CMPE 233: Human Factors

Human Reliability

- In 1958 Williams suggested that human element reliability must be included in overall system reliability.
- In 1960 proved that human error is the cause for 20-50% of all equipment failure.
- In 1962, a database known as DATA STORE containing time and human performance reliability estimates for human engineering design features was established.
- In 1980, a selective bibliography on human reliability was published covering the period from 1958 to 1978.

Human Reliability Analysis (HRA)

- The probability of accomplishing a task successfully by human at any required stage in system operations within a stated minimum time
  - What can happen, i.e., what can go wrong?
  - How likely is it that this will happen?
  - If it does happen, which are the consequences?
- Relevant terms:
  - PRA = Probabilistic Risk Assessment
  - PSA = Probabilistic Safety Analysis
  - HEP = Human Error Probability = #error/#error opportunities
  - PSF = Performance Shaping Function
  - ASF = Accident Sequence Precursor
  - MTTE = Mean Time to Human Error

Safety Critical Interactive Systems

- Safety Critical Systems
  - Software Engineers
  - System centered
  - Reliability
  - Safety requirements (certification)
  - Formal specification
  - Verification / Proof
  - Waterfall model / structured
  - Archaic interaction techniques

Maximizing Human Reliability

- Increasingly, human reliability needs to go beyond being a diagnostic tool to become a prescriptive tool
- Nuclear industry are looking at new designs for control rooms and want plants designed with human reliability in mind, not simply verified after the design is completed
- NASA has issued strict Human-Rating Requirements (NPR 8705.2) that all space systems designed to come in contact with humans must demonstrate that they impose minimal risk, they are safe for humans, and they maximize human reliability in the operation of that system
- How do we make reliable human systems?
  - Design
  - Test
  - Model
  - "classic" human factors
  - human reliability analysis

What are the links?

- HRA is a set of methods to describe incorrect human actions
- HRA functions in the constraint defined by PRA/PSA
- The accident sequence analyzed by PRA/PSA is typically represented as a tree
  - The action that the operator does is a node
  - Each node carries probability of safety risk, goal failure etc
- Historically, HRA provides the basis for calculating this probability
- HEP is traditionally the sought after probability value
- HEP contains the element of human limitations, but also other environmental factors
- These other factors are called PSF
Probabilistic Risk Assessment

- Models operational functions as trees:
  - Event trees – How can this failure occur?
  - Fault trees – What could happen if...

- Two objectives:
  1. Identify potential areas of significant risk and suggest improvements.
  2. Quantify overall risk from operation.

- Procedures:
  1. Identify sources of potential hazard.
  2. Identify initiating events that could lead to this hazard.
  3. Establish possible sequences from initiating events using event trees.
  4. Quantify each event sequence
     - Frequency of initiating event
     - Probability that safety systems fail when needed.
  5. Determine overall risk.

Event tree

Fault tree

PRA Shortcomings

- Helps identify where additional safety mechanisms are needed, but...
- Events often assumed independent.
- Neglects common-mode failures.
- Quantification can be difficult.
- Does not account for human failures.

Performance Shaping Factors (PSFs)

- Are environmental, personal, or task-oriented factors that influence the probability of human error
- Are an integral part of error modeling and characterization
- Are evaluated and used during quantification to obtain a human error rate applicable to a particular set of circumstances
  - Specifically, the basic human error probabilities obtained for generic circumstances are modified (adjusted) per the specific situation

Example PSFs
**Technique for Human Error Rate Prediction**
- Most popular means of performing HRA.
- Models people as pieces of equipment.
  - Either you succeed or you screw up
- Probability trees model various tasks with success/fail outcomes for each.
  - PSF can influence success/failure probabilities.
- Procedure:
  1. Identify system functions susceptible to human error.
  2. List and analyze related human operations.
  3. Estimate error probabilities using expert judgment and available data.
  4. Estimate effects of human errors on system failure events.

