Human Reliability Analysis in Cognitive Engineering and System Design

Ronald Laurids Boring, PhD
Human Factors Engineer
Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Psychology at an Engineering Forum?

Drug delivery systems

- Biggest challenges are making drug delivery usable and overcoming barriers toward patient or doctor adoption

Emerging nanotechnologies

- Our goal (in simplistic terms) seems to be to achieve computing power and technologies capable of mimicking or equaling the human brain

Nuclear proliferation

- We will see what the speakers say, but I would argue that proliferation is at least as much a psychological challenge as a technological one

Engineering develops tools for human use

- Psychology is part of engineering!

Overview of Today's Talk

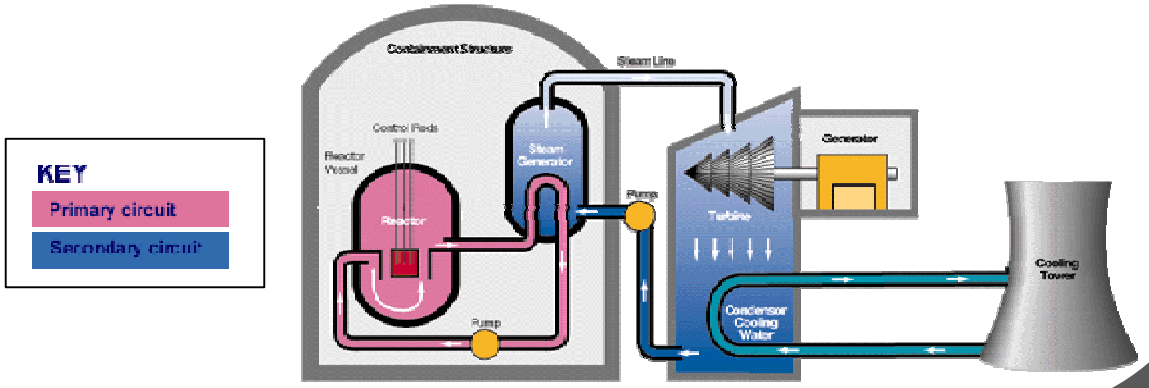
- Brief introduction to human reliability analysis (HRA)
- Discussion of connections to cognitive engineering
- Next steps

Introduction to HRA

Londonberry Township, Pennsylvania
4:00am, Wednesday, March 28, 1979

Londonberry Township, Pennsylvania
4:00am, Wednesday, March 28, 1979

The accident to reactor unit 2 happened when the reactor was operating at 97% power. It involved a relatively **minor malfunction in the secondary cooling circuit which caused the temperature of the primary coolant to rise**. This in turn caused the **reactor to shut down automatically**. Shut down took about one second. At this point a **relief valve failed to close**, but **instrumentation did not reveal the fact**, and so **much of the primary coolant drained away** such that the residual decay heat in the reactor core was not removed. The **core suffered severe damage as a result**. On March 30, it became necessary to **vent a high pressure hydrogen bubble that was forming in the reactor core**. This released approximately 12 millisieverts (mSv) of radioactive gas into the environment.



Londonberry Township, Pennsylvania
4:00am, Wednesday, March 28, 1979

Important Outcomes:

- ***Increased awareness of the risks of nuclear energy.*** Although 12 mSv of radioactive gas were released, extensive environmental monitoring as well as 20-year monitoring of 30,000 individuals living within 10 miles of plant revealed that the average exposure due to the plant was 0.08 mSv and the highest individual exposure was 1 mSv (equivalent dosage to a chest x-ray).

  From a regulatory or industry standpoint, the plant worked as planned. **Radiation was safely contained in the face of a core meltdown**.

  From the public standpoint, this was a "disaster." **No new plants** planned for nearly 30 years.

Londonberry Township, Pennsylvania
4:00am, Wednesday, March 28, 1979

Important Outcomes:

- ***Increased awareness of the importance of human factors*.** The operators were unable to diagnose or respond properly to the unplanned automatic shutdown of the reactor. Deficient control room instrumentation and inadequate emergency response training proved to be root causes of the accident.

