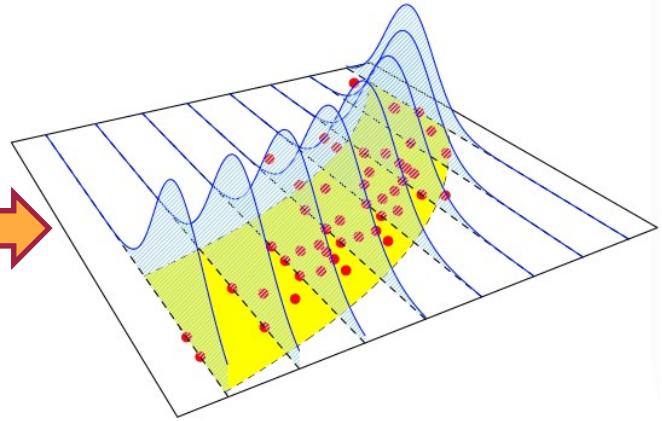


"Take the probability of loss times the amount of possible loss from the probability of gain times the amount of possible gain. That is what we're trying to do. It's imperfect, but that's what it's all about." **Warren Buffett**

Statistics

Given Data

Predict Model



"There are three kinds of lies: lies, damn lies, and statistics" **Mark Twain**

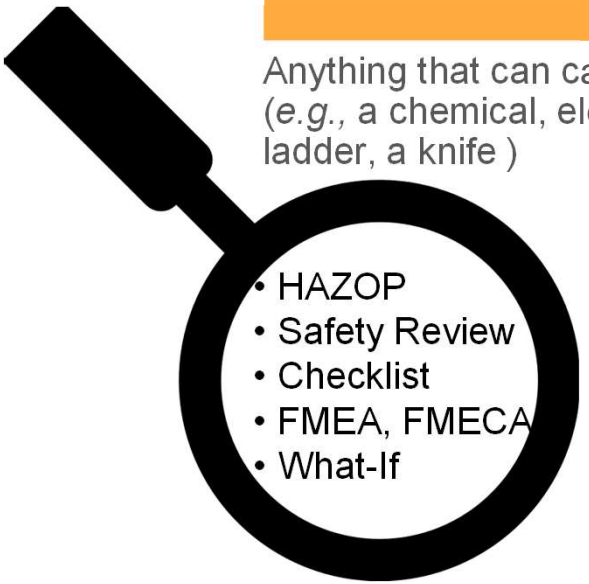
2. Hazard and Risk

Hazard

Anything that can cause harm (*e.g.*, a chemical, electricity, ladder, a knife)

Risk

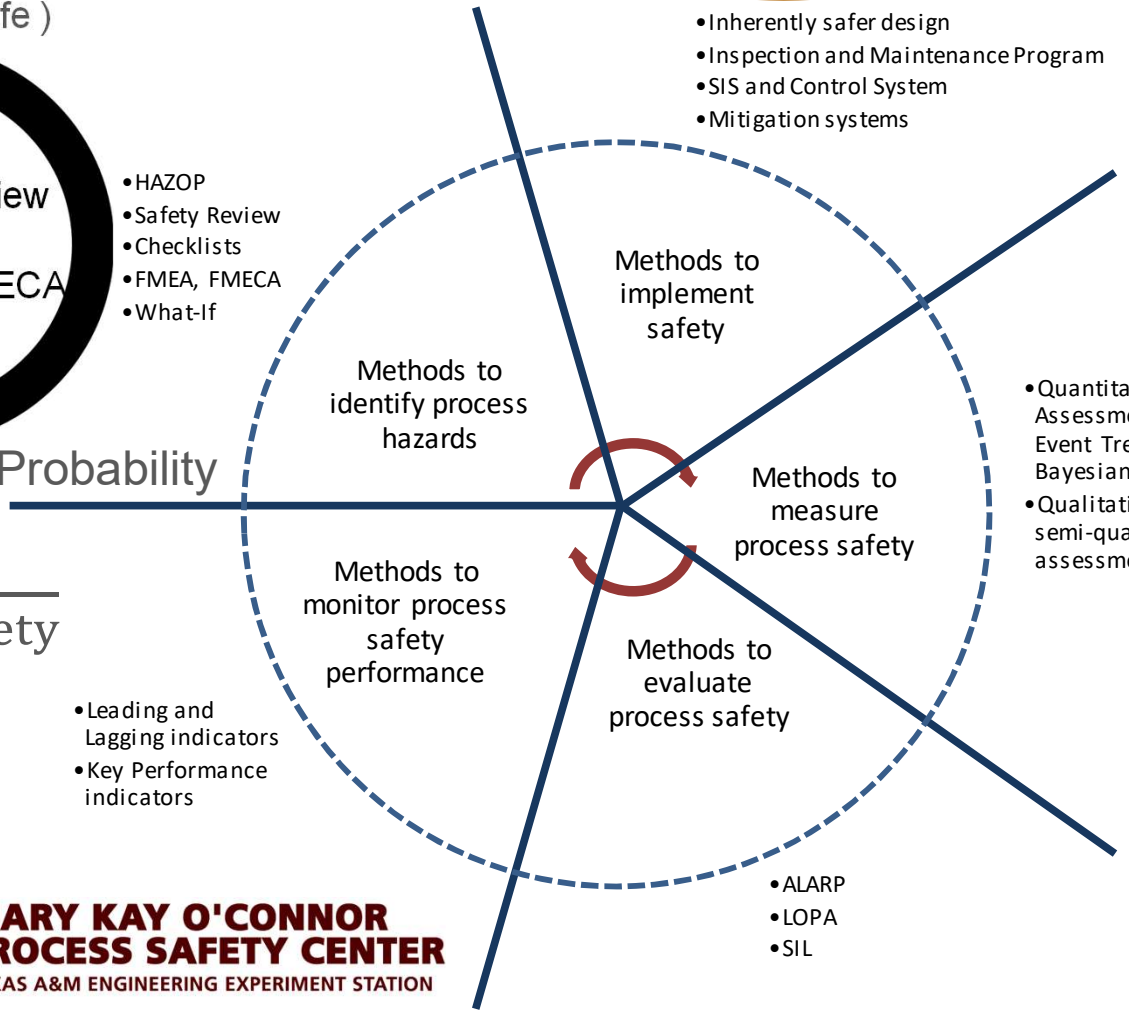
How great the chance that someone will be harmed by the hazard



- HAZOP
- Safety Review
- Checklists
- FMEA, FMECA
- What-If

Risk = Consequence x Probability

$$\text{Or, Risk} \propto \frac{1}{\text{Safety}}$$



- Inherently safer design
- Inspection and Maintenance Program
- SIS and Control System
- Mitigation systems

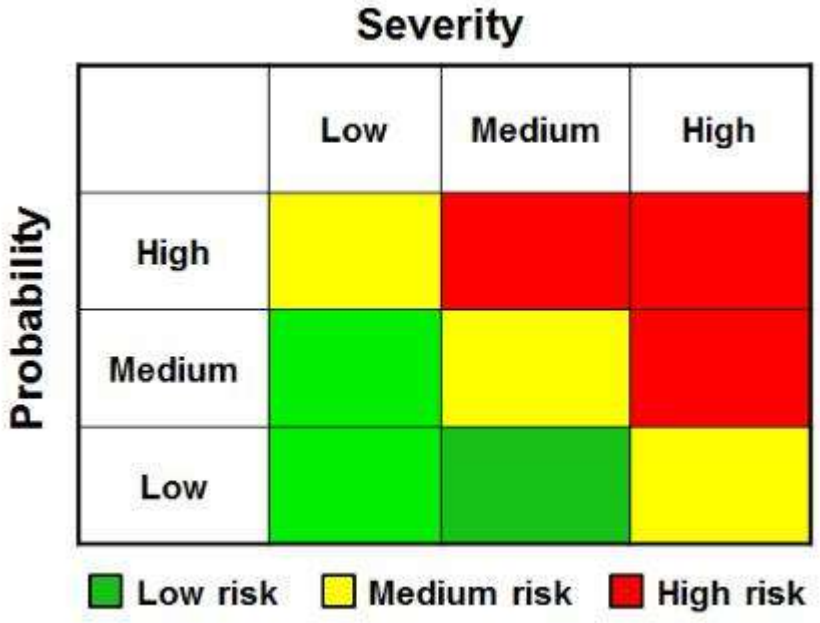
- Quantitative Risk Assessment (Fault Tree, Event Tree, Bow-Tie, Bayesian Network)
- Qualitative (Risk Matrix) and semi-quantitative risk assessment (LOPA)

