Risk Management & Human Error

"For a successful technology, reality must take precedence over public relations, for nature cannot be fooled."

— Richard P. Feynman **Report of the Presidential Commission on the Space Shuttle Challenger Accident**

EPL Institute

Agenda

- Part 1 – Introduction to Risk Management
- Part 2 – Components and processes of Risk Management
- Part 3 – Traps and common mistakes in Risk Management
- Part 4 – Human Error
- Part 5 – Risk Management tools

Part1 , Introduction to Risk Management

Agenda-Part1

- Important Definitions
- Risk Concepts
- 4 ways to deal with Risk
- Ethics
- Risk Management
  - Why perform Risk Management
  - Common myths about Risk Management
  - History of Risk Management
  - Who does Risk Management

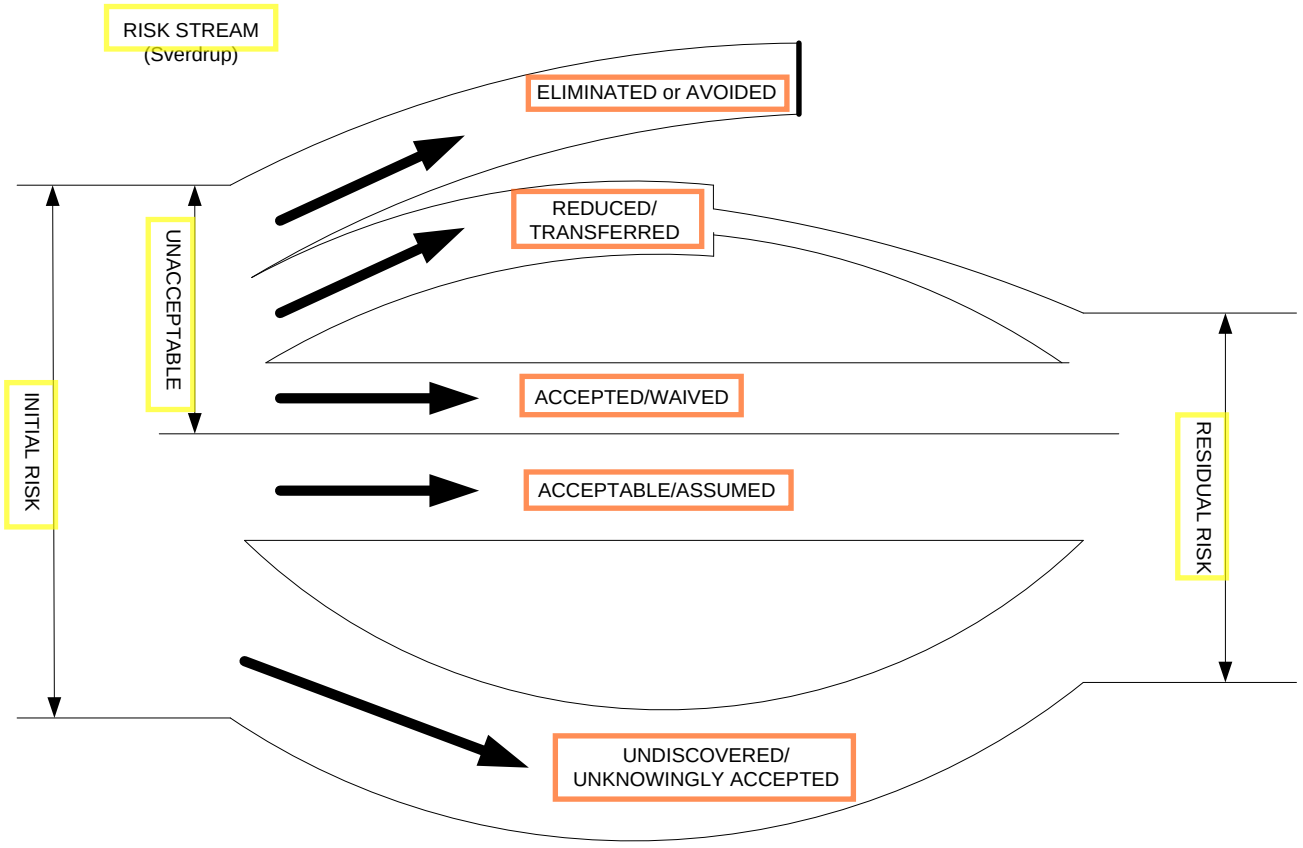
Important Definitions

- Hazard, act/condition posing threat of harm.
- Risk is an event that causes harm to people,resources or environment.
  - P = Probability for an unwanted/damaging situation to happen.
  - S = Severity if the situation happens. Loss of people/resources/goodwill.
  - RISK = P * S

Risk Concepts

- The other side of the opportunity-coin is Risk.
- Companies and organisations have different definitions for what risk is.
- Risks in themselves are not bad.
- Risks are highly subjective and can be culturally different.

Risk Concepts part2



epl Institute

There are only four ways of dealing with risk

1. Reduce – Reduce risk severity and or probablity
2. Avoid – Avoid risk by not doing task or by changing ways to work.
3. Accept – We do this by default with all risks we do not know about.
4. Transfer – Insure, outsource work but let the other party know about the risk

Ethics

- In risk management a price is often set on human suffering and life. This is often perceived as morally wrong.
- This is done in order to be able to prioritize which risks to mitigate. Otherwise there is no difference between a risk that maims 1 person vs a risk that kills 20 persons.
- The vatican ethics commitee has deemed that there is no conflict in assigning a value to human life in order to know which risks to mitigate. I.e Human life is valuable and risk management is but a tool to ensure that human life is preserved from harm.

Risk Management

- Risk Management is to:
  - plan for failures.
  - lessen the possibility of a risk to happen.
  - lessen the consequence of risk when it happens.
- RM will not remove risk, there will always be risk associated with human endeavours.
- RM gives only stochastic control over risks.

Why perform RM

- You need to perform RM in order to understand which risks you are facing.
- Certain risks can put your company out of business others will just cost you loads of money.
- Reacting and firefighting will sap your energy which should be used to further your business.

Common myths about RM

1. **It is too difficult and complex and only used by nuclear industry and the military -** True is that some industries need a stringent control over their risks but most companies will do well with simple tools.
2. **Costs too Much** – Often severe risks and production disturbances can be avoided with almost no cost in time or money. Costs too much stems from overconfidence. ie. ”*It wont happen to me*”.
3. **Not necessary, we have a management control system for our operations -** What is missed is that the management control should not only focus on the normal running of the operations but in addition to that handle out of the ordrinary situations. Example: You control emissions of your day-to-day operations but if an unforseable event happens you can make as much impact on your environment in 1 day as 10years of normal operations.

Too complex,costs too much or not needed?

Accidental release of Hydrogen Fluoride in Torshälla 1996-02-19.

Umeå, FOA 1996, 12 p.
(FOA-R--96-00267-864,4.5--SE) (Användarrapport/User report) (470)
Keywords: Utsläpp fluorväte industri riskavstånd hydrogen fluoride industrial accident release risk distance
Språk/language: Svenska/Swedish

Abstract: The report deals with an accidental release of hydrofluoric acid from a stainless steel plant.
The duration of the release was three and a half hours and the total amount of released acid was approximately 25 tons.
Calculations of the dispersion of hydrogen fluoride were made from observations during the accident.
According to the calculations 2.200 kilograms of HF evaporated into the atmosphere.
Within some areas of the plant, there were risks of lethal injuries to man.
The risk distance for severe injuries was calculated to approximately 500 meters.
Calculations for a corresponding accident during summer conditions show similar consequences.
Calculations made for the most unfavourable weather conditions shows approximately three times greater risk distance.

EPL Institute

The many uses of RM

- Guide resouce allocation for control of LO$$.
- To make ”GO / NO GO” decisions.
- RM can be done in a factory in order to minimize workrelated injuries. Then it might be called Safety Management.
- The business manager can perform RM for the business strategy currently being implemented. Then it is oriented to remove business risks.
- A project manager is doing RM for the project which is constrained to project risks only.
- The plant manager commences a RM effort for the environmental effects of the steel plant. As required by the governmental environment agencys.