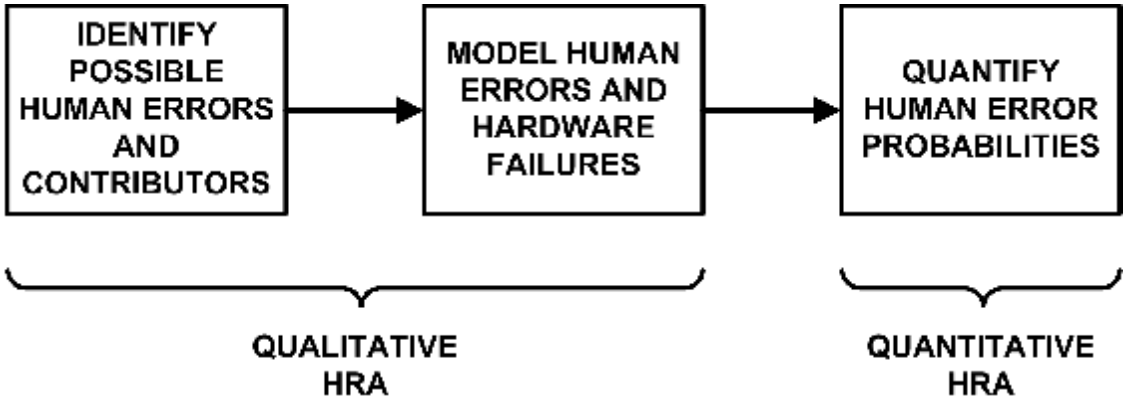
  As a result, the US Nuclear Regulatory Commission began a process of cataloguing all system interface and human performance issues that could increase plant risk.

  Resulting disciplines are called *probabilistic risk assessment* (PRA) and *human reliability analysis* (HRA).

Human Reliability Analysis (HRA)

Definition

- The use of systems engineering and human factors methods in order to render a description of the human contribution to **risk**
- A series of methods to identify sources of **human error** and to predict the likelihood of their occurrence
- Typically considered to have three phases



What is Human Error?

Simple Definition of Human Error

Human Error - Unwanted actions or inactions that result in deviations from expected standards or norms and that potentially place people, equipment, and systems at risk

Human Error is a Significant Part of Risk

Accidents at Sea	90%
Chemical Industry	80-90%
Airline Industry	60-87%
Commercial Nuclear Industry	65-85%

From: D.I. Gertman & H.S. Blackman, *Human Reliability & Safety Analysis Data Handbook*, Wiley-Interscience, 1994.

A 2000 study by the Institute of Medicine published by the National Academies suggested medical errors resulted in 44,000 - 100,000 accidental deaths each year and as many as 1,000,000 accidental injuries

Human Error Makes the News….

"Human Error" Caused Nation's Deadliest Rail Disaster In 15 Years

GILLIAN FLACCUS | September 13, 2008 11:25 PM EST | AP

Compare other versions »

Read More: Los Angeles, Los Angeles Commuter Train Crash, Los Angeles Rail Crash, Los Angeles Rail Disaster, Los Angeles Train Crash, Home News

Buzz up! Show your support. Buzz this article up.

LOS ANGELES — A commuter train engineer who ran a stop signal was blamed Saturday for the nation's deadliest rail disaster in 15 years, a wreck that killed 25 people and left such a mass of smoldering, twisted metal that it took nearly a day to recover all the bodies.

A preliminary investigation found that "it was a Metrolink engineer that failed to stop at a red signal and that was the probable cause" of Friday's collision with a freight train in Los Angeles' San Fernando Valley, Metrolink spokeswoman Denise Tyrrell said.