**Operator Action Trees (OAT)**
- Shortcomings of THERP
  - Focuses on *procedural errors* that occurred prior to an accident/incident.
  - Expert judgment is highly variable.
  - More of an art than a science.
- OATS introduced notion of *cognitive error*.
- Cognitive errors typically occur after an accident/incident has occurred.
  - Failure to detect accident event.
  - Failure to diagnose event & devise remedy.
  - Failure to implement remedy correctly.
- But shortcomings:
  - Relies on “best guesses” to fill in values for quantification curve equation.
  - Uses a single time-reliability for all cognitive activities

**Systematic Human Action Reliability Procedure (SHARP)**
- Assists practitioners in selecting appropriate HRA techniques by having defined steps:
  1. Define all possible human interactions
  2. Screen interactions that are significant to the operation and safety
  3. Define the key influence factors necessary to complete the modeling. The model consists of a representation (e.g., qualitative model), impact assessments and quantification.
  4. Assess the impact of significant human actions identified in the preceding steps
  5. Apply appropriate data or other quantification methods to assign probabilities for the various interactions examined, determine sensitivities and establish uncertainty ranges
  6. Report all information for getting a traceable, understandable, and reproducible assessment

**Design Reliability Design Triptych**
- Compliance with applicable standards and best practices documents
  - Where applicable, ANSI, ASME, IEEE, ISO, or other discipline-specific standards should be followed
- Consideration of system usability and human factors
  - System should be designed according to usability and human factors standards such as NASA-STD-3000, MIL-STD-1472, or ISO
- Tractability of design decisions
  - Where decisions have been made that could affect the functions of the system, these decisions should be clearly documented
- Verified reliability of design solutions
  - It is especially important to project system reliability throughout the system lifecycle, including considerations for maintenance once the system has been deployed
  - It is also important to incorporate the estimated mean time before failure into the estimated life of the system
### Testing

- Controlled studies that avoid confounds or experimental artifacts
  - Testing may include hardware reliability testing, human-system interaction evaluation, and software debugging
- Use of maximally realistic and representative scenarios, users, and/or conditions
  - Testing scenarios and conditions should reflect the range of actions the system will experience in actual use, including possible worst-case situations
- Use of humans-in-the-loop testing
  - A system that will be used by humans should always be tested by humans
- Use of valid metrics such as statistically significant results for acceptance criteria
  - Where feasible, the metrics should reflect system or user performance across the entire range of expected circumstances

### Modeling

- Compliance with applicable standards and best practices documents
  - E.g., NASA NPR 8705.5, PRA; Procedures for NASA Programs and Projects or NRC NUREG-1792, Good Practices for Implementing HRA
- Use of established modeling techniques
  - It is better to use an existing, vetted method than to make use of novel techniques and methods that have not been established
- Validation of models to available operational data
  - To ensure a realistic modeling representation, models must be baselined to data obtained from empirical testing or actual operational data
- Completeness of modeling scenarios at the correct level of granularity
  - A thorough task analysis, a review of relevant past operating experience, and a review by subject matter experts to ensure the completeness of the model

### Use of Simulation and Modeling

- Put the virtual back in reality!
  - Simulators: real humans + virtual environments
  - Simulation: virtual humans + virtual environments
- Human performance testing/determination of HEPs

### Human reliability evaluation modeling

- Probability tree: used to perform task analysis by diagrammatically representing critical human actions and other events associated with the system.
- Markov: a powerful reliability engineering tool that can also be used to perform time continuous human reliability analysis under fluctuating situation.
  - $\lambda_h$: human error rate $\Rightarrow$ MTTE $= \frac{1}{\lambda_h}$
  - $\lambda_{nh}$: non-human error rate
  - $P_i(t)$: the probability that system is in state i at time t
  - i=0 system operating normally
  - i=1 system failed due to nonhuman error
  - i=2 system failed due to human error
  - System reliability with human error:
    $$ R(t) = p_0(t) = \exp(- (\lambda_h + \lambda_{nh}) t) $$

### General error rate

- Follows bathtub curve