

Human Reliability Considerations for the Transition from Analog to Digital Control Technology in Nuclear Power Plants

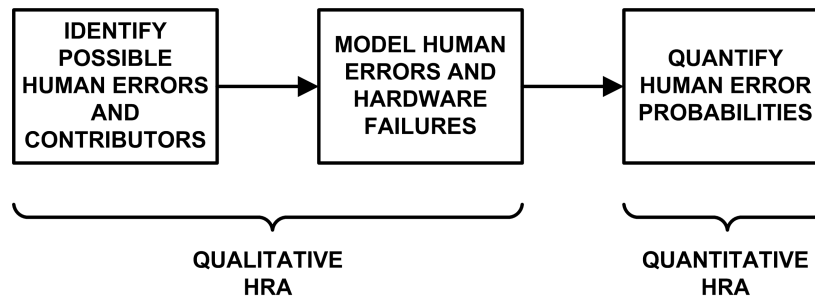
Ronald Laurids Boring, PhD
Idaho National Laboratory



Introduction: The Research Issue

Human reliability analysis (HRA) is framework to identify human component of system risk

- Originally developed for nuclear power to minimize human error
- Recent adoption in other safety-critical areas like oil and gas, aerospace, and defense



HRA has not kept pace with advances in digital human-machine interfaces (HMIs)

- HRA designed for operators in analog control rooms
- Digital HMIs potentially change types of tasks operators perform
- Human error types and probabilities may be different than for analog control rooms
- HRAs for new reactors are being completed with 40-year old methods

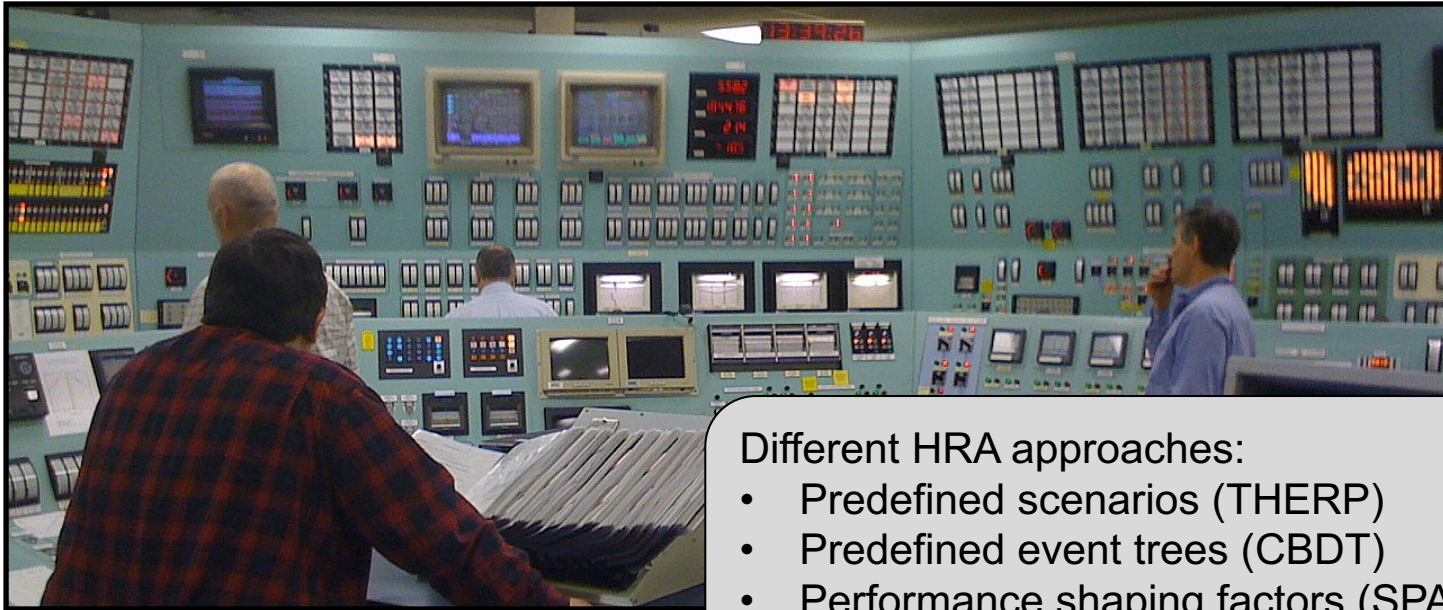
HRA Currently



Analog Main Control Rooms

- Highly proceduralized (paper)
- Analog I&C (one-to-one mapping to plant functions)
- Manual operations
- Distributed control across multiperson crew