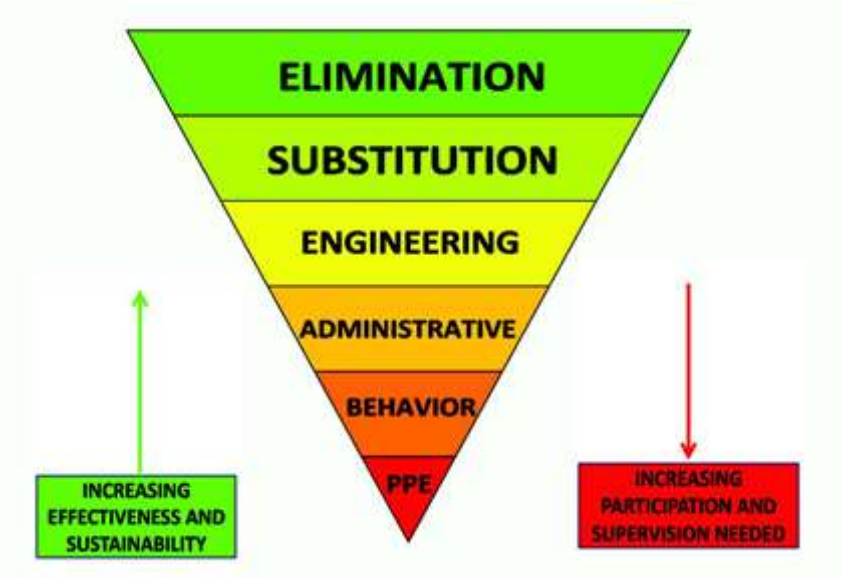
- Leading and Lagging indicators
- Key Performance indicators

- ALARP
- LOPA
- SIL

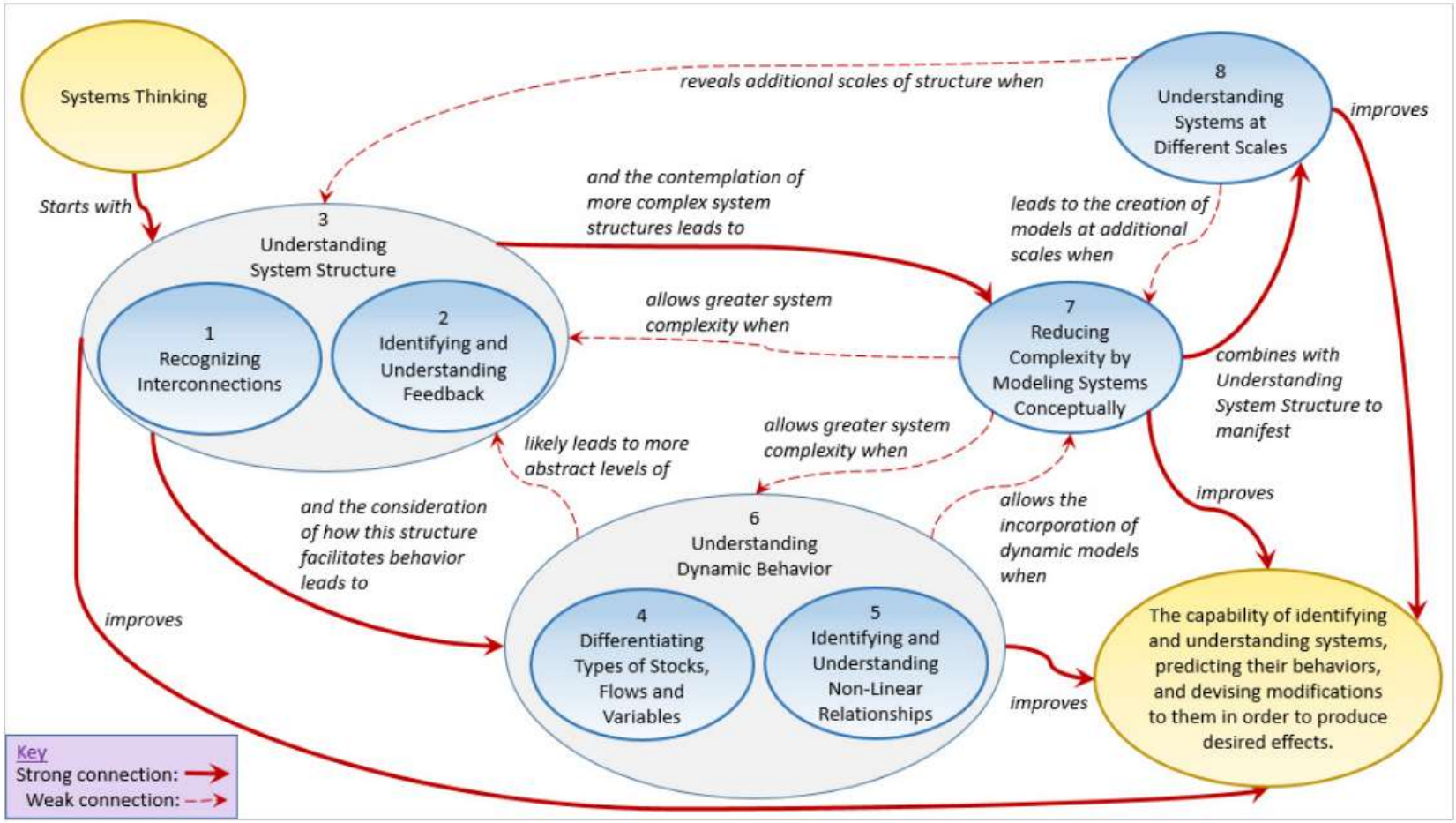
3. Risk Mitigation

- Inherently Safer Design
- Engineering Controls
  - Passive Barriers
  - Active Barriers
- Administrative Controls
- Personal Protective Equipment
- Avoid Risk Transfer or Migration
  Consider Life Cycle Approach





4. Systems Thinking: Complexity, Neutral and Engineered



Procedia Computer Science 44 (2015) pp. 669 – 678

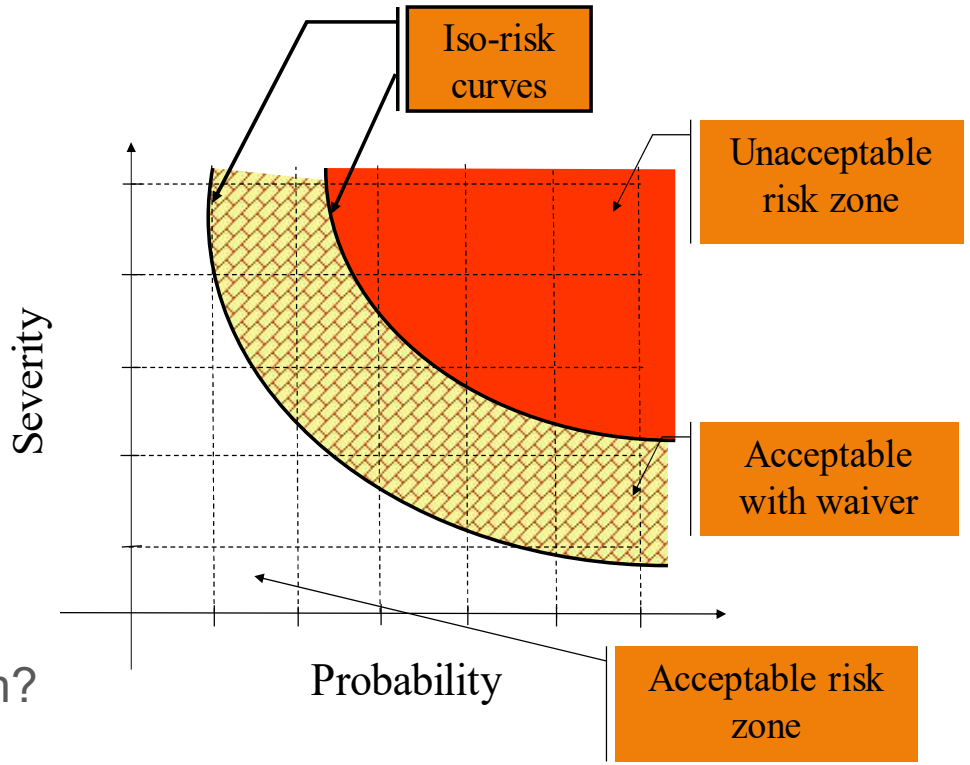
5. Risk Identification and Analysis

We accept (tolerate) risk in three cases:

- We do not know that it exists
- The risk is insignificantly low
- When it's worth the risk

Counter measures to reduce risk:

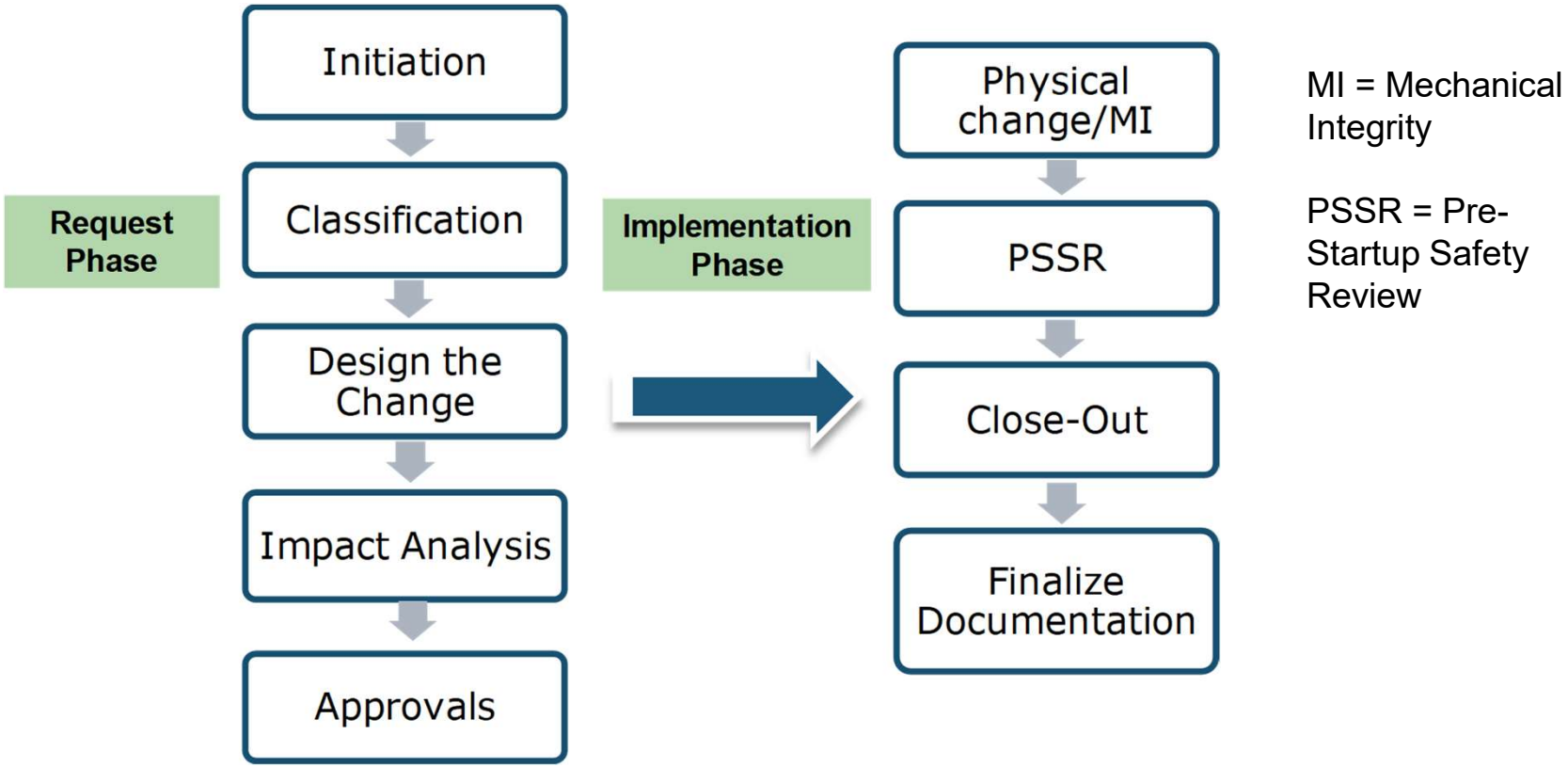
- Consider: Effectiveness, feasibility and cost
- Does the new counter measure introduce new hazards?
- Does the new countermeasure impair the performance of the system?
- Management of Change (MOC)



High Consequence and Low Probability Events ("Perfect Storm" = Multiple Threats occurring coincidentally; "Black Swan" = Unknown Threat)

6. Management of Change (MOC)

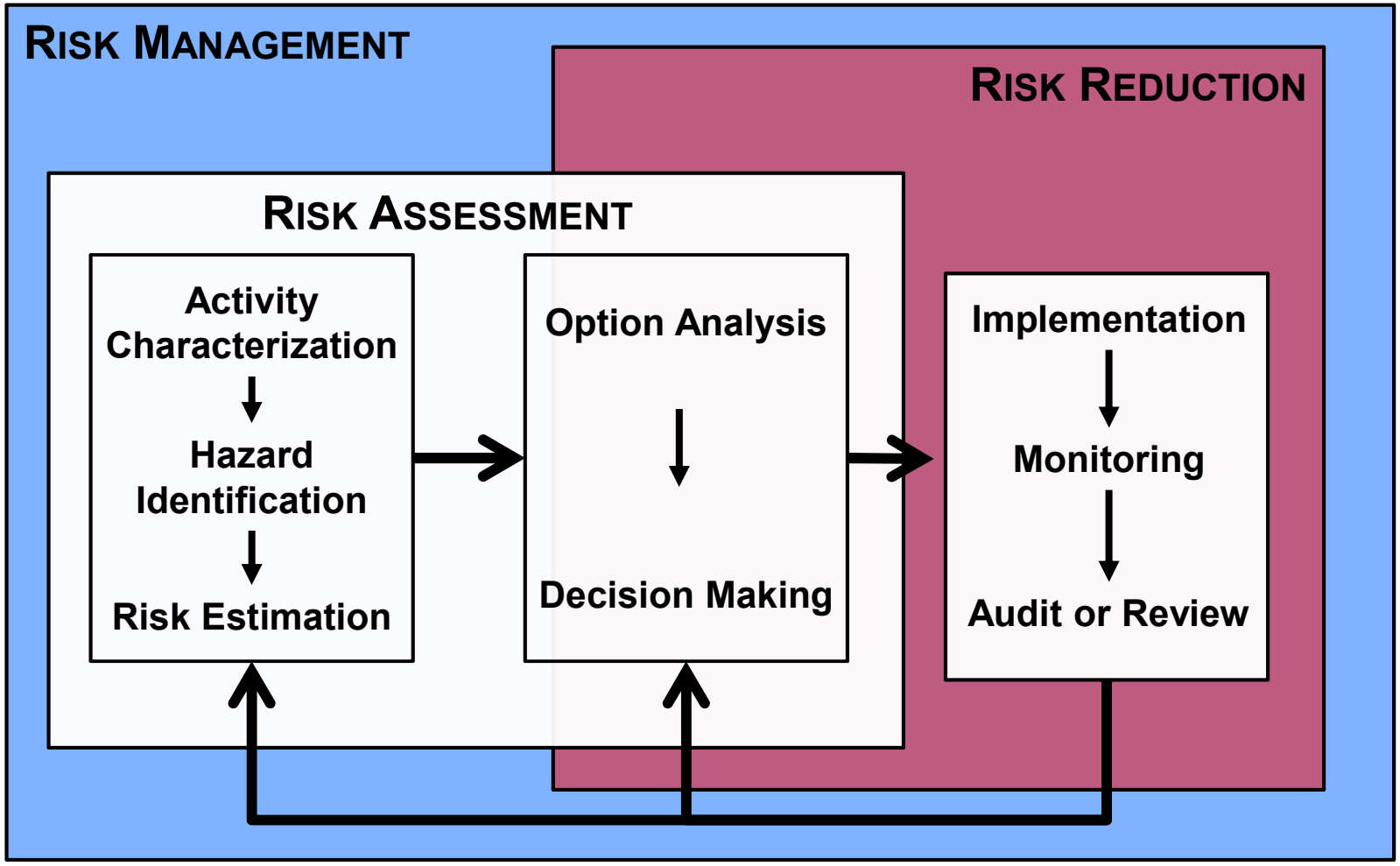
"The employer shall establish and implement written procedures to manage changes (except for "replacements in kind") to process chemicals, technology, equipment, and procedures; and, changes to facilities that affect a covered process. " **OSHA PSM 1910.119**



MOC Lifecycle

7. Managing Risk Across Life Cycle

It is crucial that risk estimation, decision making and audit/review are performed by different individuals



8. Ethics, Culture, Values

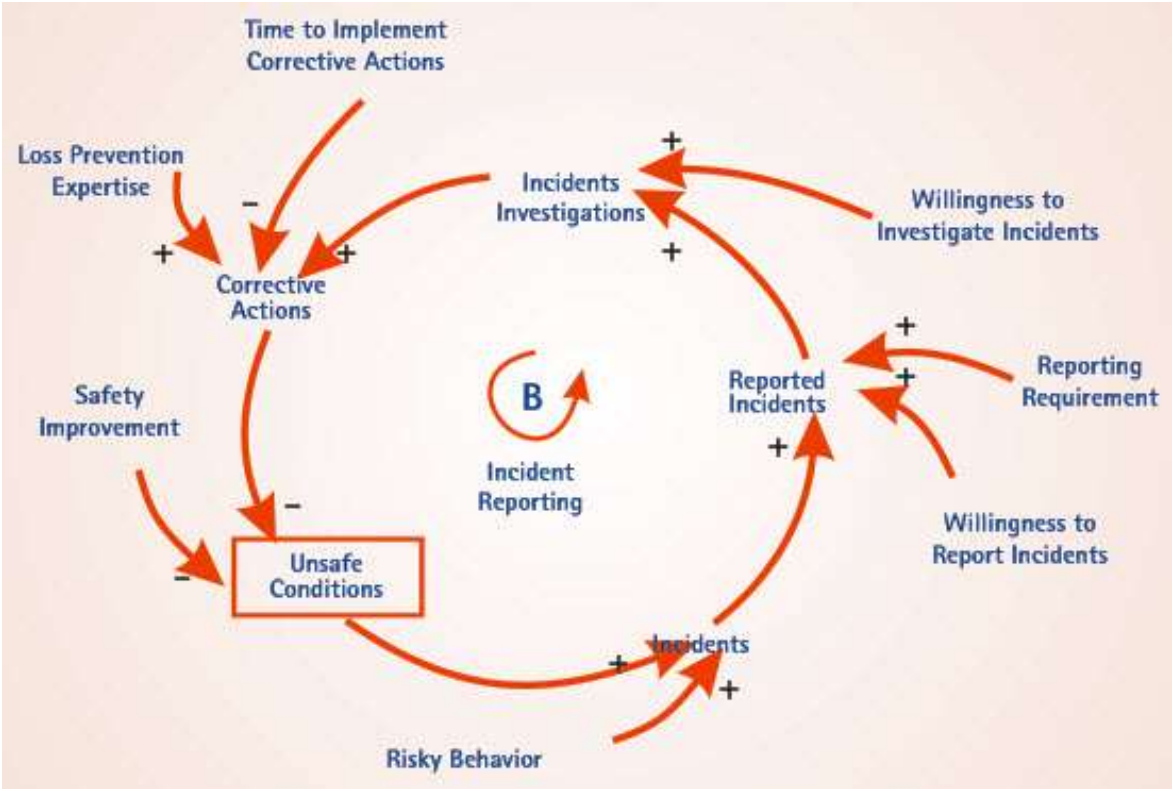
Ethics	Values
Set of moral principles, especially ones relating to or affirming a specified group, field, or form of conduct	Principles or standards of behavior
Professional	Personal
Influenced by different professions, organizations, institute, etc.	Influenced by family background, culture, religion, community, etc.
Can vary according to professions	Can vary according to individuals