Human Error Isn't About Pointing Fingers

Sidney Dekker in *The Field Guide to Understanding Human Error* (2006) suggests that the concept of "human error" may be misleading

The Old View of Human Error: The "Bad Apple" Theory

- Humans are unreliable
- Human errors cause accidents
- Failures come as unpleasant surprises

The New View of Human Error

- Human error is the effect or symptom of deeper trouble
- Human error is systematically connected to people's tools, tasks, and operating environment
- Human error is not the conclusion of an investigation but rather the starting point

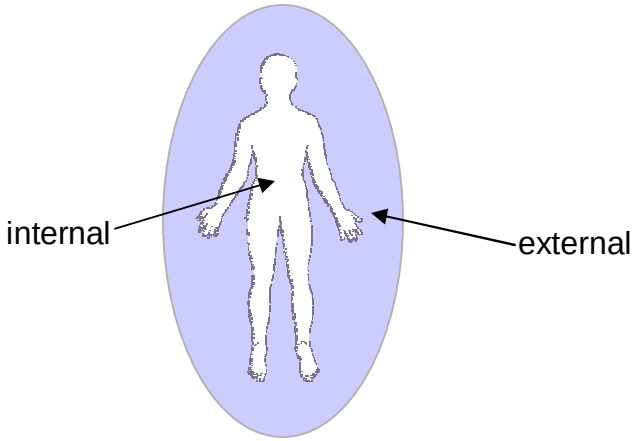
Getting to the Heart of Error with PSFs

Definition of Performance Shaping Factors (PSFs)

- Those influences that enhance or degrade human performance
- Provide basis for considering potential influences on human performance

Often characterized as internal and external

- *Internal PSFs*—influences that the individual brings to the situation such as mood, fitness, stress level, etc.
- *External PSFs*—influences in the situation, task, or environment such as temperature, noise, work practices, etc.



What Factors Might Shape Your Performance in Albuquerque?

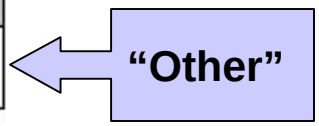
- Climate = drier
- Elevation = higher
- Air conditioning = constant
- Time zone = different

Good Practices PSFs

NUREG-1792 identifies Good Practices for HRA

- Also identifies PSFs that should be considered in a quality HRA

Good Practices PSFs (NUREG-1792)
Training and Experience
Procedures and Administrative Controls
Instrumentation
Time Available
Complexity
Workload/Time Pressure/Stress
Team/Crew dynamics
Available Staffing
Human-System Interface
Environment
Accessibility/Operability of Equipment
Need for Special Tools
Communications
Special Fitness Needs
Consideration of 'Realistic' Accident Sequence Diversions and Deviations



Types of Errors Associated with Events at US Power Plants

From NUREG/CR-6773

Procedures	65%
Training	40%
Supervision	43%
Human Engineering	40%
Communications	35%
Management & Organization	83%
Individual Issues	38%
Workload	10%
System Design	58%
Work Environment	8%

HRA: In the Beginning…

Technique for Human Error Rate Prediction (THERP)

- 1960s: First conceived by Alan Swain at Sandia in an attempt to ensure human reliability in nuclear weapons assembly
- 1970s: Gradual adaptation to nuclear power plant control rooms
- 1983: First external publication as NUREG/CR-1278 for US Nuclear Regulatory Commission
- 1987: First refinement as ASEP method
- 1994: Additional refinement as SPAR-H method
- 2000s: Continues to be widely used and the method against which newer methods are benchmarked
- Over 40 subsequent HRA methods

HRA: In the Beginning….

Sandia/Los Alamos Trivia:

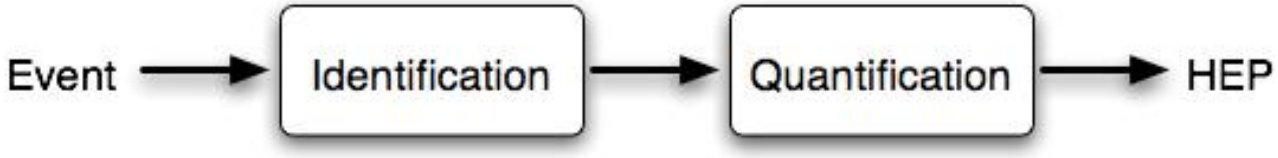
"The unwritten tie dress code"

