

UL the standard in safety

UL UNIVERSITY

## Advanced Uses of Risk Management in Safety Product Design and Development

Steve McRoberts, CSci CPhys MInstP  
Principal Engineer

Word Safety Congress  
Seoul 2008

UL the standard in safety

UL UNIVERSITY

## Outline

- What is Risk Management in Safety Product Design?
  - Purpose of Risk Management
  - Common Misconceptions
- Advanced Application of Risk Management
  - Essential Performance
  - Effective Service Life
  - State-of-the-Art Expectations
  - Gathering Post Production Information

UL the standard in safety Slide 2 UL UNIVERSITY

UL the standard in safety

UL UNIVERSITY

## What is Risk Management in Safety Product Development?

Word Safety Congress  
Seoul 2008

UL the standard in safety

UL UNIVERSITY

## Purpose of Risk Management

- Safety products cover a wide range of technologies and applications
- Can be very simple and low Risk to very complex and high Risk products
- Impossible for Standards writers to provide requirements for, or anticipate, every type of product
- Standards typically trail technology
- Emphasis is placed onto Manufacturer
  - Manufacturer 'knows their product best'
  - Risk Management is a tool to identify, control and monitor all aspects of a product that can effect its' safety and effectiveness throughout the lifecycle.

UL the standard in safety Slide 4 UL UNIVERSITY

UL the standard in safety

UL UNIVERSITY

## Manufacturer's Responsibility

- To systematically apply management policies, procedures, and practices for the purpose of identifying and minimizing Risks from safety products
- To demonstrate a net benefit from use of a safety product over the Risks associated with the product
- 'Assurance' that they are meeting safety requirements, as demonstrated by implementation of the above, on an ongoing basis

UL the standard in safety Slide 5 UL UNIVERSITY

UL the standard in safety

UL UNIVERSITY

## The Failed Paradigm

- When Risk Management is used to legitimize completed design
- When Risk Management is used only to collate risks already identified and attribute arbitrary estimations
- When Risk Evaluation is assumed to be the job of standards writers
- When Risk Management is assumed only to be used in the design phase of a product lifecycle
- When Risk Management is only for new design products

UL the standard in safety Slide 6 UL UNIVERSITY

### The Real Use of Risk Management

- Used to guide a design and make decisions early about methods of controlling design
- Risk Management information develops and evolves with the design
- Risk Evaluation is the job of the manufacturer with input from users and other stakeholders, specific to any safety product
- Risk Management is full lifecycle. Most important phase is production and post production
- Risk Management should be carefully applied to completed designs, focussing on gathering post production information to develop information

UL the standard in safety Slide 7 UL UNIVERSITY

UL the standard in safety UL UNIVERSITY

## Advanced Applications of Risk Management

Word Safety Congress Seoul 2008

### Advanced Applications

- The Risk Management process generates a wealth of information.
- Information and data should not just be left in a raw (albeit organized) form
- Derivations can be made to simplify information into safety concepts focussing on user requirements
  - Essential Performance
  - Essential Service Life
  - High Integrity Characteristics
  - State-of-the-Art Expectations

UL the standard in safety Slide 9 UL UNIVERSITY

### ESSENTIAL PERFORMANCE

- Defined: The performance necessary to achieve freedom from unacceptable risk
- Unacceptable risk to the user, bystanders, environment, property.
- Unacceptable as defined by the safety product manufacturer
- Refers to ability of the equipment to operate or fail in a manner that does not cause unacceptable risk.

UL the standard in safety Slide 10 UL UNIVERSITY

### Identification of Essential Performance

- Identification
  - Using Risk Management information, the manufacturer shall identify which functions of the product relate directly to the products main use and are relied upon for the safety of persons, environment and property
- That directly enable the safety product to carry out its intended use

UL the standard in safety Slide 11 UL UNIVERSITY

### Identification Process

- Comprehensively Identify all product
  - Aspects
  - Features
  - functions
  - Parameters
- What are the core factors relied upon by the user to ensure safety of self, other persons, property or environment?

UL the standard in safety Slide 12 UL UNIVERSITY

## Assumptions

- Taking each function in turn decide whether it forms part of the Essential Performance
- Identify whether function is
  - Degradable Performance
  - Absolute Performance
- Assume a hazardous situation in which there is failure or degradation of these aspects of operation
  - Ignore the probability of factors that lead to hazardous situation
    - Essential Performance must always be preserved in design
  - Assume that in the event of hazardous situation the probability of harm is 100%
    - Worst case condition

## Is it Detectable?

- Will the absence or failure of feature/function be evident to the operator
  - If yes, consider if the operator shall take action that is likely to result in unacceptable use
    - Continue to operate in unsafe condition
    - Make decisions on incorrect operation
    - Rely on inoperable equipment in emergency situation
  - If yes, the feature forms part of essential performance
  - If function is degradable, identify breakpoint
    - Above which the risk of above is acceptable
    - Below which the risk of above is unacceptable

## Is it undetectable?

- Will the absence or failure of feature/function be evident to the operator
  - If 'no,' will the continued operation of the equipment (and exposure to foreseeable 'probable' events) cause unacceptable risk
  - If 'yes,' operation of the function is part of essential performance

## Failure and Risk Addressed State

- The feature or function of the product does not need operate perpetually (nothing does)
- Product should be designed to fail safe
- The safe state should take into account risks related to health safety of persons, damage to property or Environment
- This is the Risk Addressed State
  - A predictable backup response or reduction still part of the Essential Performance

## Concatenation

- The Functions and the response to the functions form part of the complete Essential Performance
- In any foreseen event whether normal condition or fault condition, the product will:
  - act in a proscribed manner maintaining the health and safety of persons, property or environment
  - fail (safe) in a proscribed manner maintaining the health and safety of persons, property or environment
- These are the core values of the design, that must always be evident in all likely events of use, misuse and failure to protect the safety of patient, operator and others.