- High values lead to objective and fair decision making
- Each organizational culture has its own ethical practices

9. Learning from Events or Incidents

Disastrous industrial accidents with many fatalities and injuries:

- Bhopal 1984
- Piper Alpha, 1988
- Phillips Pasadena, 1989
- Exxon Valdez, 1989
- BP Texas City, 2005
- Deepwater Horizon, 2010
- Tazreen Fire, 2012
- West Explosion, 2013
- Tianjin Explosion, 2015

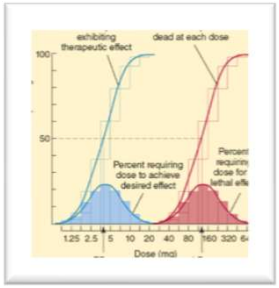


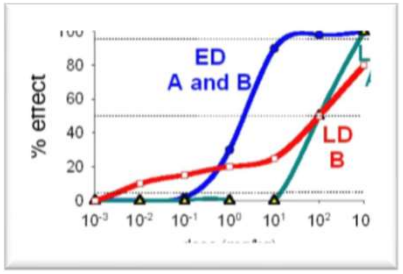
Disaster Management Institute, Bhopal

Data mining will be needed to select and implement the learning

10. Risk Receptors, Impacts, and Multi-dimensional Uncertainty: example *toxicity* probit

Analogue probits of people, structures for:
- *Radiant heat*
- *Blast overpressure*





Uncertainty and **Variability** in Risk Metric (*e.g.*, MOE for peak brain concentration)

Uncertainty and **Variability** in Exposure Parameters

Uncertainty and **Variability** in model Parameters

Uncertainty and **Variability** in Dose-Response model Parameters

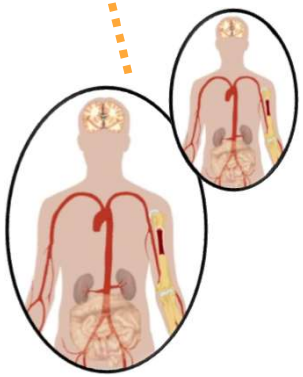
Exposure → Dose → Effects

Rodent (in vivo) ⟷ Humans (in vivo)

Uncertainty

Rodent (in vitro) ⟷ Humans (in vitro)

Extrapolation

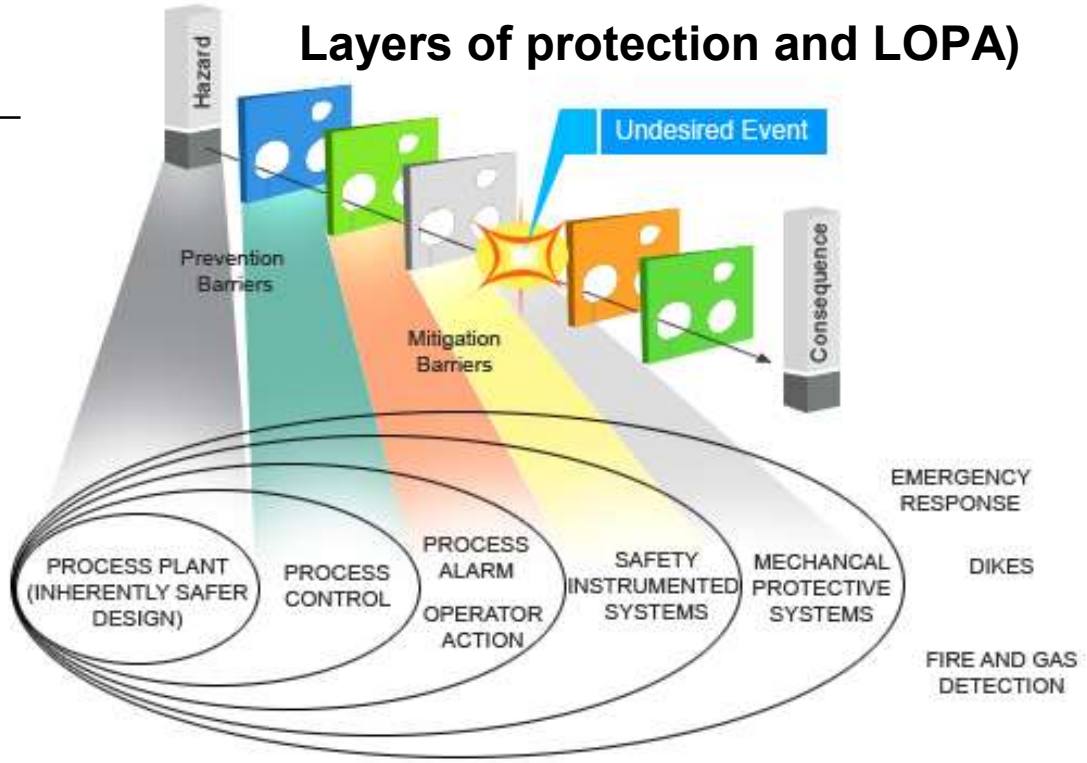


11. Concepts of Function, and Failure (things fail)

Each fault/failure produces a scenario of secondary causes and effects

- Probability of Fault, Failure, Reliability, and Unavailability or other threat
- Hazard & Operability study (HAZOP), Failure Mode and Effect Analysis (FMEA).
- Fault-Tree, Event Tree, combined to Bow-Tie shows cause-effect scenarios.
- Safety function reduces the risk to a tolerable limit.

	Probability of Failure on Demand (PFD)
Pressure relief valve	$10^{-1} – 10^{-5}$
Water sprays, deluges, foam systems	$1 – 10^{-1}$
Basic Process Control Systems	$10^{-1} – 10^{-2}$
Safety Instrumented Function (SIF) requirements	SIL 1: $10^{-1} – 10^{-2}$ SIL 2: $10^{-1} – 10^{-2}$ SIL 3: $10^{-1} – 10^{-2}$



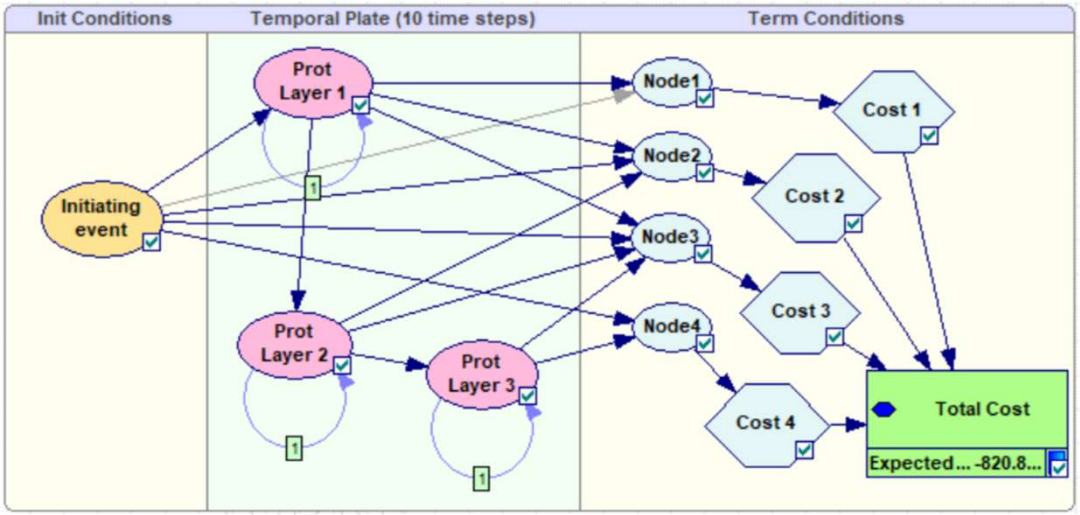
12. Dynamic and Operational Risk Analysis

Risk analysis is to determine risk of each possible fault/failure scenario.

Bayesian network connects causes and effects, calculates joint probability.

Risk can be updated with time (Dynamic & Opn. Risk → Risk Dashboard):

- Failure probability can change with time (e.g., slow barrier deterioration).
- Uncertainty resulting from changes due to inspection, tests, events, maintenance.
- Monitoring processes through technical, safety and management indicators made possible by means of Hidden Markov Model coupled to Bayesian Network.