- Skinny black tie = engineer
- Bowtie = chemist
- Bolo tie = physicist

Qualitative v. Quantitative HRA

Qualitative HRA

- Focused on identification of the event or error
- Common result of task analysis or incident investigation



Quantitative (Probabilistic) HRA

- Focused on translating identified event or error into a **Human Error Probability (HEP)**

Qualitative and quantitative are complementary

- Not all events/accidents/incidents are well enough understood to be quantified (especially events that haven't actually happened)

Quantitative HRA Methods

Expert Estimation

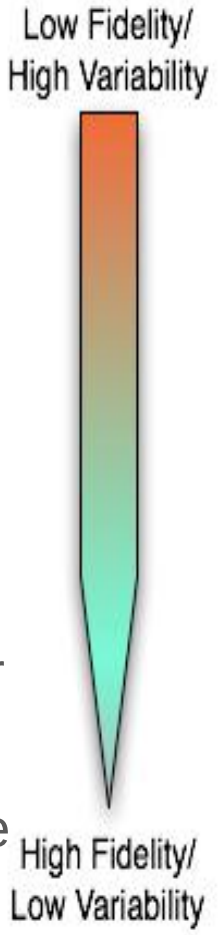
- Determination of an HEP based on expert knowledge of the likelihood that a person would falter in a given context

Performance Shaping Factors (PSFs)

- Use of factors known to degrade or improve human performance over an established baseline
- PSFs often treated as multipliers on a nominal HEP

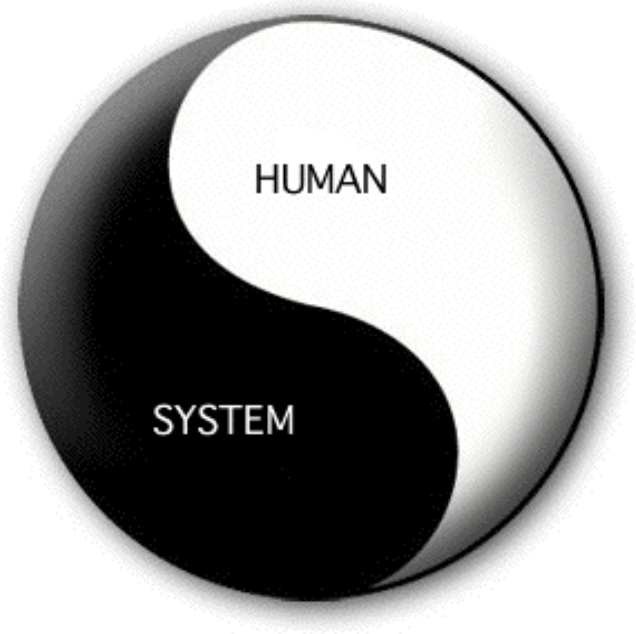
Frequency Based Estimation

- Use of performance data derived from observation of similar events or contexts
- Error is the number of observed failures divided by the number of observed trials in which the human performed the task



HRA and Cognitive Engineering

Two Ways of Looking at Things



Cognitive Engineering

- How do we improve the design of the system to complement the capabilities of the human?

Human Reliability

- How do we decrease the human contribution to the overall system risk?

Two Types of HRA

Retrospective HRA

- Review previous incidents and determine the root cause of the incident in terms of human error
- Review the likelihood of the incident occurrence given the context and ways to prevent recurrence
- Example: Regulator review of licensee event

Prospective HRA

- Identify possible sources of human error in a system that has not been implemented or for an incident that has not been encountered
- Example: Licensee submittals for regulatory approval

A New Emphasis on HRA for Design

- Increasingly, human reliability needs to go beyond being a diagnostic tool to become a prescriptive tool
  - US NRC and 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