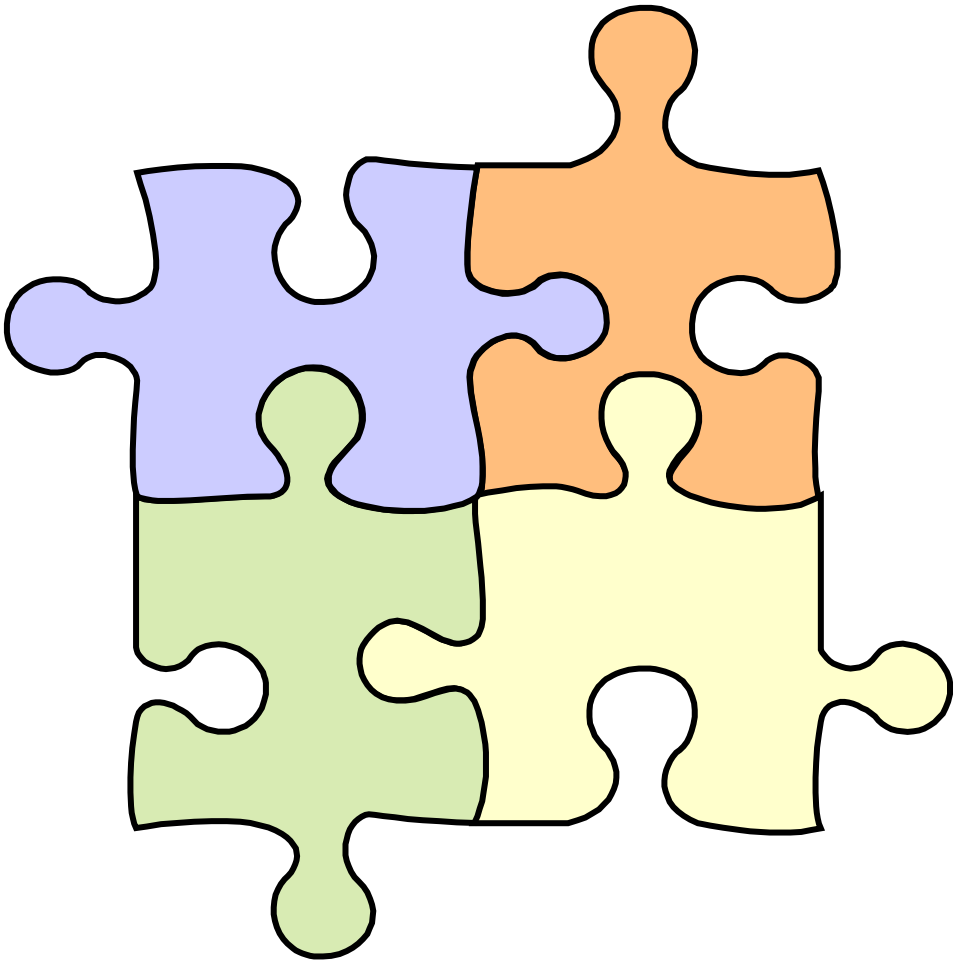
History of Risk Management

- Formal riskmanagement started in the insurance companies.
- Probabilities of different occurances where stored and used for calculations of premium payments.
- Insurance companies mitigated their own risks by insuring part of their portfolio in other insurance companies.

Who does RM

- Oli Industry
- Nuclear Power Industry
- Military
- Hospitals and medicin industry
- Computer and High Tech Industry
- Insurance Industries
- Construction Companies
- Transportation industry’
- NASA & ESA

Part 2 , components and processes



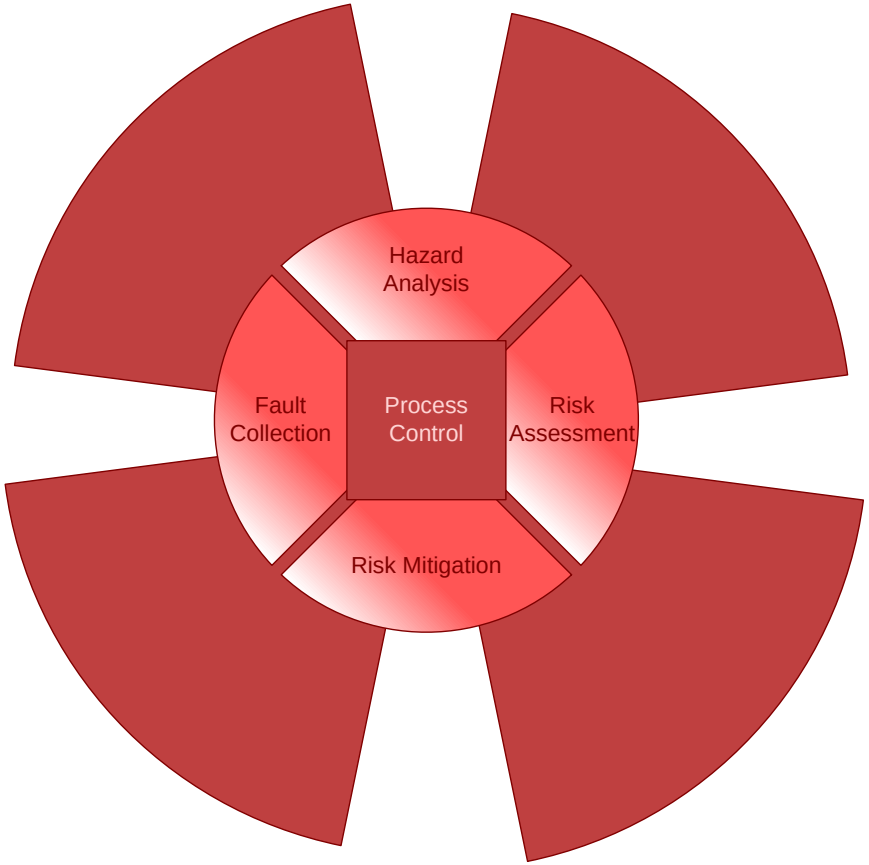
Agenda-Part2

- Components of Risk Management
- Hazard Analysis
  - Domains & steps in Hazard Analysis
  - Finding & describing hazards
- Assessing Risk
  - Risk Assessment Matrix
- Risk Mitigation
  - Effectivness of countermeasures
- Process control & Fault collection
  - Revising Hazard analysis & Risk Assessment
- Disaster Planning

Components of Risk Management

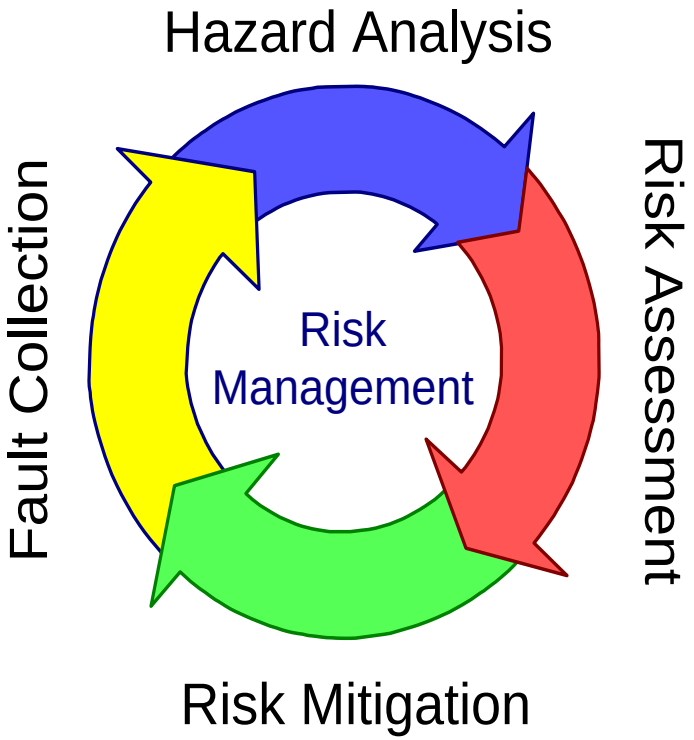
Risk Management consists of several components:

- Process Control
- Hazard Analysis
- Risk Assessment
- Risk Mitigation
- Fault Collection



Process Control

- The RM process is about controlling activities associated with RM.
- Answering questions like:
  - Who
  - When
  - How
  - Which goals
  - Assigning responsiblities and authority
  - Are performing to expectiation?