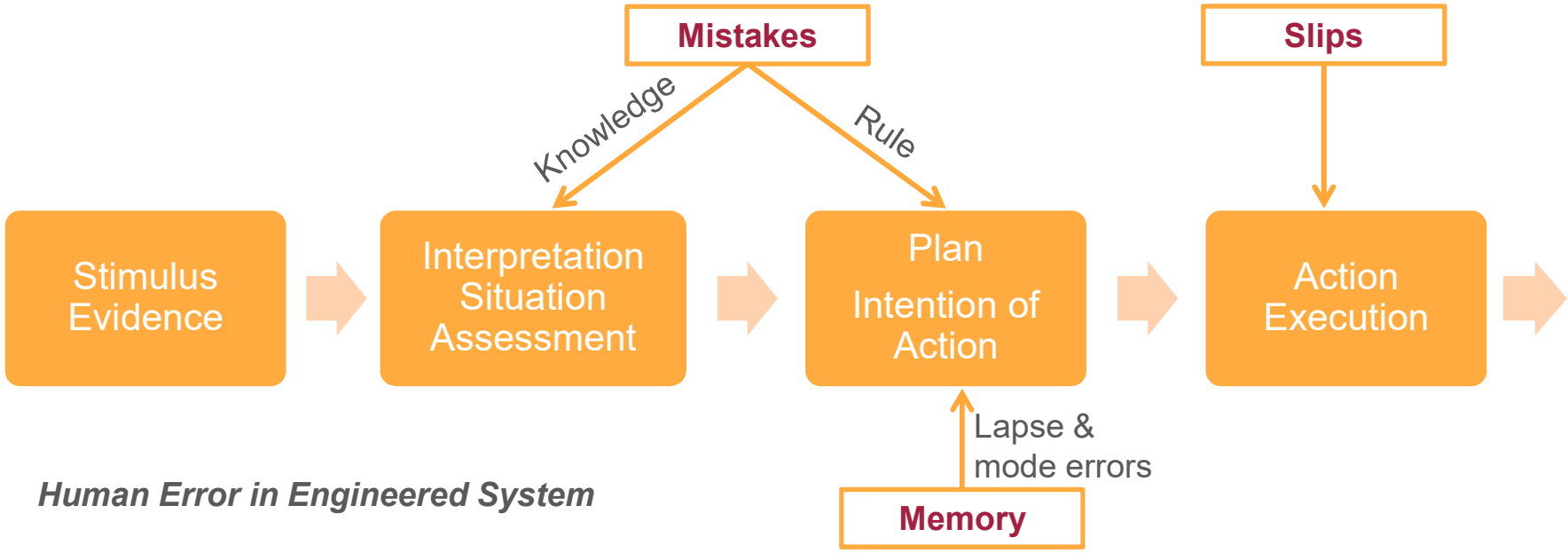


Example of Dynamic Bayesian Network of cost calculation of Layer of Protection system (3 layers). Degradation is according to exponential law. By varying the number of time steps, effect of different time durations can be calculated.

13. Humans in Engineered System

"Either we manage human error, or human error will manage us" **James Reason**

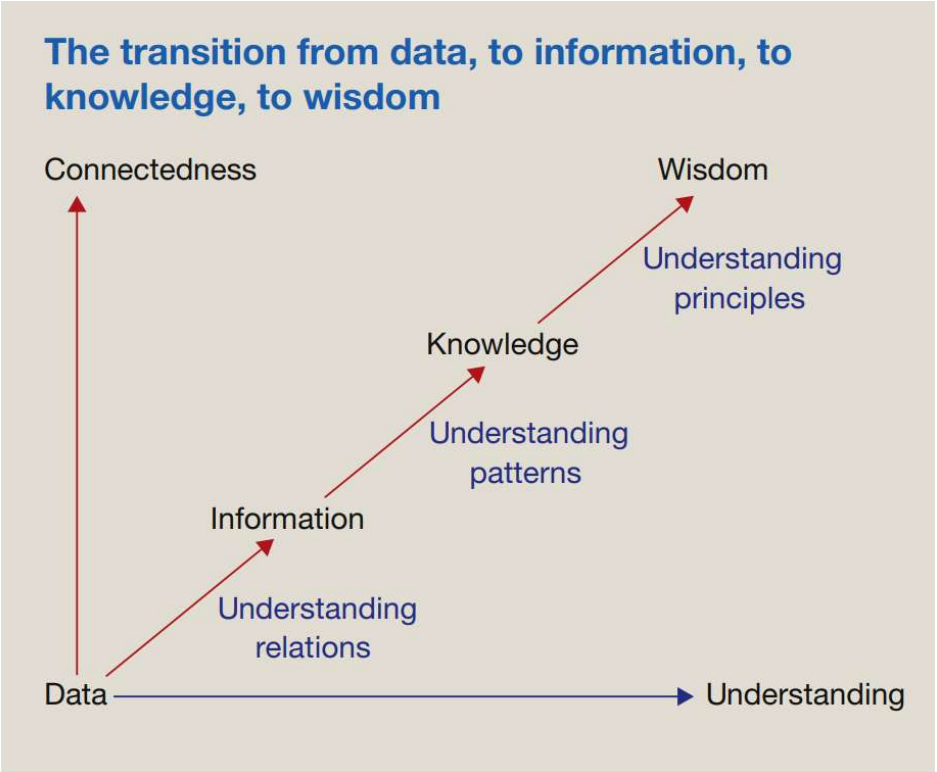
- Design for error: Interlocks, lock-ins, lockouts
- Human centered approaches are effective to train people
- Organizational approaches *e.g.,* planning workflows and shifts are important



Human Error in Engineered System

14. Data, Information, and Knowledge

- Data by itself has no meaning; when placed in context it gives information
- When organized and structured by processing and validation, information becomes knowledge
  - Explicit: readily available
  - Implicit: gained by experience
- Wisdom is an extrapolative process which includes knowledge in an ethical and systematic framework; by this process we discern right and wrong



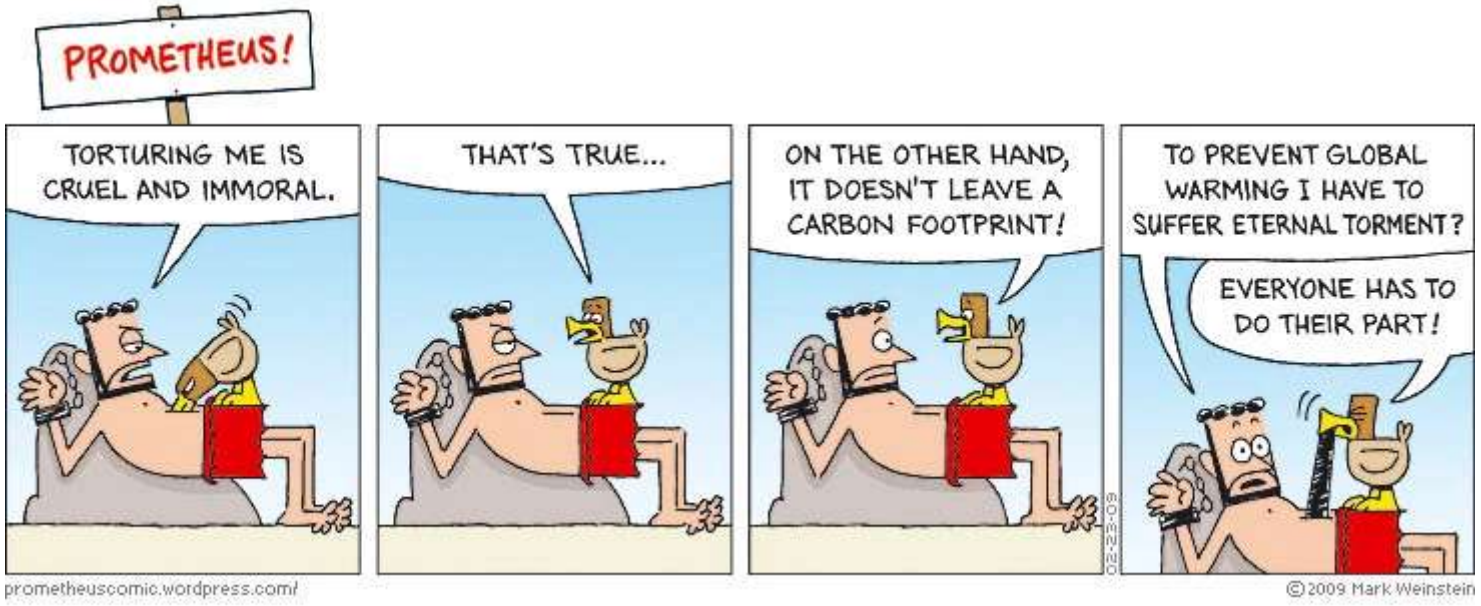
Anaesthesia & Intensive Care Medicine, Vol 18, Issue 1, 2017, pp. 55-56

15. Trade-offs : Technical, Economic

Management decision making:

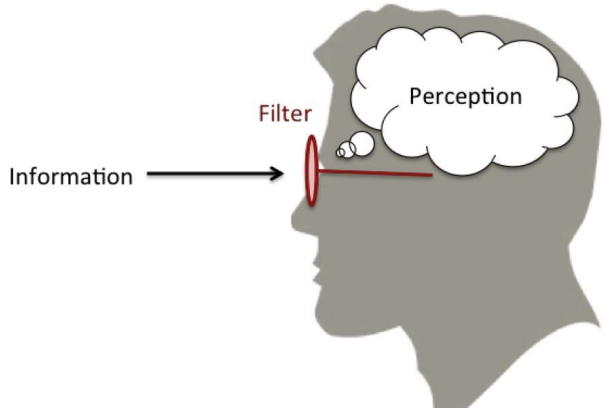
When one thing is given up in order to get another:

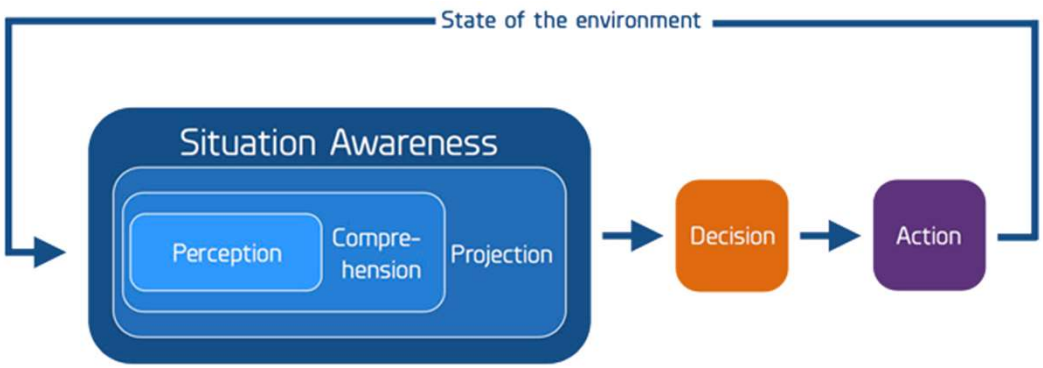
- Every choice involves trade-offs
- Economical trade-offs: scarcity forces to make choices
- Technical trade-offs: economics forces to make choices

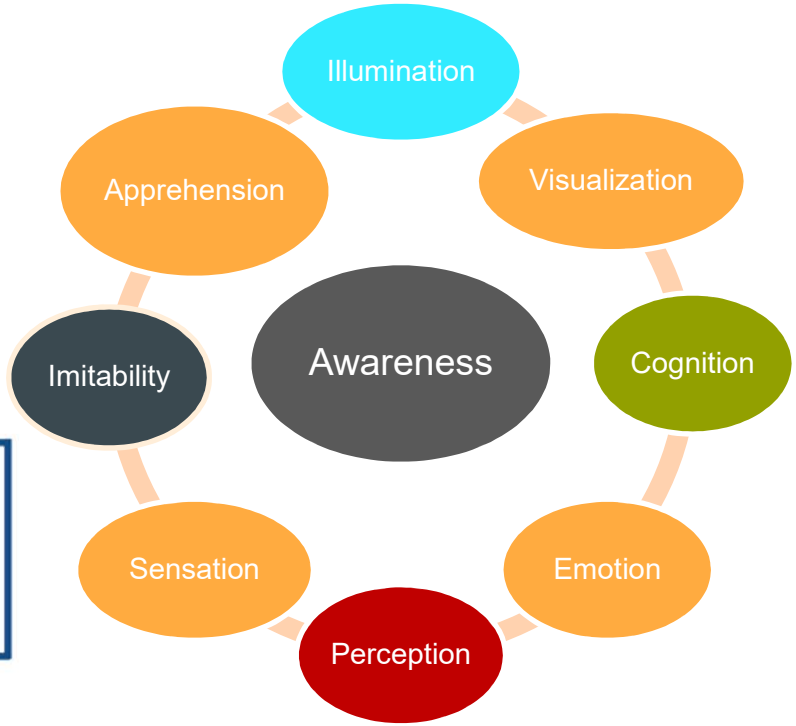


16. Perception and Awareness : Self, Situational

Perception is awareness shaped by belief. Belief "controls" perception. Rewrite beliefs and you will rewrite perception.



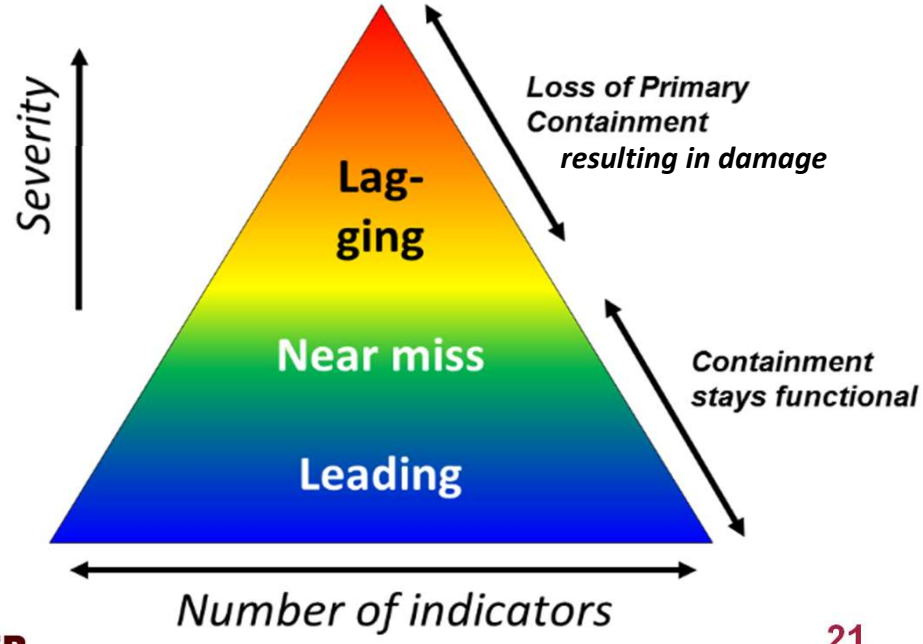




17. Indicators : Leading and Lagging

Adapted from Wang, M., Mentzer, R.A., Gao, X., Richardson, J. and Mannan, M.S. (2013). Normalization of process safety lagging metrics. Process Safety Progress, 32(4), 337-345

Safety performance indicators can be selected based on safety management system items, see slide point # 22. Near misses are challenges to the safety systems; leading ones are defects to the operating discipline.



18. Competence, Limitations, and Roles

Competency Tiers

- Awareness
- Basic application
- Skilled application or proficiency
- Mastery or expert

"It is not, of course, sufficient to have knowledge. It is necessary to be able to apply it to real-life problems" **Trevor Kletz**

Organizational Competency

- Frontline: Operator, Maintenance, Supervisor
- Engineers: Integrity, Reliability, Project, other Technical
- Support: PS advisor, PS leader, HSE site/corporate, QC, Human resource
- Management: Manager, Superintendent
- Executive: Directors, Board Chairs, Safety Committee Chairs, Specialist

19. Emergency Response (ER)

"*Failing to plan is planning to fail*" **Benjamin Franklin**

- PEAR: People, Environment, Asset, and Reputation
- Well written procedures, pre-defined team with clear roles
- Internal and external notifications, by and to whom
- Training/drills, and schedule

Hurricane Harvey, Houston

Arkema Chemical Plant, Crosby, Texas

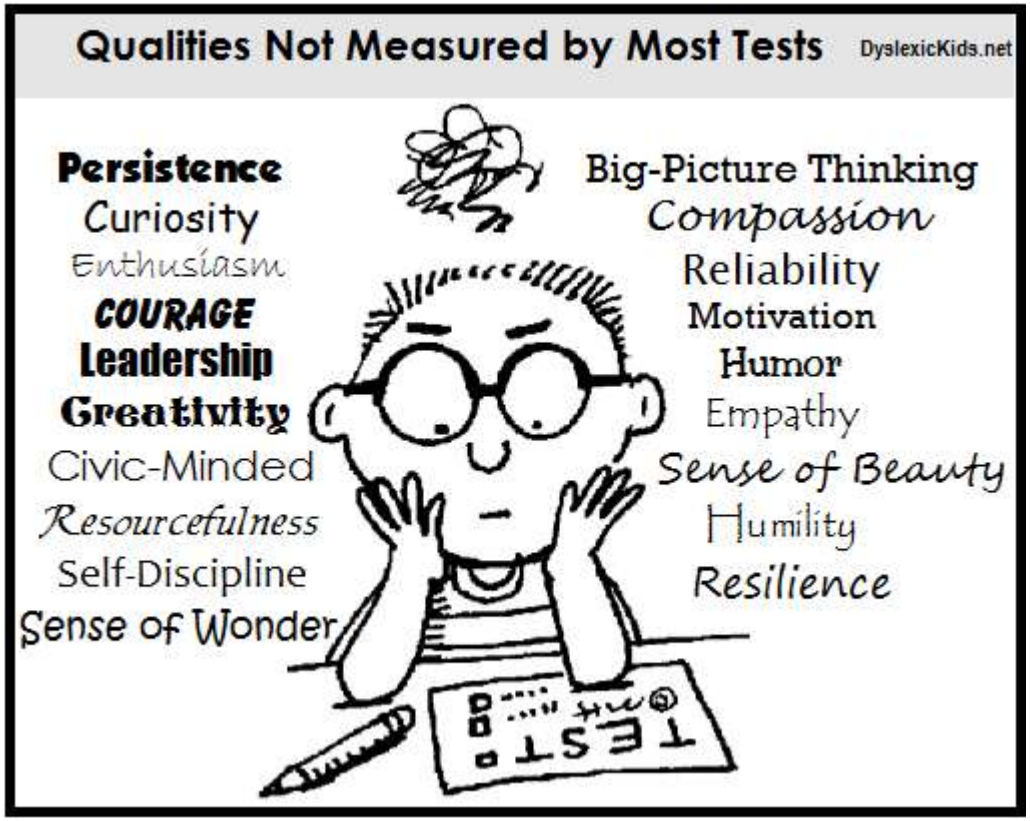
20. Questioning Mentality with Professional Disposition