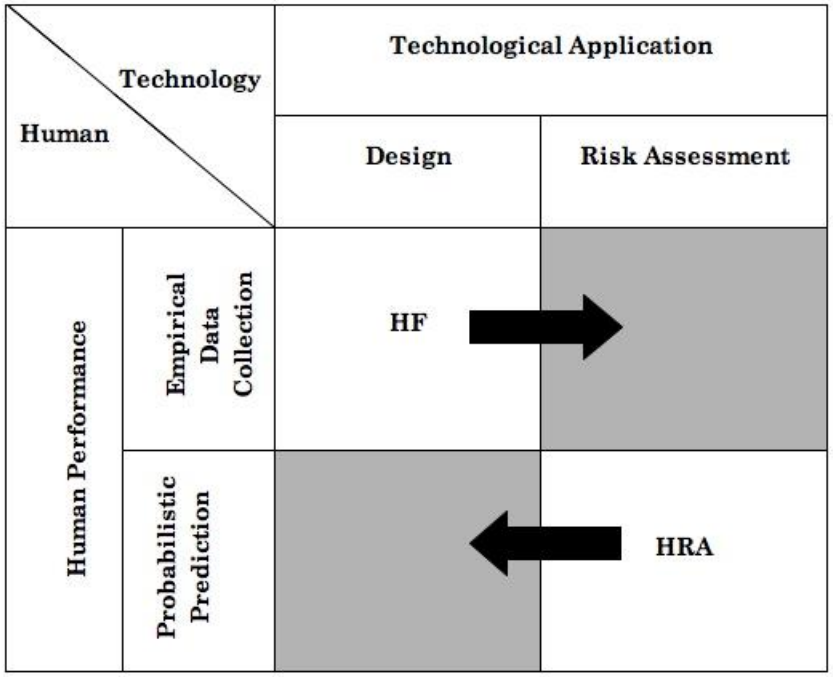
  } "classic" human factors
  - Model

  } human reliability analysis

A Different Way of Thinking About It

HRA and Human Factors Complement Each Other

- HRA receives tremendous benefit from the infusion of human factors data
- But, human factors also gains something
  - HRA uniquely offers ways to prioritize issues, something that must often be done through costly empirical study in human factors
  - Infusing predictive risk modeling in human factors can facilitate more rapid assessment of design work