Hazard Analysis

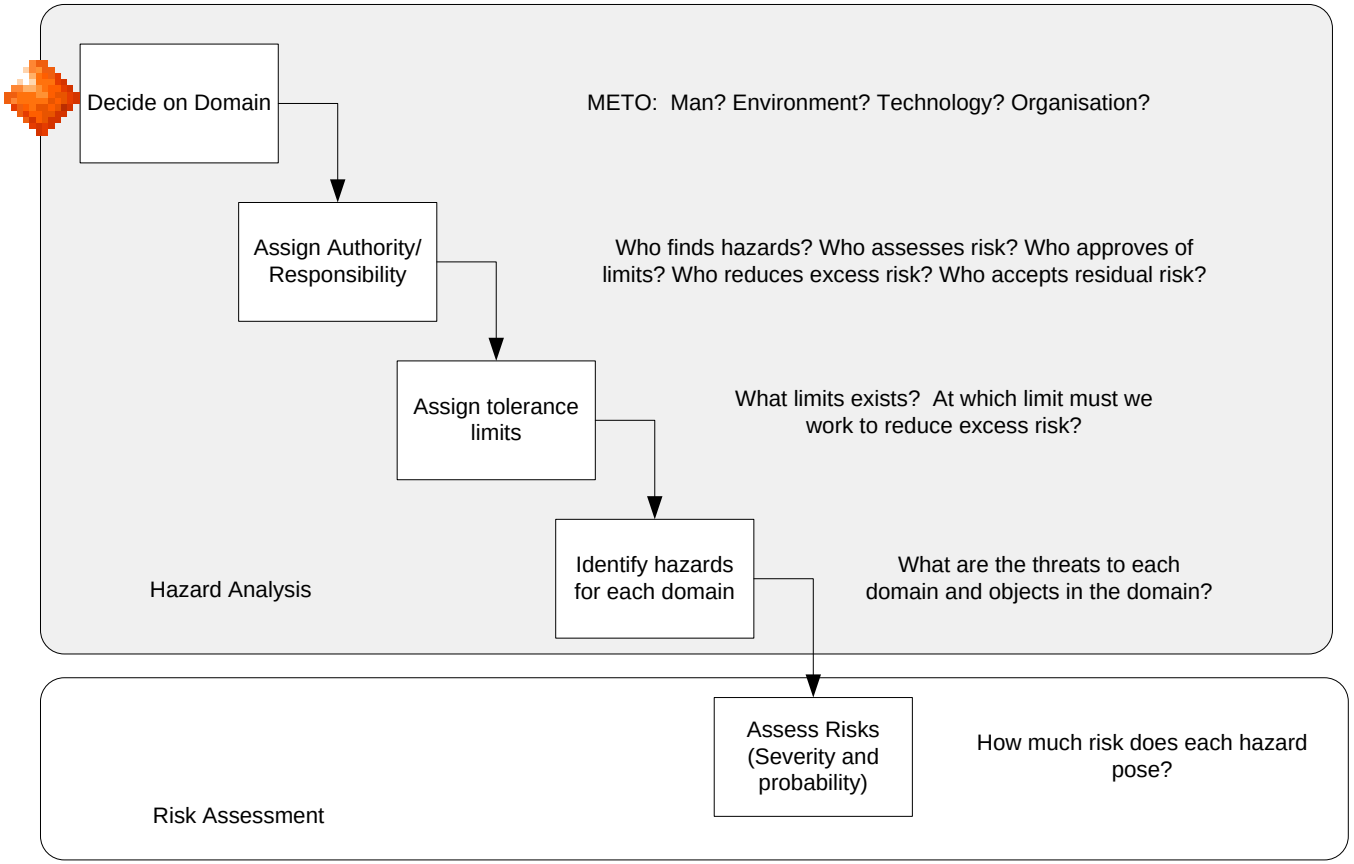
Goal of Hazard Analysis is to:

- Identify hazards that lead to risk
- Assess hazards that lead to risk
  - quantify uncertainty
  - quantify consequences

Domains of Hazard Analysis

- Hazard Analysis must address risks to following domains M.E.T.O.:
  - **M**an: workers & their family, people living nearby etc.
  - **E**nvironment: in and outside of the company.
  - **T**echnology: Machines, tools etc.
  - **O**rganisation: The company, parts thereof or whole, reputation.

Steps in Hazard Analysis



Finding Hazards – performing a Preliminary Hazard Analysis

So how do we find Hazards? Here is a few ways to do that:

- Use intuitive ”Engineering Sense”.
- Perform Walkthoughs.
- Perform simulations.
- Consider regulations/standards.
- Review prior system safety studies for similiar systems.
- Review historical data.
- Consider external influences.
- Scenario development.
- Energy flow/Barrier Analysis.
- Consider ”common causes”.
- Consider ”operational phasing”.

Performing a PHA is more of an ART than SCIENCE. But remember that the foundation of success is cemented at this level!

Describing Hazards – think *Source / Mechanism / Outcome*

- A common fault is that hazard descriptions do not descibe hazards instead they describe the outcome. This can lead to masking of further sources.
- A hazard description consists of three elements that express a threat:
  1. A source – an activity and/or condition that serves as the root.
  2. A mechanism – a means by which the root can bring about harm.
  3. An outcome – the harm to be suffered

Expected Status Quo (2)

- THE PROBLEM — For the usual system, hazards and their risks vary from operational phase to operational phase. (An operational phase is a functionally discrete portion of system life cycle.) Most system failures occur not during the phase when the system is "up" and running normally, doing its intended thing. Failures more often occur during a start-up or a shut down or a load change or a maintenance "transient." BUT …most System Safety analyses treat only the full-up system, running steady-state, as intended, at nameplate rating. SEE THE FLAW?
- THE CURE — To be thorough, System Safety analyses must consider the hazards and risks peculiar to each of the operating phases that can be occupied by the system. Some hazards may be unique to certain phases. And for some hazards that are present during several phases, the risk may vary from phase to phase, requiring a separate consideration for each of the phases. (See next slide.)

Hazard description example 1

”Rain slick pavement caused car to skid and lead to head on collision with opposite traffic.”

- Source: Rain slick pavement
- Mechanism: skid
- Outcome: head on collision

Hazard Description assignment1.

”Open canister of petrol stored in the furnance room of the daycare center.”

- Perform Hazard Description of the open canister sentence. Using Source / Mechanism / Outcome.

Hazard Description assignment2.

”Open canister of petrol standing in the desert hundred of miles from any people.”

- Perform Hazard Description of the open canister sentence. Using Source / Mechanism / Outcome.

Hazard Description Assigment 3

Decide if sentences describe Source/ Mechanism/Outcome:

- I cut myself while working
- Using a knife on unprotected skin
- I slipped in the stairs and hurt my knee
- Fall injury
- Electrocution
- Stress injury
- Hearing damage

Risk Assessment with Risk Matrix

- Forces organisation to think/define/accept definitions for probability and severity.
- Easy to communicate risks in this manner.

Severity of Consequences	Probability of Risk					
	F Impossible	E Improbable	D Remote	C Occasional	B Probable	A Frequent
I Catastrophic						
II Critical						
III Marginal						
IV Negligible						

Adapted from MIL-STD-822D

Risk Code/ Actions		Imperative to suppress risk to lower level.		Operation requires written time limited waiver from management		Operation permissable

Severity/Probability interpretations

Probability of Risk		
Level	**Descriptive Word**	**Definition**
A	**Frequent**	Likely to occur repeatedly in system life cycle.
B	**Probable**	Likely to occur several times in system life cycle.
C	**Occasional**	Likely to occur sometime in system life cycle.
D	**Remote**	Not Likely to occur in system life cycle, but possible.
E	**Improbable**	So unlikely that occurrence can be assumed not to be experienced.
F	**Impossible**	Physically impossible to occur

Severity of Consequences					
Category	**Personal Injury**	**Equipment Loss ($)**	**Downtime**	**Product loss**	**Environmental Effect**
I Catastrophic	Death	› 1M	4 months	› 1M	Long term (5 yrs or greater) environmental damage or requiring › $1M to correct or in penalties
II Critical	Severe Injury or severe occupational illness	250K – 1M	2 weeks to 4 months	250K – 1M	Medium term(1-5yrs) environmental damage or requiring $250K-1M to correct or in penalties.
III Marginal	Minor Injury or minor occupational illness	1K-250K	1day to 2 weeks	1K-250K	Short term(‹ 1yrs) environmental damage or requiring $1K-250K to correct or in penalties.
IV Negligible	No injury or illness	1K	‹ 1 day	1K	Minor environmental damage, readily repaired or requiring ‹$1K to correct or in penalties

Risk Assessment pointers

- Probability must always be attached to an interval. Often a system lifetime of 25 years is selected for systems.
- For project-risks the project lifetime should be used or exposure in manhours.

Risk Assessment is highly subjective

- People perceive risk in different ways, some focus on:
  - Probability
  - Severity
  - Severity and Probability
- Research has shown that people that focus on probability usually grade risks lower than people that focus on severity or count both probability and severity as equal factors.
- Furthermore is risk perception determined by the following factors:
  1. Source mechanism, a risk source that is new or not well understood is perceived as riskier than something what we understand well and have lived with for some time. Ex, skin cancer from sunbathing is perceived as lower risk than cancer risk from eating food with akrylamid. (sweden 2002)
  2. Severity/Consequence, A risk with serious consequence is often perceived as riskier due to the scare effect of the consequence.
  3. Degree of control, If the consequence can be controlled after the risk has happened we perceive the risk to be lesser than if we cannot control or mitigate the effects of the risk.

Calibration of the Risk Matrix

- Often very exciting discussions arise when assigning Hazard Scenarios to the Risk Matrix. Novices and professionals alike often come with different views.
- Calibration of the matrix will help when assigning hazards to different risk classes in the Risk Matrix.
- A good calibrator to choose is one with the highest severity that we accept today=cell I/E. (I-Catastrophic and E-Improbable).