## Disclosure and Consent

- Preservation of aspects of Essential Performance are (acceptable) Residual Risks
- Manufacturer should consider disclosure of information of Essential Performance to user to allow informed consent of using actual product eg via
  - IFU – inclusions
  - Provision of Training
- Also to further mitigate risks if operator needs to act in a certain manner

## EXPECTED SERVICE LIFE

- A safety product must continue to operate or function or fail safely throughout its determined life
  - Basic safety, and
  - Essential Performance
- Features or functions should not be compromised during the lifetime of the product when the product is subjected to the stresses which can occur during normal conditions of use

## Distinction

- ESL has two components
- “Shelf-Life” – mainly applies to single shot products.
  - How long can a product be stored (within specified parameters) such that when used it will meet its essential performance and safety?
- “Lifespan” – mainly applies to Re-usable and Multi-shot Products
  - how long can a product be used for, such that it still retains its essential safety and performance?

## Analysis

- ESL of any safety product is an implicit customer requirement and forms part of the specifications of the safety product
- Manufacturer must demonstrate that the product continues to meet its essential safety and effectiveness throughout that ESL.
- Ability of a product to be safe and effective over its declared ESL is best evaluated using risk management activity

## Hazard Analysis

- Ability of the product to fail to operate or to cause harm through aging is a hazard
- The defined ESL is the risk acceptability criteria
  - Does not cause unacceptable risk within lifetime meets the Risk Acceptability Criteria
  - To cause unacceptable risk within lifetime does not meet the Risk Acceptability Criteria

## Consider

- The analysis should consider such hazards:
  - Number of cycles or uses and associated wear and tear of components or parts over those uses
  - Material degradation leading to safety hazards
  - Reduction of performance
- Implement risk control measures to control such hazards
  - Preventive maintenance and servicing regimes
  - High Integrity Components – for primary safety means
  - Self Diagnostics
  - User Diagnostics and Inspections

## Consider

- Verify Effectiveness of risk control options
  - Accelerated aging tests
  - User understanding
  - Coverage of self diagnostics
  - Verify number of uses/shots is accurate
- Also consider
  - Use beyond ESL may be a foreseeable misuse
    - Informing of ESL is a mitigation means. Should allow manufacturer to detect when equipment is nearing end of its ESL (Risk Disclosure)
  - Availability of, or willingness to supply servicing and maintenance
  - Availability of spare parts

## STATE OF THE ART

- Does not refer to cutting edge technology
- Refers to user (societal) expectation of risks and benefit from a safety product
  - Maximization of benefit
  - Minimization of risk
  - Expectations of benefit over risk from use and purchase of a safety product
- Differs depending on the specific purpose of the product

## Safety

- Safety or perceived safety is not absolute
  - Incrementally changes with time because of trial and error, accident and incident
  - Real World Events
  - Importance of gathering feedback from real users on expectations and tribulations of the product, its uses, risks and benefits
- Safety of a product is based on what the manufacturer expects and what happens with that expectation

## Generally Acknowledged State-of-the-Art

- Greater safety is achieved by understanding and meeting user's expectation
- Ensuring that solutions to safety problems, essential performance, expected service life and risk control means are aligned with expectations of risk and benefit
- Manufacturer must understand this concept in design and re-design of safety products
- 6 questions to ask

## Six Questions

- How does the subject product compare to currently accepted products?
- Is the Risk the same or less than current accepted products?
- Is the benefit equal to or greater than currently accepted products?
- How does the product compare to other options?
- Are the Risks comparable to similar products for similar (but different) uses?
- Is it 'safer' to refine existing technology before introducing (less understood) new technology

## POST DESIGN INFORMATION

- Product in the hands of actual users
- Risks are no longer intangible
  - Real users, real Risks.
  - Potential harm can be real harm
  - Are all our assumptions correct?
  - Are all our identifications complete?
- Product decommission and disposal are also Risks to be managed

## Feedback

- Institute a pro-active system to gather feedback on the product after design
  - Includes the production and post production phases
- Information should be gathered systematically from
  - Users, Operators
  - Production personnel
  - Installation personnel
  - Service personnel

## Feedback

- Feedback system designed to gather product specific and pertinent information on
  - New unidentified Risks
  - Effectiveness of Risk controls
  - Misuse of product
  - Risk acceptability
- Awareness of similar products in similar use or similar technologies
- Awareness of new standards and new regulations

## Reactive

- Post-production information may consider reactions to anticipated events
  - Ready identification of intolerable Risks
  - Criteria and preparedness for recall
- Be prepared to act on intolerable events

## Improvement

- Gathered information shall be reviewed and inputted back into the Risk Management system
  - Analysis, evaluation and control new hazards pertinent to the product
  - Continued safety and effectiveness for intended use
  - Refinement of product
- Management can trend and analyse all feedback
  - Identify weaknesses and make improvements in parts of the Risk Management system
  - Refinement of system

Thank you for your attention

## Bibliography and References

- IEC ACOS 488/DC
- IEC 60601-1:2005
- ISO 14971:2007
- ISO 9000:2000
- ISO/TR 14969:2004
- A Wildavsky, Searching for safety 1988
- H Petrovski, Success through Failure, The Paradox of Design - 2006