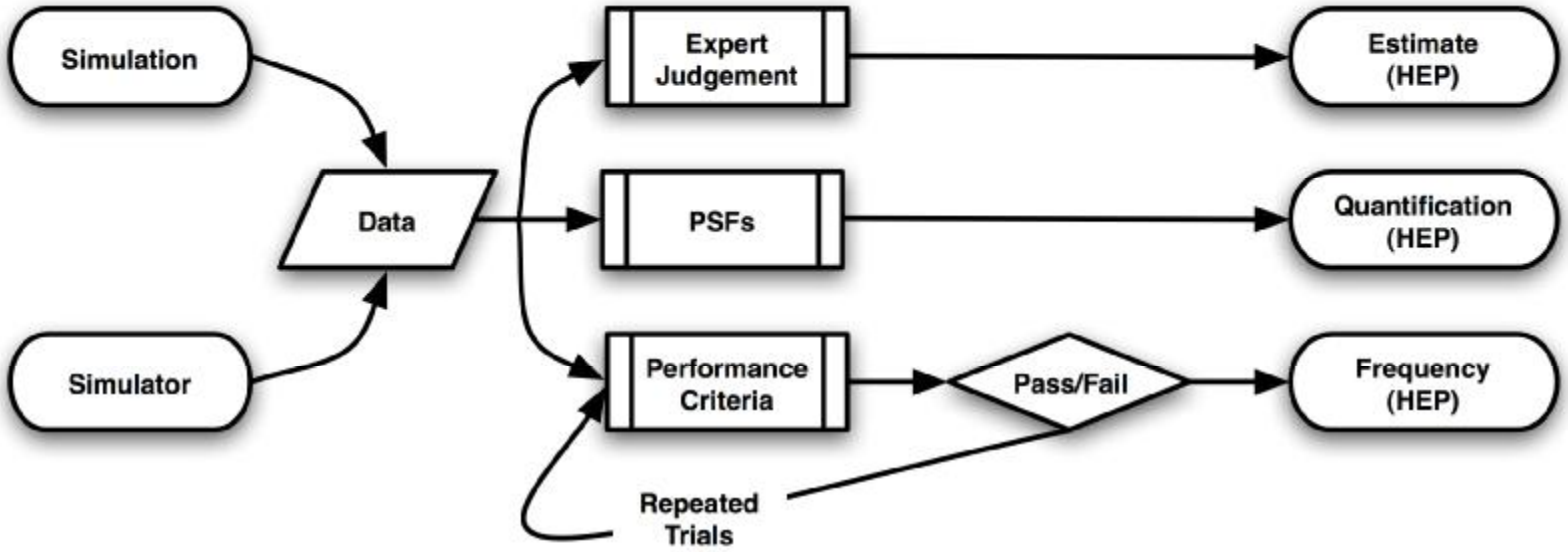
Next Steps for HRA

Data Scrutability

- Earlier HRA methods have not always been carefully validated
  - The PSF multipliers and overall quantification may **not** have drawn on human performance data sources
  - A two-pronged problem
    - Disconnect between human factors and HRA, such that most empirical results from human factors do not readily map to HRA
      - Both are interested in probabilities: Human factors reports significance levels ($p < .05$), but not always the size of the performance effect, enhancement or degradation (ΔHEP)
    - Many HRA methods draw heavily on expert estimation to determine either the PSF multipliers or the overall HEP
      - A normative model of risk should not be based on somebody's best guess!

Use of Simulation and Modeling

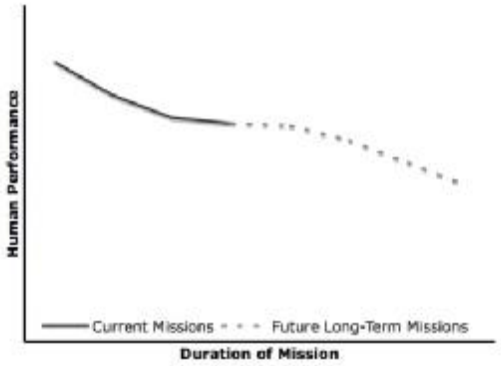
- Put the virtual back in reality!
  - Simulators: real humans + virtual environments
  - Simulation: virtual humans + virtual environments
- Human performance testing/determination of HEPs



Simulation and Modeling for HRA

Quantification through Simulation: "Third Generation" HRA?

- Use of modeling and simulation system with virtual representation of humans to determine situations that may challenge human performance in novel situations
- Process
  - System extensively calibrated to human performance in known situations
  - Across many Monte Carlo style trials, performance extrapolated to novel situation (e.g., long-duration space flight) for which actual human performance data have not been collected



  - Provides preliminary estimates of human error as well as "red flags" for situations that need to be further investigated to determine actual risk to humans or risk of human error

Simulator Studies for HRA

Simulator studies use actual crews to test performance in control room scenarios

- Have primarily been used for human factors design work
  - Test novel control room configurations
- Increasingly being seen as a tool for informing HRA
  - Help to determine the delta between the expected crew performance and actual crew performance
    - International HRA benchmark activity
    - Compare HRA method predictions to actual crew performance
  - Useful for validating PSFs and HEPs

The Key to Improving HRA

HRA needs data!

- Empirical research specific to HRA is underfunded
  - HRA is a tool used in practice, not a research domain in and of itself
- Key to capturing human performance data suitable for HRA is to leverage human factors research
  - Research into Bayesian approaches or meta-analytic techniques to use information from human factors studies and translate it into probabilistic performance data
  - We have no Rosetta Stone from human factors data to HRA

Concluding Thoughts

HRA is a solid set of tools and methods that helps ensure human contributions to risk are identified and mitigated

- Even as a qualitative tool, HRA provides tremendous insights
- HRA may have been too quick to adopt the quantification framework of its hardware reliability siblings
  - HEPs need a data basis
    - There are many efforts using databases, simulations, and simulator studies to gather data
    - More data can be gained by finding a closer union between human factors/cognitive engineering and HRA

RLBORIN@sandia.gov

Human Error Spoiler:
No “G”