Severity of Consequences	Probability of Risk					
	F Impossible	E Improbable	D Remote	C Occasional	B Probable	A Frequent
I Catastrophic		I/E				
II Critical						
III Marginal						
IV Negligible						

Adapted from MIL-STD-822D

Risk Code/ Actions					
	Imperative to suppress risk to lower level.		Operation requires written time limited waiver from management		Operation permissable

Calibration Scenario: **Risk of commuting to/from work 20km/day on highly trafficked roads with speeds over 90km/h with rain and ice during wintertime.**

This is clearly I-Catastrophic since people die in traffic. Probability is clearly not F-Impossible but it is not D-Remote where specific permit must be gained before you are allowed to take your trip. But if the Risk where to happen more often than today countermeasures would be implemented to minimize the risk.

EPL Institute

Some probability data ...

Possibility for annual death in USA for:

- Heart Disease 1:397
- Cancer 1:511
- Stroke 1:1 699
- Accident 1:3 014
- Motor vehicle accident 1:6 745
- Altzheimer 1:5 752
- Suicide 1:12 091
- Homicide 1:15 440
- Food Poisoning 1:56 424
- Drowning 1:64 031
- Fire 1:82 997
- Bicycle Accident 1:376 165
- Lightning 1:4 478 159
- Bioterrorism 1:56 424 800

Risk Mitigation

- Decide on countermeasures to mitigate risk.
- Priorities of Risk Mitigation
  1. Minimize serverity of Risk
  2. Minimize probablity of Risk

Effectivness of Countermeasures

- Design – Adopt a design that excludes the hazard. *If hazard is Flooding build above groundlevel.*
- Engineered Safety Features – Use redundant backups, automatic preventers/correctors (active devices). *Install a sump with pumps operated by a flotation device.*
- Safety Devices – Guards, shields, surpressors (passive devices). *Waterproof the basement with leadoff valves.*
- Warning Systems –Use audible/visual signals to trigger avoidance reactions or corrective responses. *Use horns/bells/whistles operated by a moisture detector.*
- Procedures and Training – Develop/implement work methods which control risk. *Formulate inspection procedures and bailing plan. Train personnel in their use.*

Revising Hazard Analysis/Risk Assessment

- There has been a ”Near Miss” or a ”direct hit”.
- The ”system” has been changed.
- System maintenance has been altered.
- System Duty is different.
- Operating Environment is different.

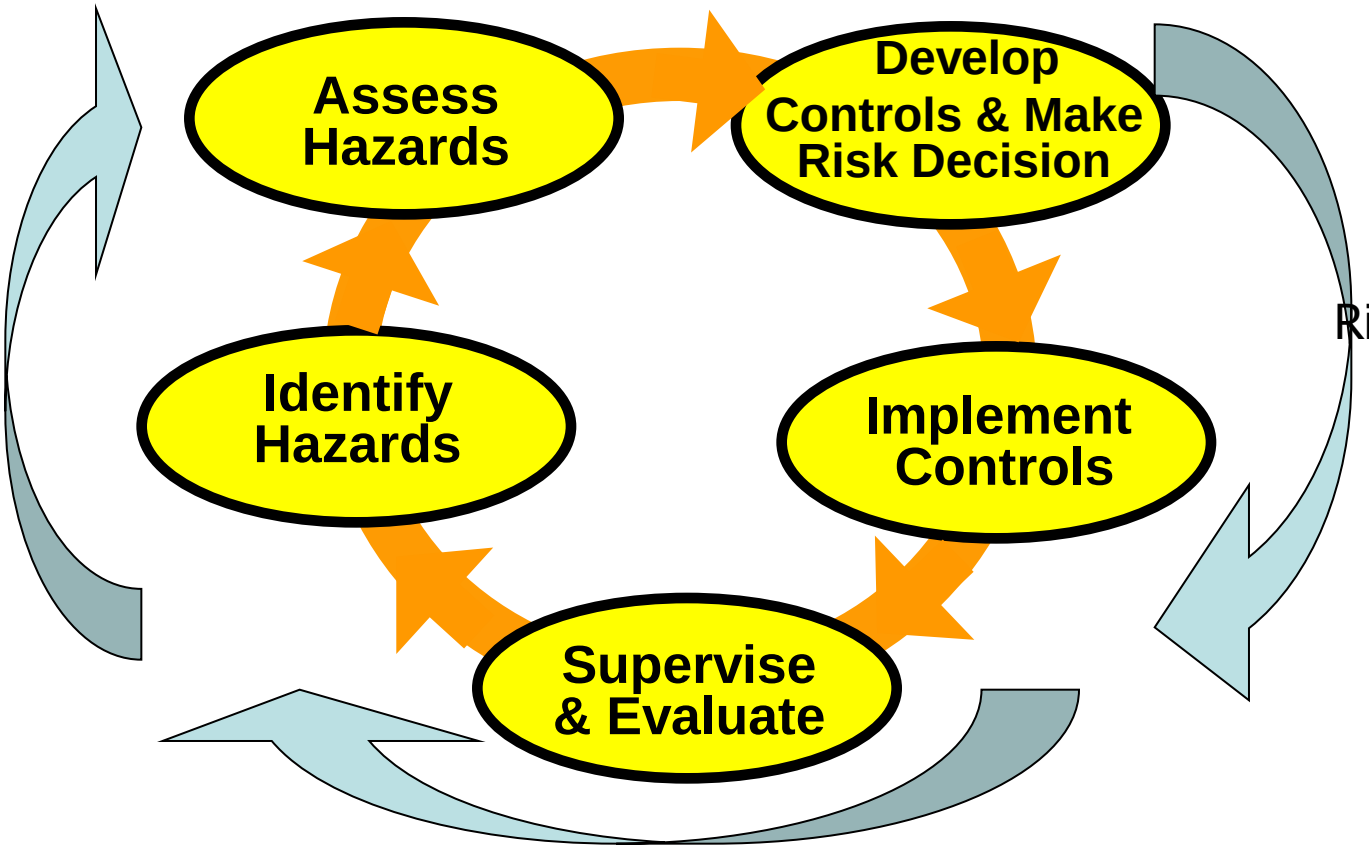
Collecting Faults

- This is the feedback mechanism needed for any knowledge to transform itself to organisational wisdom.
  - i.e. Collecting and analysing risks that happened is beneficial for future Risk Management.
- Analysis of the occurred risks can be done with Accident Evolution Barrier model.

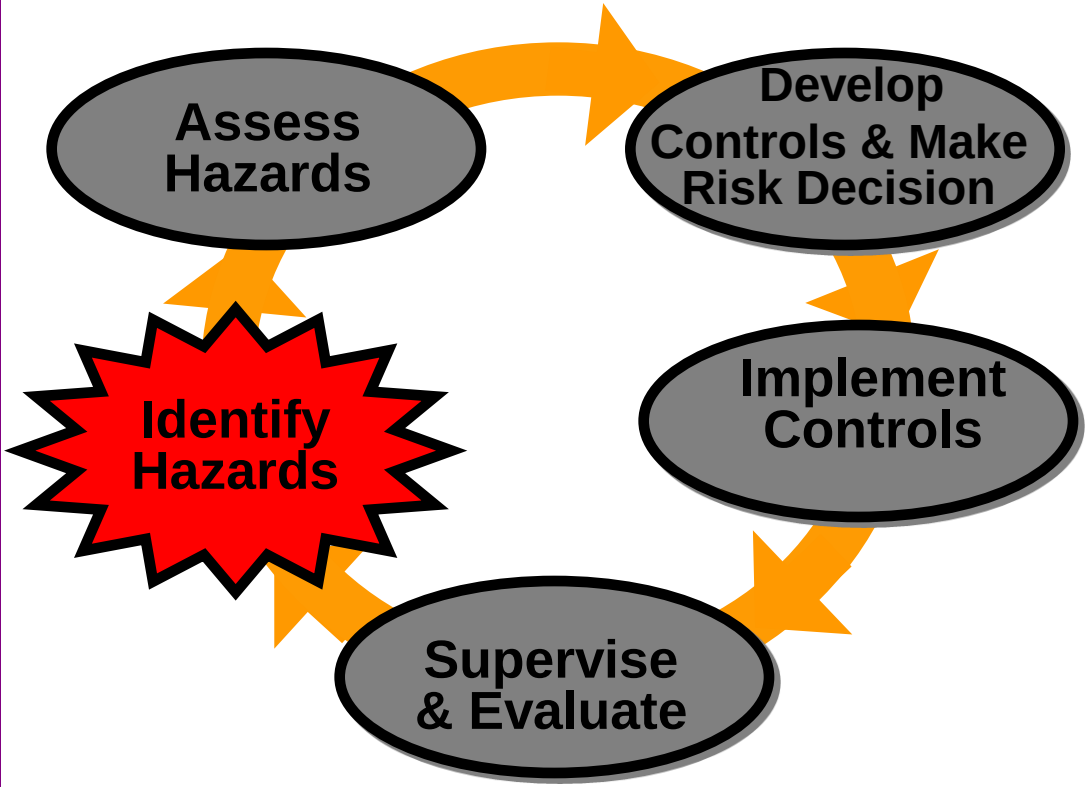
Disaster Planning

- Disaster Planning is a special case of Risk Mitigation which deserves focus on its own for handling extreme situations.
- Disaster Planning deals with how to contain/minimize damage and save lives after an distaster has occurred.