HRA Currently



Different HRA approaches:

- Predefined scenarios (THERP)
- Predefined event trees (CBDT)
- Performance shaping factors (SPAR-H)

Method estimates validated to this environment

Analog Main Control Rooms

- Highly proceduralized (paper)
- Analog I&C (one-to-one mapping to plant functions)
- Manual operations
- Distributed control across multiperson crew

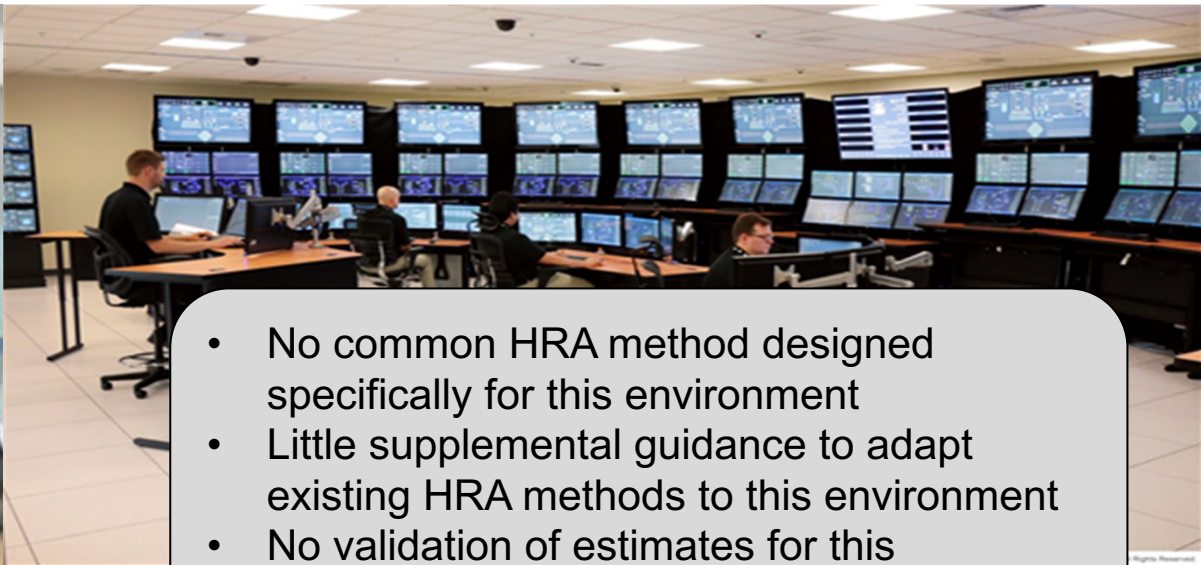
Emerging HRA



Digital Main Control Rooms

- Highly proceduralized (digital)
- Digital HMI (localized control screens and shared overview displays)
- Desktop operations and automation
- Localized control by crew members
- Potential remote control rooms for micro reactors