"*The important thing is not to stop questioning*" **Albert Einstein**

- **Be a Model:** Lead by example, search for new opportunities, ask lots of "why" and "what-if" questions
- **Improve:** Establish mentality that everything should be improved, encourage to ask "How" questions
- **Do Differently:** Encourage to challenge assumptions, run "the best question" contest
- **Reassess:** Assign teams to reassess past decisions periodically, are they still effective in changing environment?
- **Educate:** Train to ask effective searching and open-ended questions, promote coaching by questioning

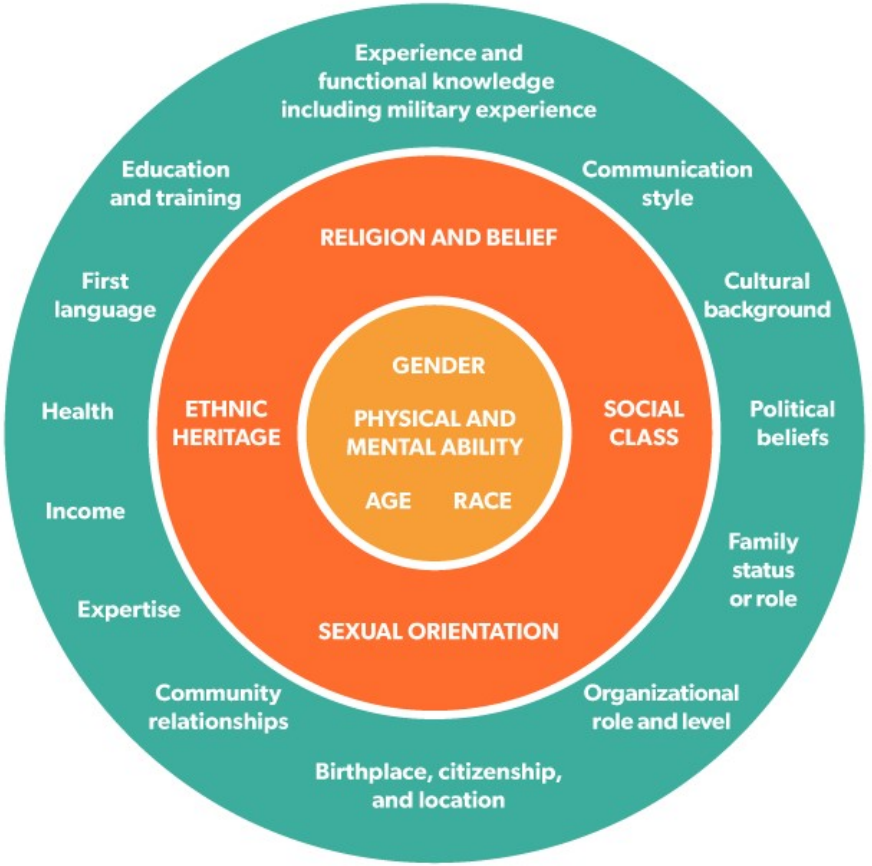
21. Courage and Humility

"*Courage is what it takes to stand up and speak; courage is also what it takes to sit down and listen."* **Winston Churchill**

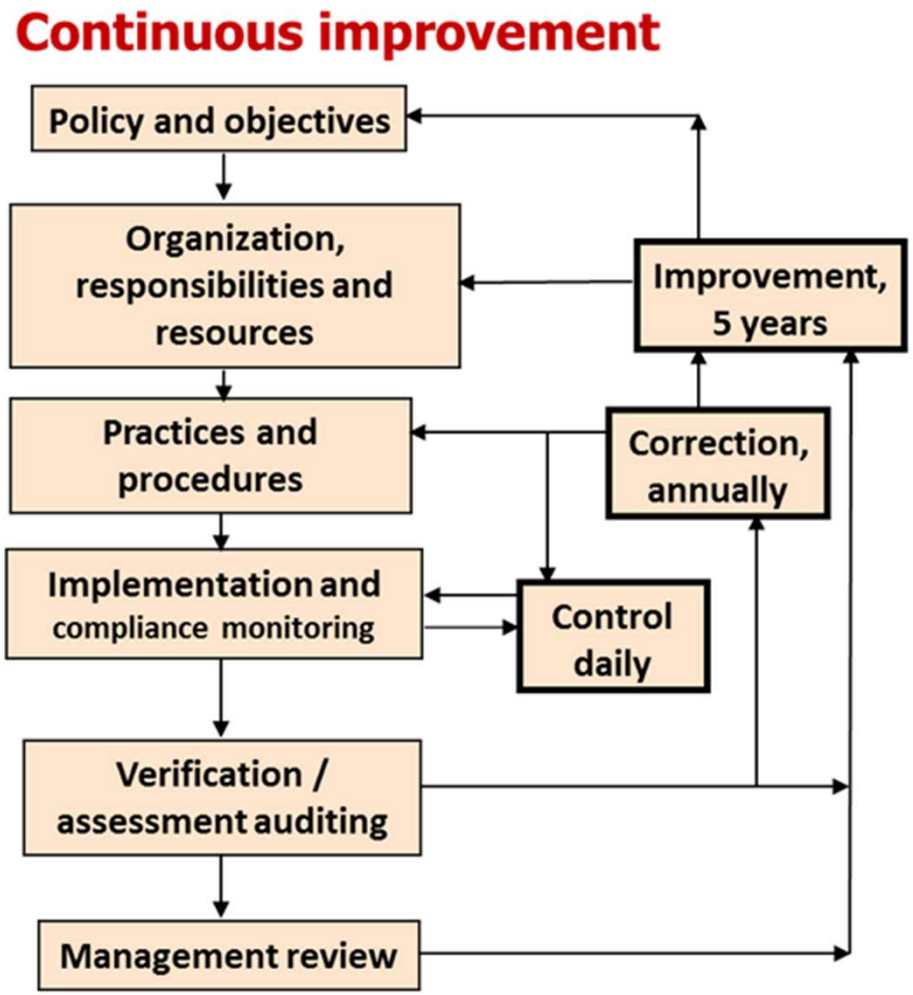


22. Diversity, Discipline, Culture, and Experience

- Diverse background brings unique experience and perceptions in group
- Strengthens teams' productivity and responsiveness to changing conditions
- Exposure to new ideas, culture and perspectives help to be intellectual and gain clearer view of future
- Provides opportunity for personal growth



23. Safety Management System (SMS)

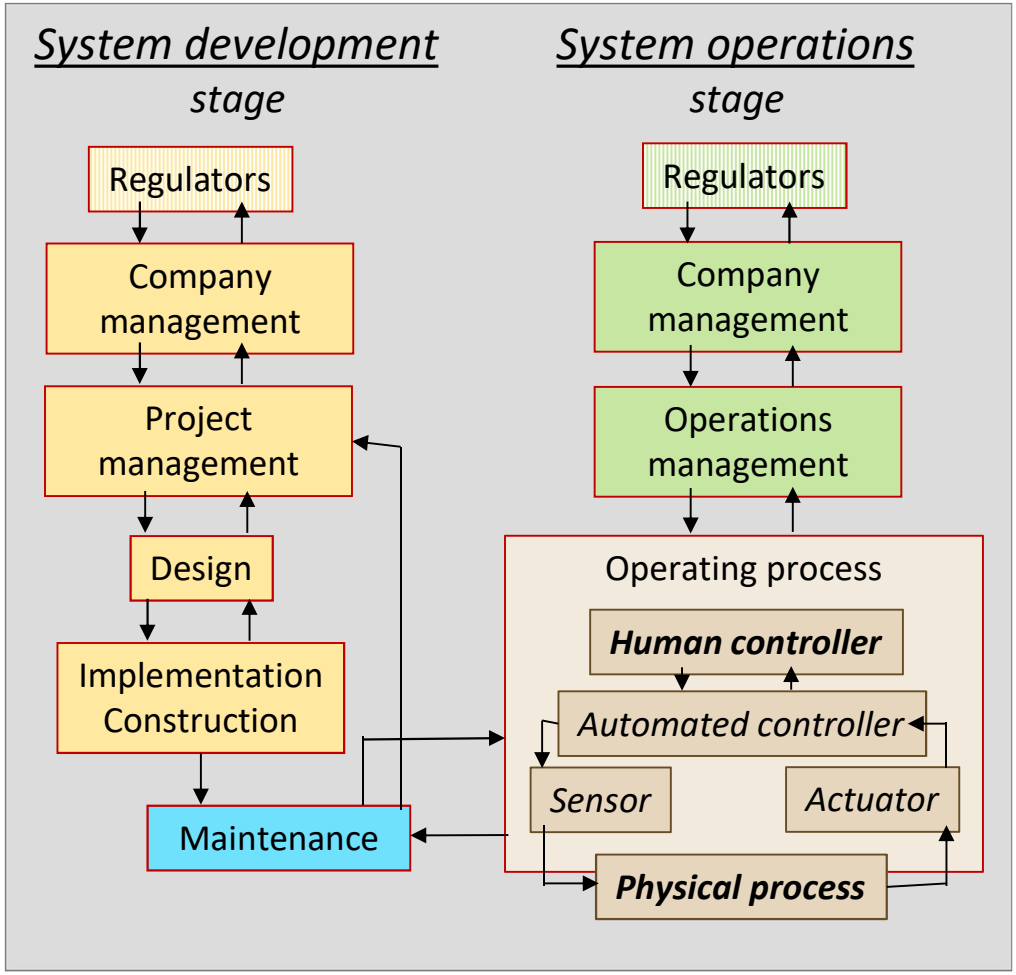


1. ***COMMIT to PROCESS SAFETY***
   - Process Safety Culture
   - Compliance with Standards
   - Process Safety Competency
   - Workforce Involvement
   - Stakeholder Outreach
2. ***UNDERSTAND HAZARDS and RISK***
   - Process Knowledge Management
   - Hazard Identification, Risk Analysis
3. ***MANAGE RISKS***
   - Operating Procedures
   - Safe Work Practices
   - Asset Integrity and Reliability
   - Contractor Management
   - Training and Performance Insurance
   - Management of Change
   - Operational Readiness
   - Conduct of Operations
   - Emergency Management
4. ***LEARN from EXPERIENCE***
   - Incident Investigation
   - Measurement and Metrics
   - Auditing
   - Management Review and Continuous Improvement