Example of Risk Management Process

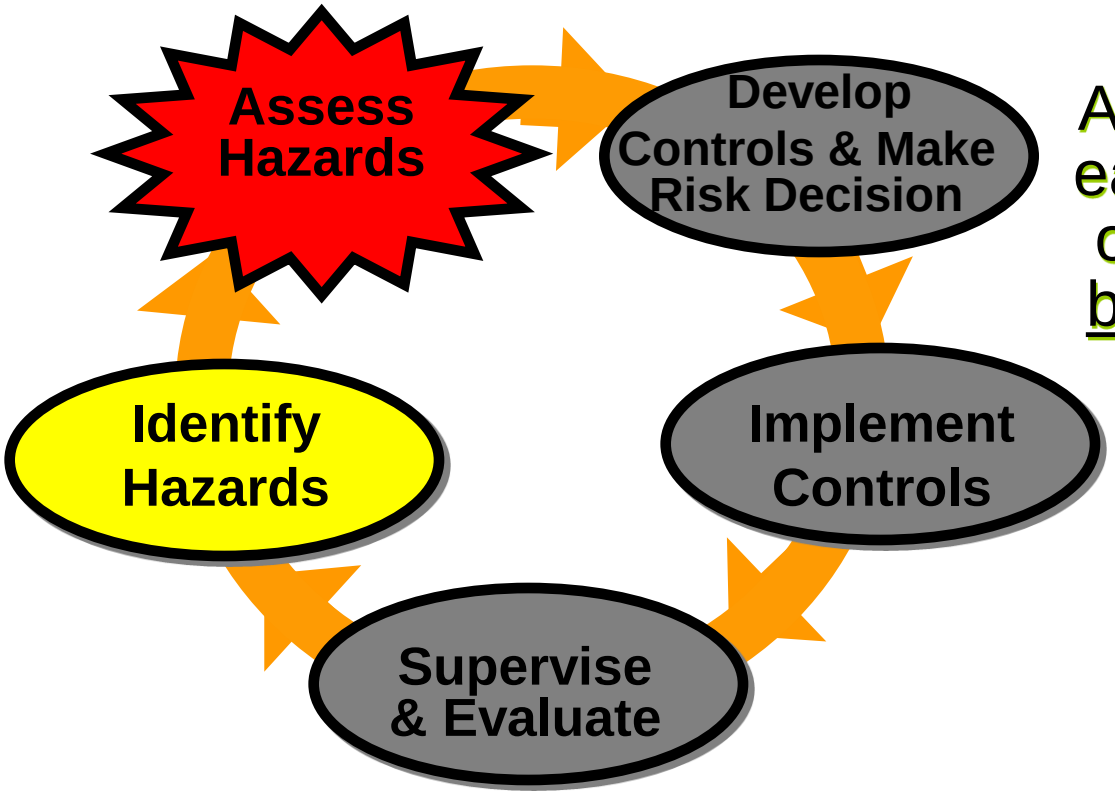


Step 1: Identify Hazards



The objective is to identify hazards that may cause accidents.

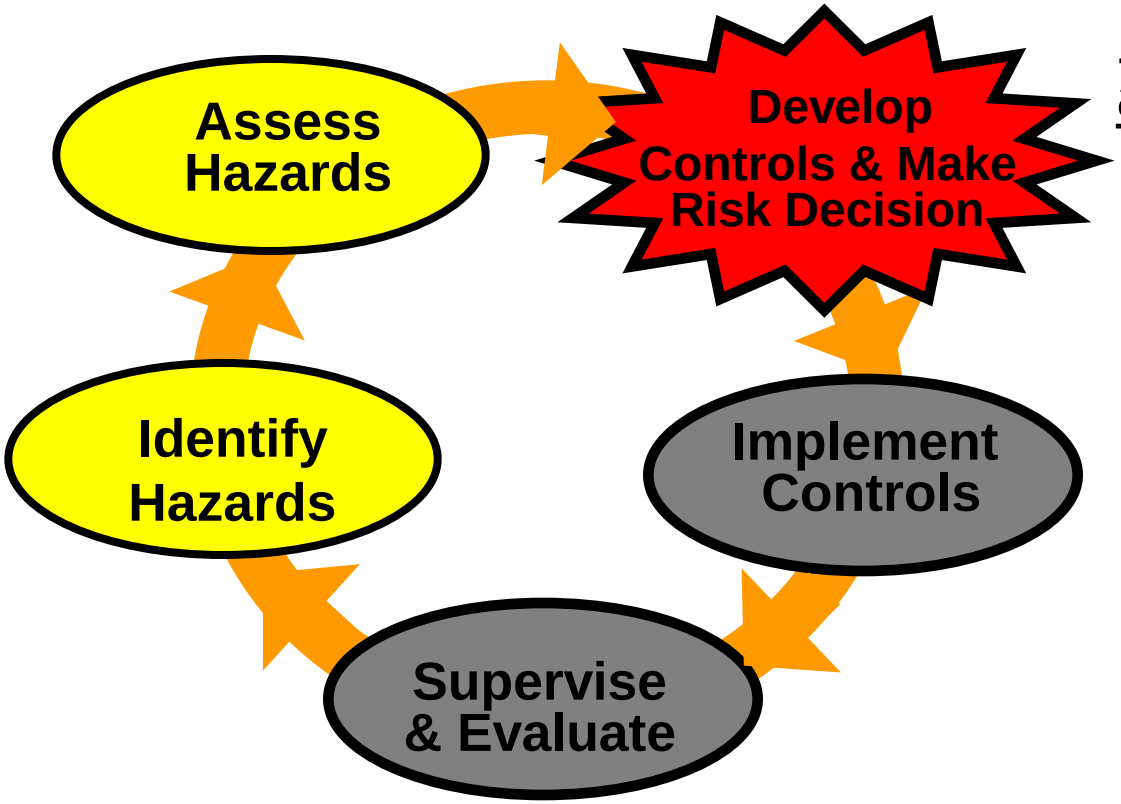
Step 2: Assess Hazards



Assess hazards to determine risks.

Assess the impact of each hazard in terms of potential for loss, based on probability and severity

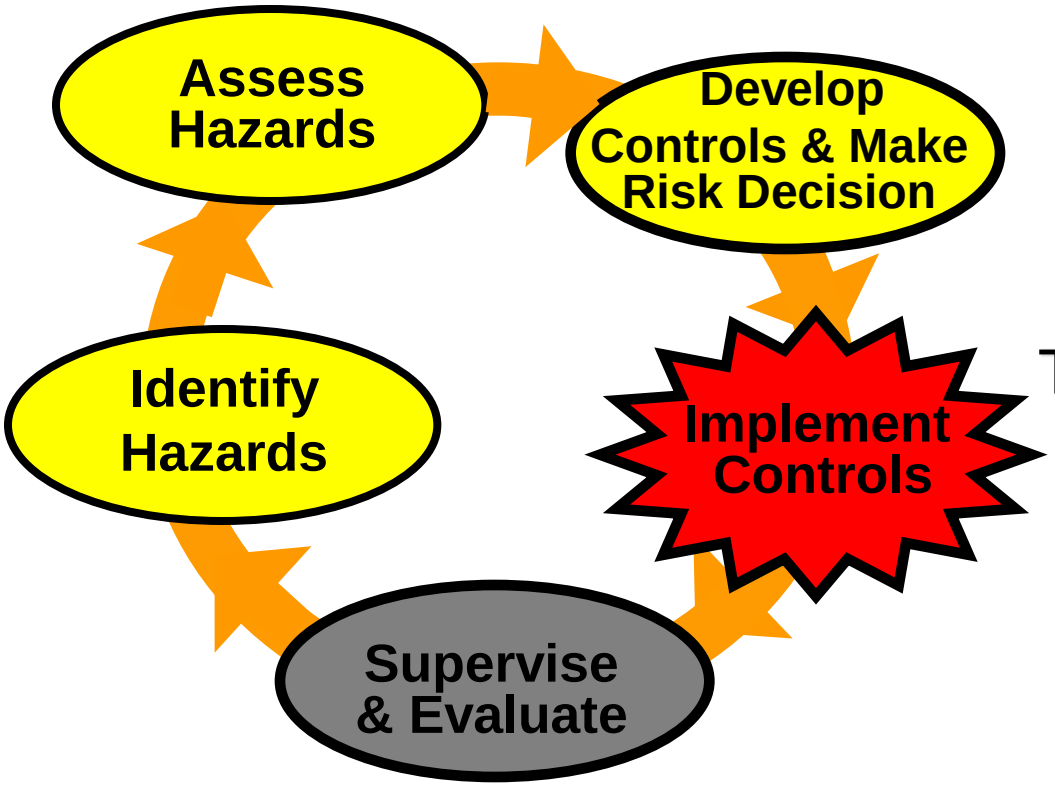
Step 3: Develop Controls & Make Decision