Emerging HRA



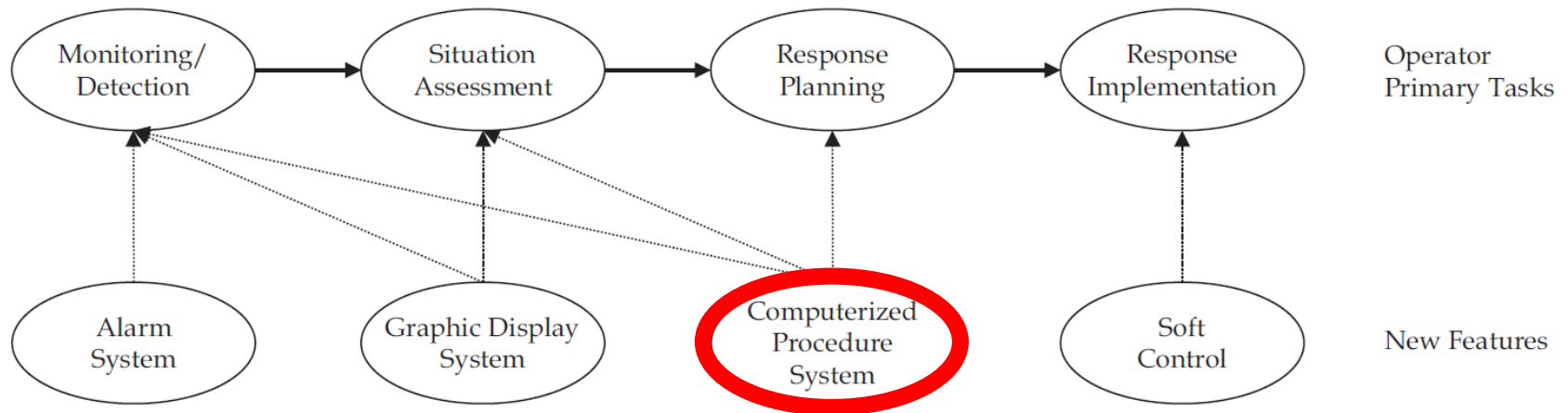
- No common HRA method designed specifically for this environment
- Little supplemental guidance to adapt existing HRA methods to this environment
- No validation of estimates for this environment

Digital Main Control Rooms

- Highly proceduralized (digital)
- Digital HMI (localized control screens and shared overview displays)
- Desktop operations and automation
- Localized control by crew members
- Potential remote control rooms for micro reactors

What Are the Differences

- To identify candidate technologies, Kim and Dang (2011) suggest pairing technologies to operator primary tasks

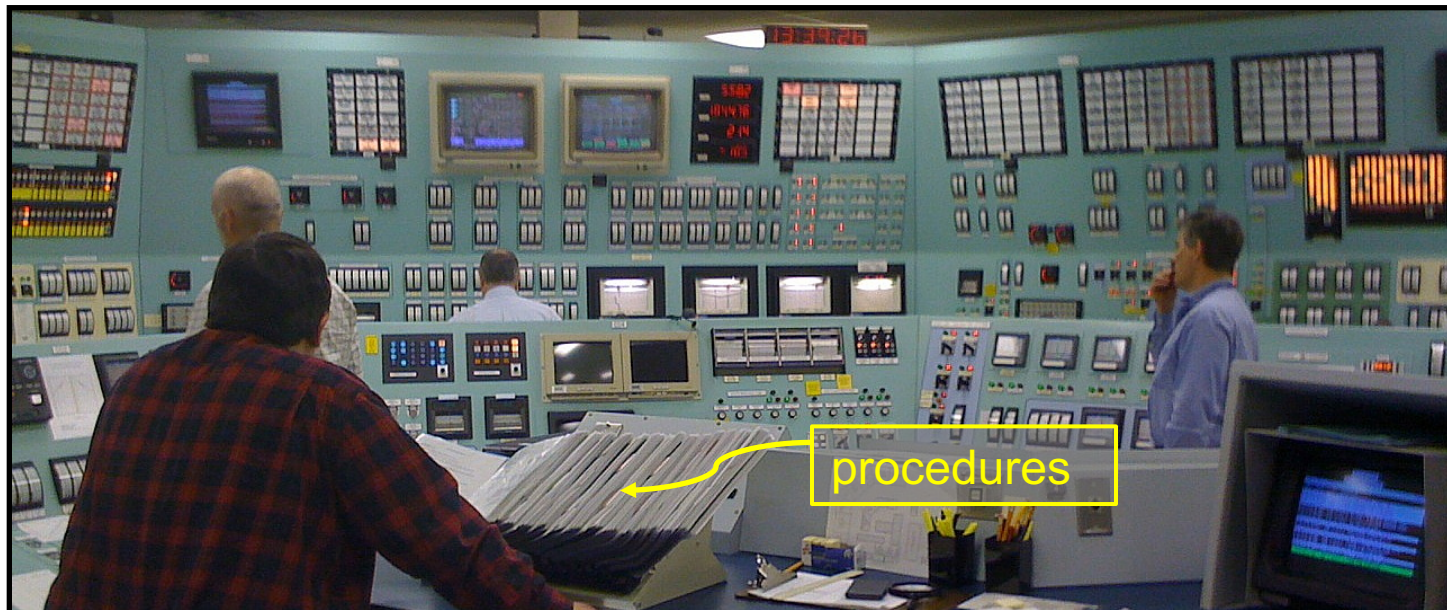


- Framework may omit some important aspects of technology interaction like **automation** or **crew interactions** and new error types such as caused by **cybersecurity exploits**
- Serves as useful starting point for identifying technologies and human interactions with that technology