CCPS, Guidelines for process safety metrics. Wiley 2010, ISBN 978-0-470-57212-2

24. Socio-Technical System (STS)

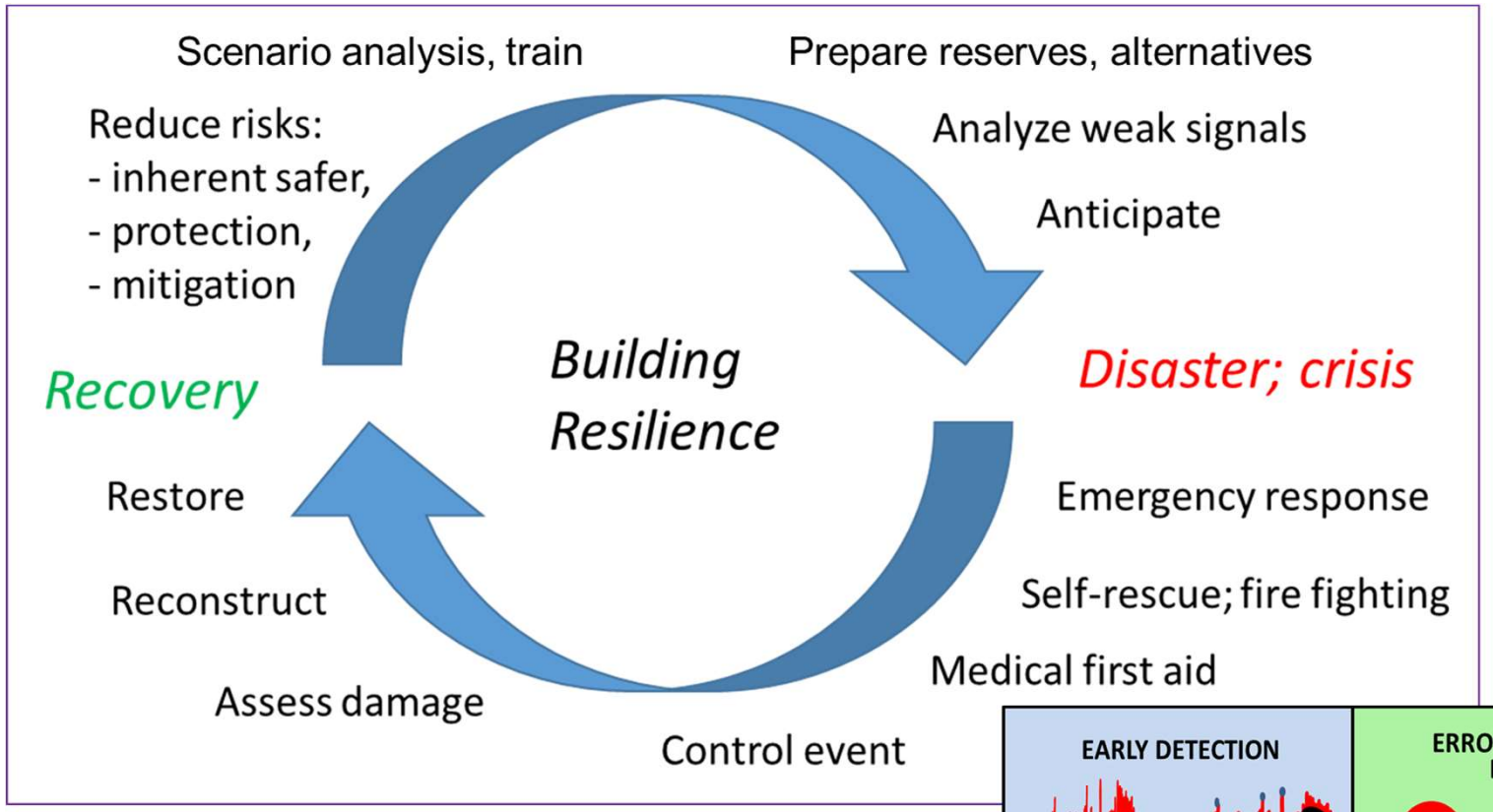
Jens Rasmussen, 1997. Risk Management in a Dynamic Society: A modelling Problem, Saf. Sci., 27, 183-213
Nancy G. Leveson, 2011. Engineering a safer world, systems thinking applied to safety, The MIT Press

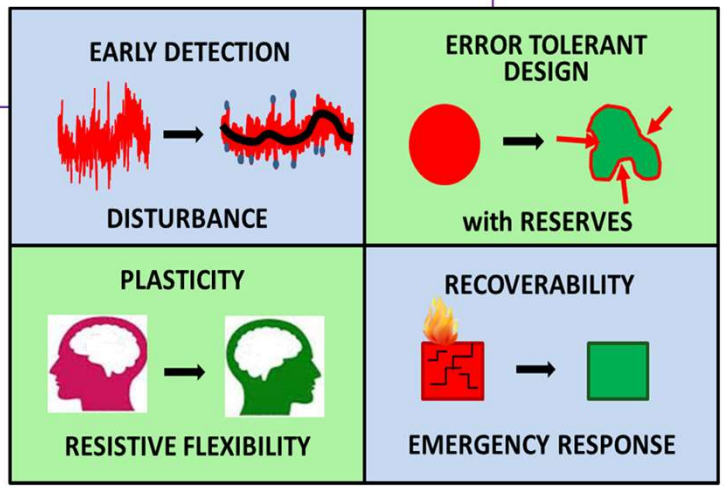


- System is more than the sum of parts -> dysfunctionality and non-linearity. Safety is emergent.
- Complex system: hierarchy of organizational levels, connected by information links; human & organizational factors.
- Actually, complexity is not a system property; it is a limitation of the human mind.
- System-theoretic accident model and processes: STAMP.
- System-theoretical process analysis: STPA for identification.

25. Resilience Engineering

Defense measures against unexpected/unknown threats





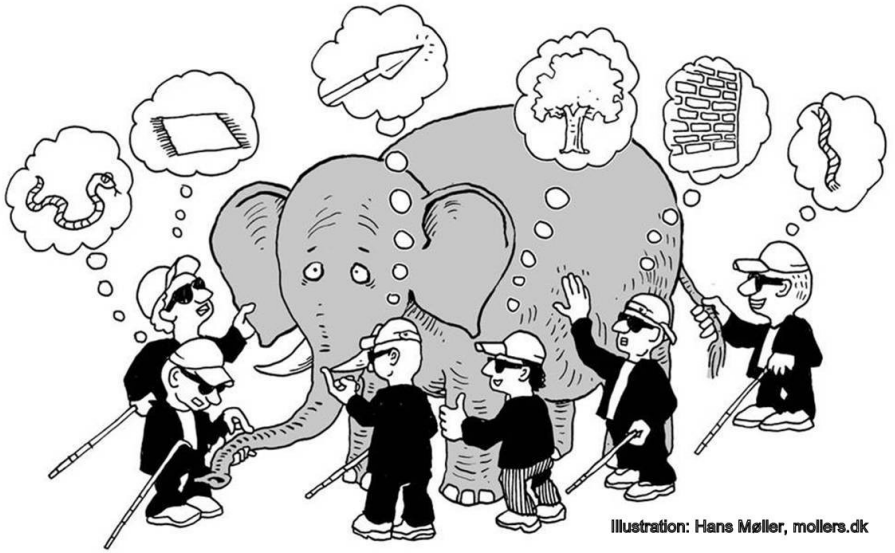
Resilience requires: Leadership, Pro-active posture, Situation Awareness, Creativity, Resources, Networks, Stress testing

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

26. Multidisciplinary Activity

Chemical engineers take the chemicals prepared by chemists and design processes that produce them

- On a larger scale
- Safely
- Environmentally friendly
- Economically



Multidisciplinary Engineering includes -

- Environmental Engineering
- Material Science
- Biotechnology

Acknowledgement

● This slide presentation for educational purpose has been developed by late Dr. Sam Mannan in 2017, but adaptations and some additions are made by Dr. Monir Ahammad and by Dr. Hans Pasman in 2018.

THANK YOU

Questions ?

HP13

Slide 32

HP13 Hans Pasman, 05-Dec-18