Develop control measures that eliminate the hazard or reduce its risk to an acceptable level

EPL Institute

Step 4: Implement Controls



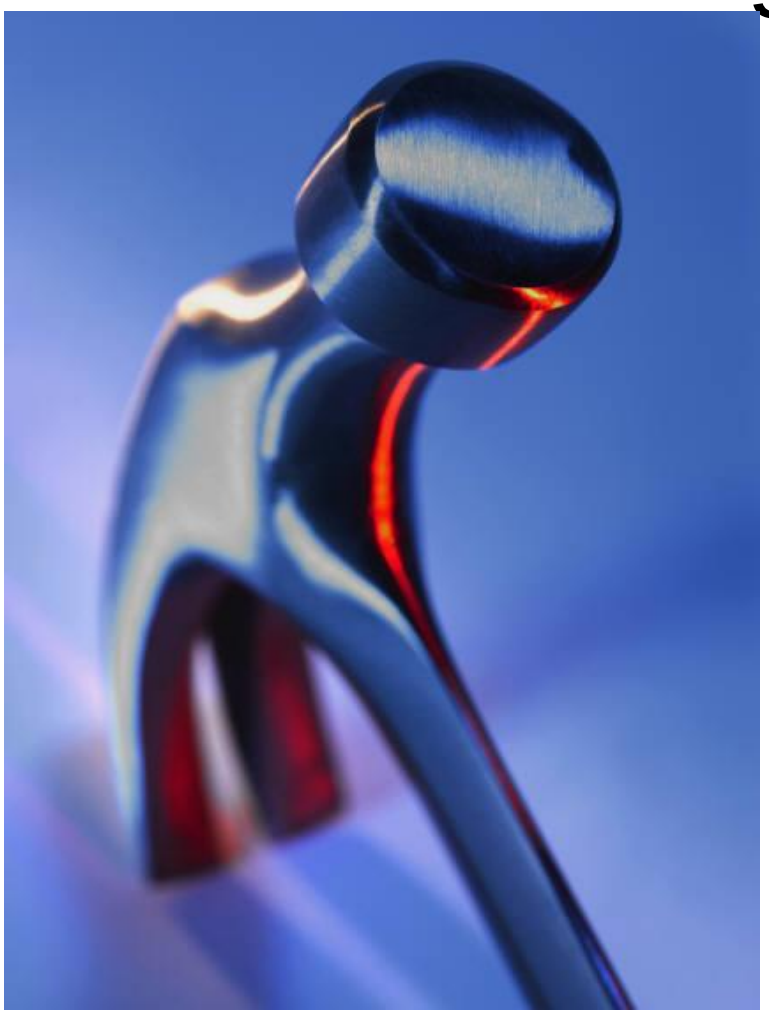
Take action to put the controls in place that eliminate the hazards or reduce their risks

Step 5: Supervise & Evaluate

Perform to, and enforce standards and controls.

Evaluate the effectiveness of controls and adjust/ update as necessary

Part 3 – Traps and common mistakes in Risk Management



Expected Status Quo

- Doing a *HAZARD ANALYSIS?* think *OPERATIONAL PHASE* — Checking the System for Symptoms when it's *Healthy* won't disclose its *Next Disease!*

Expected Status Quo (3)

- SOME OPERATIONAL PHASE EXAMPLES
  - Transport
    Delivery
    Installation
    Calibration
    Checkout
    Shake Down
    Activation
    Standard Start
    Emergency Start
    Normal Operation
    Load Change
    Coupling/Uncoupling
    Stressed Operation
    Standard Shutdown/Stop
    Emergency Shutdown/Stop
    Trouble Shooting
    Maintenance
    …all others…?

Expected Status Quo (4)

- BOTTOM LINE
  Things rarely go wrong when everything's running as it should. The law of Status Quo: If nothing changes, everything will be the same. 1st Corollary: If something changes, things'll be different. Unexpected failure is an annoying difference to have to put up with!

Individuals and RM

- Risk Analysis is done by individs and groups and this is where the biggest lapses are done.
  - Overconfidence
  - Confirmation Bias
  - Gamblers fallacy
  - Anchoring
  - Out of sight out of mind
  - Workspace limitation-problem presentation
  - Biased reviewing
  - Illusory correlation
  - Halo effects
  - Problems with causality

Individuals and RM – Overconfidence

- Decision makers and risk analysts often suffer from overconfidence about the correctness and applicability of their data and analysis of the situation.
- A sign of this is to search for confirmatory evidence and ignore contradictory signs.
- Once you have your data or analysis perform a search for any information which might contradict your findings or to restrict it in space and time.
- If you have already created a plan based on your analysis this plan will be hard to modify or to abandon since in some ways it is a anxiety reducer since it helps you to make sense of the world.

Individuals and RM – Overconfidence2

- Resistance to change is greatest when:
  - The plan is very elaborate, involving a lot of details.
  - When the plan is a product of considerable labour and emotional investment and its completion was associated with a reduction in tension or anxiety.
  - When the plan was the result of a small elite team of people.
  - When the plan has hidden objectives.

Individuals and RM – confirmation bias

- People do not want to change once they have made up their mind!
- Several studies show that decisions made on early on with little or no data interfere with decisionmaking even after plenty of correct and reliable data is available.
- Postpone judgement and decisions until you have gathered all data.

Individuals and RM – Gamblers fallacy or *chance has no memory.*

- The fallacy to assume that because something has not happen for a long time it should happen now or that because something happened recently it should not happen for a long time.
- Gamblers fallacy can make us to be over or underconfident in our decisionmaking.

Individuals and RM - Anchoring

- Your mind develops estimates by using an initial anchor value which is based upon whatever information is provided.
- Anchoring explains to us why first impressions are important. Many people have great difficulties with dispensing of their initial anchors.

Individuals and RM – out of sight out of mind.

- Named the *availability heuristics* by Kahneman (1982) affects us in two ways.
  1. We weight facts stronger if they come readily to mind.
  2. We ignore facts that are not immediatly present.

Individuals and RM – workspace limitation – problem presentation

- This stems from the fact that as humans we have limited resources at hand in our mental ”workspace”.
- Problems put a cognitive strain or load upon us when we try to integrate several mental models to accomodate for the problem.
- This load steers us to work in a first in-first out manner. Therefore the way the problem is presented for us affects the way we try to analyze and solve it.
- Always draft several descriptions of the problem and look at it from different viewpoints.

Individuals and RM – Biased Reviewing

- Also termed as the ”check-off” illusion.
- Before executing most decision makers perform a self check: ”*Have i taken account of all possible factors bearing upon my choice of action?*” They will review which factors were considered and almost the search shows a satiesfactory number.
- We fail to notice that our mental workspace is severly limited and at any given time we considered at maximum 1-2 factors or their rapidly changing representations and not a systematic walkthrough of all factors.

Individuals and RM – Illusory correlation (chapman & chapman, 1967)

- We tend to be poor at detecting covariation relationships except when our world view says that we should expect it.

Individuals and RM – Halo Effect (De Soto, 1967)

- The perceiver's general impression of a target distorts his or her perception of the target on specific dimensions.
- For example, a subordinate who has made a good overall impression on a supervisor is rated as performing high-quality work and always meeting deadlines even when work is flawed.

Individuals and RM – problems with causality.

- We tend to oversimplify causality since we are guided by occurences in the past, we underestimate the irregularities of the future.
- As a rule we plan for fewer contingencies than will actually occur.
- Causal analysis is furthermore influenced by:
  - Reprensentativeness and availability heuristics (tversky & kahneman 1974).
  - Belief that any given event can only have one suffiecient cause. (Nisbett & Ross, 1980)
  - Hindsight bias – Knowledge of a prior event increases the perceived likelihood of that outcome.
  - Due to Hindsight Bias we tend to overestimate our ability of controlling future events. Thus suffering from ”illusion of control”.

Groups and RM

- Largest problem for groups are:
  - Linguistic Imprecision
  - Boss syndrome
  - Willingness to be led

Groups and RM - groupthink

- Groupthink syndrom where hazards/problems are not defined in depth and not really understood.
- The group perceives the problem to be a normal one which is solved by ”business as usual” decision making.