Procedure Use as a Quick Example

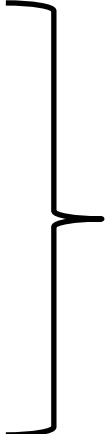
Operators are Required to Follow Procedures Closely

- No decision or action taken without procedural guidance
- Threeway communication following procedures: Shift Supervisor - Reactor Operator – Shift Supervisor



Procedure Types

Every Control Room Activity in Plant Has Procedure

- Normal Operating procedures
 - Alarm Response Procedures
 - Emergency Operating Procedures
 - Severe Accident Management Guidelines
 - Etc....
- 
- Focus of
most
HRA

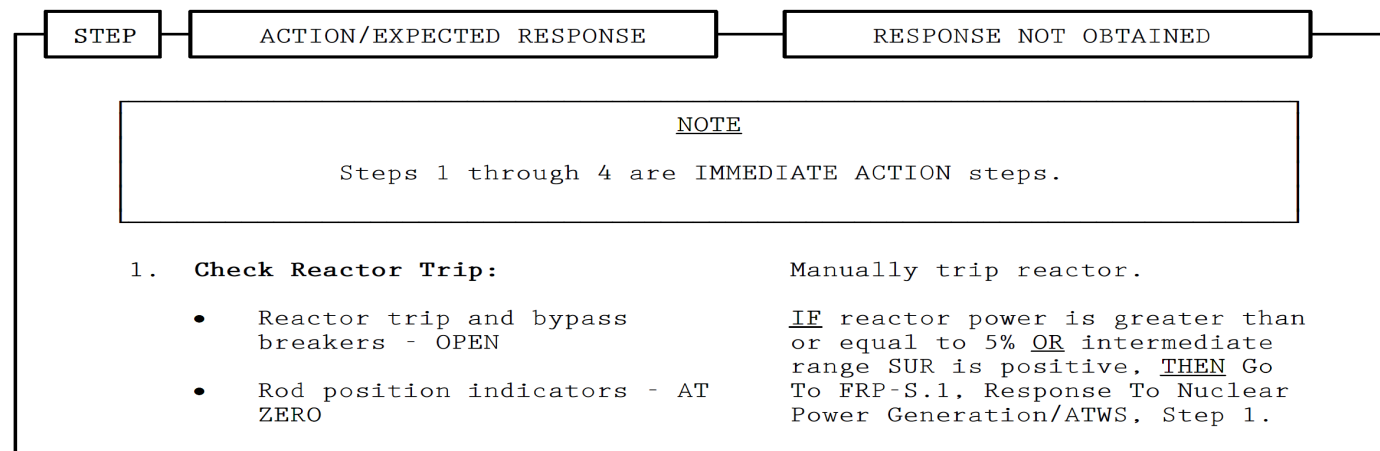
Procedures Outside Control Room are Less Formalized

- Work orders
- Pre-job briefs

Paper-Based Procedures

Currently, Procedures in US NPPs are Paper

- Following Three Mile Island, procedures have been symptom-oriented
 - Symptom – Action – Plant Response – Alternative Action (if First Action Doesn't Work)



- Currently maintain 1000s of pages of procedures in control room

Issues with Paper-Based Procedures

Multiple Simultaneous Procedures

- More than one thing happening at a time
- Placekeeping and navigational challenges for operators

Sequential Presentation of Steps in Procedures

- Operators must loop through procedures, even when they know what's wrong
- No jump ahead and no pause to wait for change in conditions (somewhat resolved by continuous action)

Procedural Information is Static

- May not represent actual plant parameters or conditions

Cautions and Warnings May be Unusable

- Paper foldouts difficult to use

Computerized Procedures

Advantages

- Minimize paper and provide easier updates as needed
- Provide easier navigation to other procedures
- Provide embedded process information
 - Specific parameters needed by procedure can be shown in procedure
- Automatic placekeeping
- Automatic execution of procedure steps

Disadvantages

- Less reliable than paper (need power, hardware, and software)
- Breakdown in control room communication (keyhole effect)

Types of Computerized Procedures

Capability	Computerized Procedures		
	Type 1	Type 2	Type 3
Select and display procedure on computer screen	Yes	Yes	Yes
Provide navigation links within or between procedures	Yes	Yes	Yes
Display process data in the body of procedure steps	No	Yes	Yes
Evaluate procedure step logic and display results	No	Yes	Yes
Provide access links to process displays and soft controls that reside on a separate system	No	Yes	Yes
Issue control commands to equipment from embedded soft controls	No	No	Yes
On operator command, evaluate a sequence of steps that is predefined by the procedure	No	No	Yes

Type 4 = fully automated operations?