Organisations and RM

- The single worst mistake an organisation can make in RM is to limit communication of data and findings.
- The second worst is to ignore uncomfortable information.
- The strenght of an organisation is that while some managers are not suited to head up Risk Management work (i.e. Gung Ho, Can Do attitude persons) there are always some people that are right for this kind of work.

Organisational responses to hazards (Westrum 1988)

- Denial Actions
  - Suppression: Observers are punished or dismissed, and the observations expunged from the record.
  - Encapsulation: Observers are retained, but the validity of their observations is disputed or denied.
- Repair Actions
  - Public Relations: Observations emerge publicly, but theri significance is denied; they are suger-coated.
  - Local Repairs: The problem is admitted and fixed at the local level, but its wider implications are denied.
- Reform Actions
  - Dissemination: The problem is admitted to be global, and global action is taken upon it.
  - Reorganisation: Action on problem leads to reconsideration and reform of the operational system.

Part 4 – Human Error

Human Error

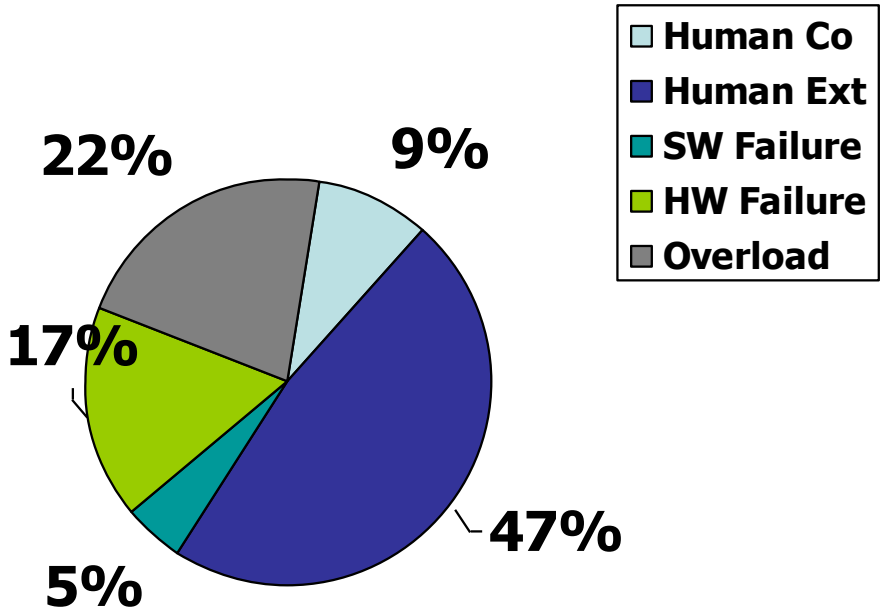
- Theory of human error
- Human error and accident theory
- Addressing human error

Human Error definition

- An inappropriate or undesirable human decision or behavior that reduces or has the potential to reduce effectiveness, safety, or system performance.
- A human action/decision that exceeds system tolerances

Data from Telecom sector

- FCC-collected data on outages in the US public-switched telephone network
  - metric: breakdown of customer calls blocked by system outages (excluding natural disasters). Jan-June 2001



Data from experiments and real life shows

- Training and familiarity don't eliminate errors.
- Types of errors change: mistakes vs. slips/lapses.
- Rate of Human Errors do not go down. I.e. we are not better than humans for 30 years ago.

Theory of Human Error

- The best theory today comes from J.Reasons research and was published 1990. Reason developled the GEMS model for human errors.
- GEMS = General Error Modelling System. Model to understand where human errors stem from.

Origin of Errors according to GEMS

- GEMS identifies three *levels* of cognitive task processing
  - **skill-based:** familiar, automatic procedural tasks
    - usually low-level tasks
  - **rule-based:** tasks approached by pattern-matching from a set of internal problem-solving rules
    - "observed symptoms X mean system is in state Y"
    - "if system state is Y, I should probably do Z to fix it"
  - **knowledge-based:** tasks approached by reasoning from first principles
    - when rules and experience don't apply

GEMS and Errors

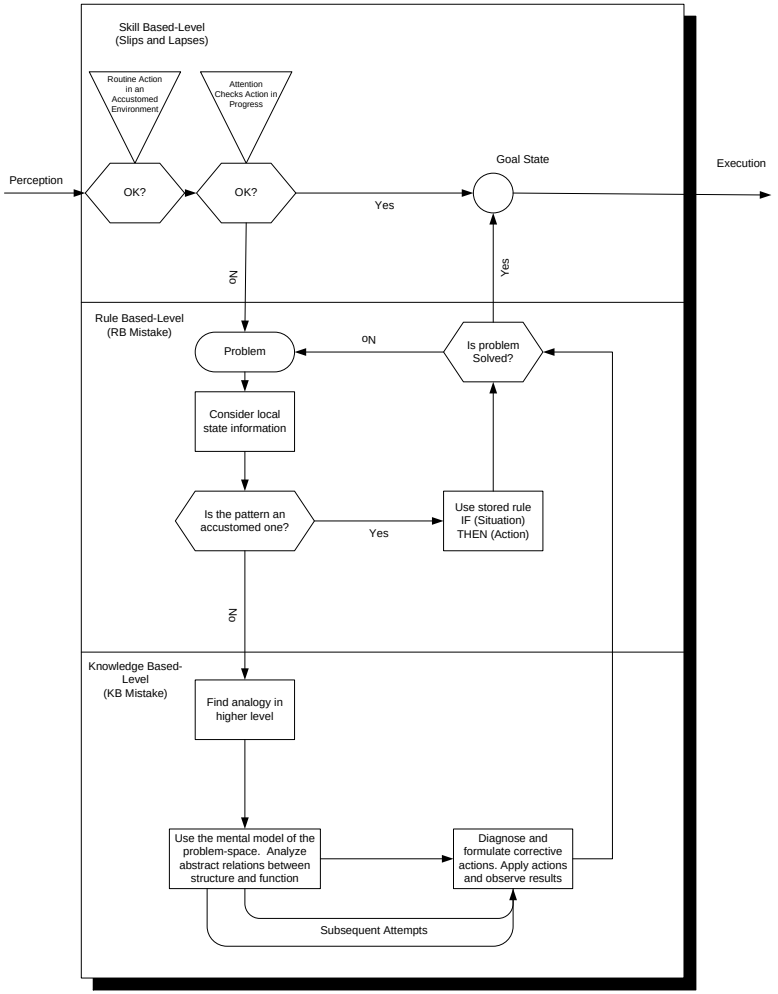
- Errors can occur at each level
  - **skill-based:** slips and lapses
    - usually errors of inattention or misplaced attention
  - **rule-based:** mistakes
    - usually a result of picking an inappropriate rule
    - caused by misconstrued view of state, over-zealous pattern matching, frequency gambling, deficient rules
  - **knowledge-based:** mistakes
    - due to incomplete/inaccurate understanding of system, confirmation bias, overconfidence, cognitive strain, ...
- Errors can result from operating at wrong level
  - humans are reluctant to move from Rule Base to Knowledge Base level even if rules aren't working. We would rather be pattern matching than analyzing.

Contributing Factors

- Inadequate understanding
- Time pressures
- Routine actions and responses
- System status or environmental cues
- Physical / mental fatigue
- Incorrect / distorted information
- Equipment
- Environment
- Management

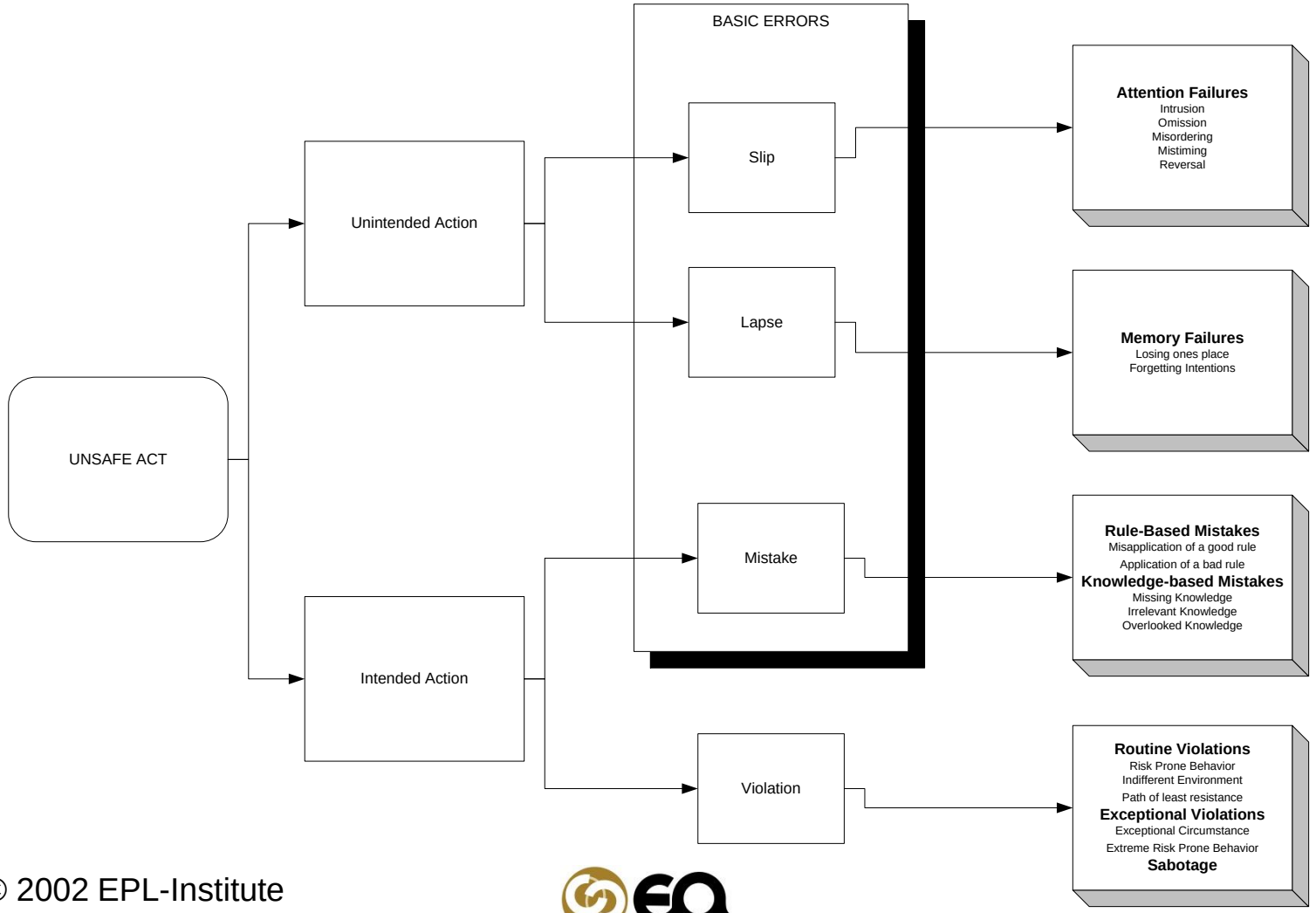
GEMS cognitive Model

- The model shows how we escalate our problem solving depending on the perception of the situation.



Risk Management

GEMS-Generic Error Modelling System



EPL Institute

Error Frequences

- In raw frequencies, SB >> RB > KB
  - 61% of errors are at skill-based level
  - 27% of errors are at rule-based level
  - 11% of errors are at knowledge-based level
- But if we look at *opportunities* for error, the order reverses
  - humans perform vastly more SB tasks than RB, and vastly more RB than KB
  - so a given KB task is more likely to result in error than a given RB or SB task

Error detection and frequences

- Basic detection mechanism is self-monitoring
  - periodic attentional checks, measurement of progress toward goal, discovery of surprise inconsistencies, ...
- Effectiveness of self-detection of errors
  - SB errors: 75-95% detected, avg 86%
    - but some lapse-type errors were resistant to detection
  - RB errors: 50-90% detected, avg 73%
  - KB errors: 50-80% detected, avg 70%
- Including correction tells a different story:
  - SB: ~70% of all errors detected and corrected
  - RB: ~50% detected and corrected
  - KB: ~25% detected and corrected

Minimizing Human Error

- Personnel Selection
- Training
- Design
  - Exclusion Designs
  - Preventative Designs
  - Fail-Safe Designs

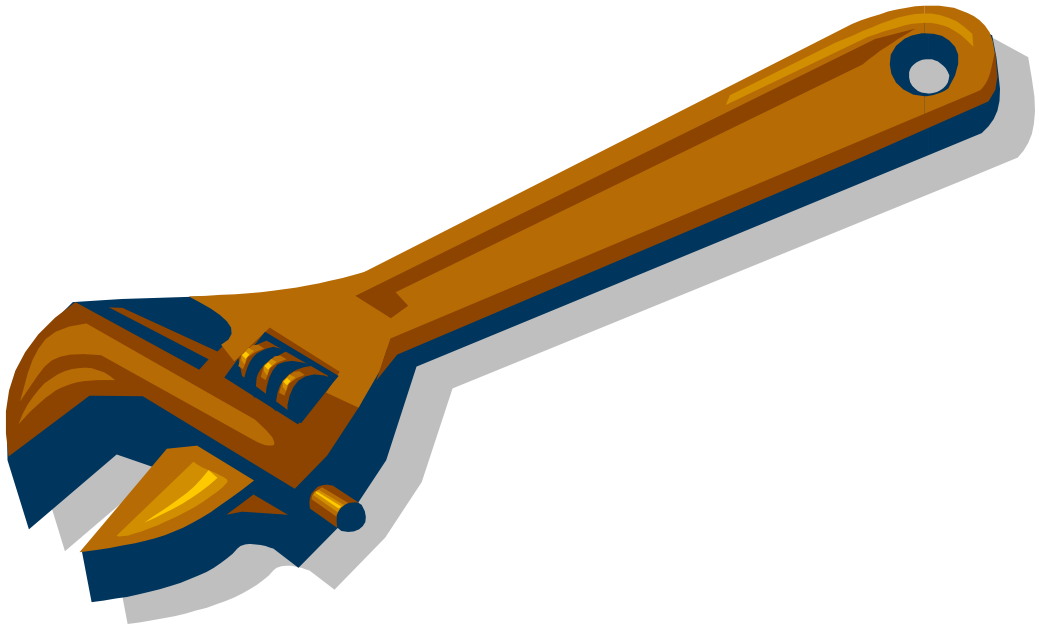
Techniques for Human Error Identification

- Technique for human error rate prediction (THERP)
- Hazard and operability study (HAZOP)
- Skill, rule and knowledge model (SKR)
- Systematic human error reduction and prediction approach(SHERPA)
- Generic error modeling system (GEMS)
- Potential Human Error Cause Analysis (PHECA)
- Murphy Diagrams
- Critical Action and Decision Approach (CADA)
- Human Reliability Management System (HRMS)
- Influence modeling and assessment system (IMAS)
- Confusion Matrices
- Cognitive Environment Simulation (CES)

Error Summary

- Humans are critical to any system dependability
  - human error is the single largest cause of failures
- Human error is inescapable: “to err is human”
  - yet we blame the operator instead of fixing systems
- Human error comes in many forms
  - mistakes, slips, lapses at KB/RB/SB levels of operation
  - but is nearly always detectable
- Best way to address human error is tolerance
  - human-aware Process/System design can help

Part 5 – Risk Management Tools



Which tools for what

- When System Safety Society counted the number of analytical approaches available they found 101 different methods.
- We will present a few wellknown ones which will work fine.
- Differentiate between TYPES and TECHNIQUES
  - TYPES of analysis address *where, when* or *what* to analyze.
  - TECHNIQUES address *how* to analyze.

Some TYPES of analysis

- Preliminary Hazard Analysis (PHA)
- Subsystem Hazard Analysis (SSHA)
- System Hazard Analysis (SHA)
- Operating & Support Hazard Analysis (O&SHA)
- And many more....

Preliminary Hazard Analysis (PHA)

- Is a high-level exercise used to identify system-level safety issues in the earliest development phase of the project.
- Focus on SYSTEM-LEVEL Hazards.
- Used to develop/build away these risks.

Subsystem Hazard Analysis (SSHA)

- Focus on SUBSYSTEMS in order to:
  - Find new Hazards. (critical human input errors, component failure modes..)
  - Verify compliance to safety protocols
  - Recommend actions to reduce or control risk.

System Hazard Analysis (SHA)

- Focus on SYSTEM in order to:
  - Find new Hazards mainly in the interfaces between subsystems and the function of the complete system
  - Verify compliance to safety protocols and functional specifications
  - Recommend actions to reduce or control risk.

Operating & Support Hazard Analysis (O&SHA)

- Focus on OPERATIONAL and SUPPORT:
  - Find new Hazards: in the human factors introduced when operating, supporting and maintaining the system.
  - Assess amended procedures used to eliminate/control or mitigate risks.
  - Recommend actions to reduce or control risk.

Some TECHNIQUES

- Preliminary Hazard Analysis (PHA)
- Fault Tree Analysis(FTA) (backwards and forwards)
- Failures Modes and Effects Analysis (FMEA)
- Probabilistic Risk Assessment (PRA)
- Event Tree Analysis(ETA) (forward)
- Cause Consequence Analysis (CCA)
- Accident Evolution Barrier Analysis (AEB)