Historic HRA Treatment of Procedures

Most HRA Methods Address Paper-Based Procedures

- Earliest HRA method (Technique for Human Error Rate Prediction—THERP) addressed:
 - Errors in the preparation of written procedures (Table 20-5)
 - Failure of written procedure use during normal and abnormal operations (Table 20-6)
 - Omission of a step (as a function of how many steps) (Table 20-7)
 - Different effects of procedures on stress for skilled vs. novice operators (Table 20-16)
- In THERP, poor procedures increase likelihood of error

Current HRA Treatment of Procedures

HRA Methods Treat Procedures as a Performance Shaping Factor

- Procedural Quality (*poor quality increases human error*)
- Procedural Adherence or Use
- Experience and Training on Procedures

Procedures in Practice in HRA

- HRA assumes high quality of procedures, adherence, and training for control room applications
- Only when poor quality, adherence, or experience that human error is increased in the HRA
- Emerging insight: plant, cultural, and regulatory differences in what level of adherence is expected

Human Failure Events for Procedures

HRA Methods Model Most Common Failures in Using Procedures

- Skipping a step
- Misreading or misinterpreting a step
- Performing steps in wrong order
- Performing steps too early or too late for plant requirements
- Going to the wrong procedure
 - Operators must often branch to different procedures
 - e.g., AOP-16 goes to E-0 goes to E-3 for SGTR

New Performance Shaping Factors

Communications

- Computerized procedures with embedded system indications may eliminate the common frame of reference across the control room

Workload

- Ideally, workload decreased by added functionality and ease of use
- If computerized procedure fails, actually increases workload

Human-System Interface Quality and Usability

- Good human factors engineering required for presentation, navigation, and functionality of computerized displays

New Human Failure Modes

Failure to Transfer to Backup Procedures

- Can operator transfer to other computerized or paper backup procedures if computerized system crashes?

Operator Failure Under Degraded Functionality

- Automated diagnosis in computerized procedures may fail, requiring considerable operator expertise beyond what is normally required

Operator Failure to Recover from Input Errors

- If operator initiates wrong action, must be able to backtrack, even if a series of automated actions

Operator Failure to Follow Computerized Procedures

- Skipped step can result in missed information and wrong displays

New HRA Methods?

Current HRA Not Optimized for Computerized Procedures

- THERP, ASEP, CBDT, SPAR-H, and ATHEANA don't address computerized procedures
- No method addresses all aspects of computerized procedures

International Development of New HRA Methods

- MERMOS: French HRA method designed to model the dynamic nature of computerized procedures with automatic diagnosis found in original N4 reactors
- KAERI: Korean HRA method being developed for computerized procedures and other digital HMIs

Commonalities Across Digital Systems

New ways of interacting

- Presentation of information is different
 - Opportunity for crews to work individually
 - Information is consolidated and distilled and not necessarily always visible or shared
- Controls are different
 - Embedded controls in display allow workstation operation individually
 - Higher automation risks taking operator out of loop
- Different drivers on performance
 - Different human failure events
 - Different human error probabilities

Conclusions

HRA is Needed

- Identify where human error traps occur (and prevent them)
- Credit human successful human actions that improve plant performance
- Identify safety margins on human activities where economic efficiencies may be gained

INL is Conducting HRA research

- Gather empirical data with digital HMIs to inform HRA
 - Use full-scope and microworld simulators
- Adapt existing HRA methods to be more digital friendly
 - Current efforts centered on SPAR-H HRA method
- Develop new HRA approaches
 - Dynamic HRA using virtual reactor operators to test wider range of performance including errors of commission
- These HRA activities will improve licensing process



Idaho National Laboratory

ronald.boring@inl.gov