Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria

doi: 10.3850/ESREL2026061419_esrel26-p27665-cd

Human Error Recovery Modeling Using Fault Tree Analysis (FTA): Case Studies in the Steel Industry

Laudelino C. Fonseca Junior
Reliability Department, ArcelorMittal, Brazil. E-mail: laudelino.fonseca@arcelormittal.com.br

Luiza Paneto Grassi
Reliability Department, ArcelorMittal, Brazil. E-mail: luizagrassi34@gmail.com

Celso Luiz Santiago Figueiroa Filho
DSc. Industrial Engineer, Reliability researcher, G-RAMS Inovação, Brazil. E-mail: celso@g-rams.com

Ivan Eric Santos Bergstén
Reliability researcher, Universidade Federal da Bahia, Brazil. E-mail: ivanbergsten@ufba.br

Human reliability is determinant for process safety and operational consistency in steelmaking. Error recovery contributes directly to the final failure probability, yet applied studies addressing how system characteristics influence recoverability and how to represent error and recovery in an integrated model remain limited. Human Reliability Analysis (HRA) techniques provide a basis for recovery modeling, but their guidance is often insufficient for complex industrial applications. This study presents a methodology that integrates Fault Tree Analysis (FTA) with the HRA techniques HEART, SPAR-H, Petro-HRA, and APOA to model human error recovery in operation and maintenance tasks in steelmaking processes. The approach is structured around a cognitive recovery sequence composed of detection, diagnosis, planning, and execution, represented in FTA by an AND gate combining the failure of each stage. Human Error Probabilities (HEP) were estimated using HEART and SPAR-H to assess recovery under operating conditions. Two FTAs were developed as case studies: hot metal sampling in the blast furnace, including selection of the sampling point and positioning of the lance in the metal stream, and replacement of the planetary gear shaft of an overhead crane. The results show differences between HEP estimates, indicating that HEART provides a more detailed representation of recoverability due to its contextual criteria. The proposed methodology supports the identification of critical tasks and deviations affecting recovery and can be generalized to other human-centered activities.

Keywords: Human Reliability Analysis; Steelmaking; HEART; SPAR-H; Petro-HRA; APOA; Fault Tree Analysis; Error Recovery; Human–Machine Interface.

1. Introduction

Human Reliability Analysis (HRA) techniques were originally developed to complement Probabilistic Risk Assessment (PRA) and Process Safety Assessment (PSA), primarily in the context of nuclear power plants (Swain and Guttmann (1983)). These techniques aim to quantify the contribution of human actions to system risk by estimating Human Error Probabilities (HEP) and identifying factors that influence human performance. Over time, several HRA methods have been proposed, including THERP, HEART, SPAR-H, and CREAM, which differ in their modeling assumptions, data requirements, and treatment of contextual influences (Preischl and Hellmich (2013)).

THERP (Swain and Guttmann (1983)) represents the first formal and quantitative HRA technique. It is based on Event Tree Analysis (ETA) and provides a framework for decomposing tasks and estimating HEP through nominal error probabilities adjusted by Performance Shaping Factors (PSF). THERP also introduced the modeling of recovery actions, allowing the representation of corrective steps following an initial error. The quantitative formulation of HEP and the use of multiplicative PSFs were later consolidated in the technical guidelines NUREG/CR-1278 and the Human Reliability and Safety Analysis Data Handbook (Gertman and Blackman (1994)).

Other techniques, such as HEART (Williams (1985)) and SPAR-H Gertman et al. (2005), proposed alternative approaches to HEP estimation. Both methods rely on predefined nominal error probabilities and emphasize the role of contextual factors in shaping human performance. In these techniques, task analysis is typically performed before HEP estimation, but it is not directly embedded in the probabilistic structure of the model. SPAR-H acknowledges the use of Fault Tree Analysis (FTA) as a complementary representation tool; however, FTA is not incorporated as a core element of the method. In contrast, HEART does not reference fault tree modeling in its original formulation.

In the oil and gas sector, the SPAR-H framework was adapted to address industry-specific operational characteristics (Elidolu et al. (2023)), one of the products resulting in the Petro-HRA methodology (Bye et al. (2022);Taylor et al. (2020)). Petro-HRA maintains the general structure of SPAR-H while incorporating sector-specific PSFs, task taxonomies, and guidance for application in offshore and onshore operations. To support the modeling of operational scenarios, Petro-HRA introduced complementary techniques, including the Accident Precursor and Operational Analysis (APOA) (Øie et al. (2023), which employs Fault Tree Analysis to represent causal relationships among technical, organizational, and human factors (Cai et al. (2013)).

FTA is a deductive, logic-based method used in reliability and risk analysis to model combinations of failures that lead to an undesired top event (Vesely et al. (1981)). In the context of HRA, FTA provides a means to represent dependencies between human actions, system states, and recovery opportunities. The integration of FTA with HRA techniques remains limited, particularly with respect to the structured representation of human error recovery processes (Kim et al. (2018); Kirwan et al. (2008)).

Error recovery influences the final probability of failure in industrial environments involving operation, maintenance, and human–machine interaction. Recovery can be described as a cognitive and operational sequence involving error detection, diagnosis, planning of corrective actions, and execution. However, many HRA applications treat recovery in a simplified manner or address it qualitatively, without a probabilistic representation of its constituent stages.

In steelmaking processes, operational and maintenance activities are conducted under conditions that impose constraints on human performance, including time pressure, thermal exposure, and complex human–machine interfaces. These characteristics increase the relevance of error detection and recovery mechanisms in determining the final probability of task failure. Despite this, applied HRA studies in the steel industry rarely address recovery as a structured process, and the integration of recovery stages into probabilistic models remains limited.

In this context, this study applies an integrated HRA–FTA approach to represent human error recovery. Two steelmaking activities were selected as case studies to illustrate the proposed approach. The first case concerns hot metal sampling in a blast furnace, focusing on operator actions related to sampling point selection and lance positioning during routine operation, a task performed frequently throughout the day. The second case addresses a maintenance activity involving the replacement of a planetary gear shaft in an overhead crane, characterized by lower execution frequency and the need for coordinated human actions under constrained operational conditions. Together, these cases allow the evaluation of recovery modeling across distinct task types and frequencies within steelmaking operations.

2. Description Of the Method

This section describes the procedure used to combine Fault Tree Analysis with the HRA techniques HEART, SPAR-H, Petro-HRA, and APOA to model human error recovery in operation and maintenance tasks in steelmaking processes. Recovery is represented within a probabilistic structure that allows the evaluation of how task characteristics and contextual factors influence the probability of successful recovery.

2.1. *Conceptual framework for recovery modeling in FTA*

The proposed approach represents human error recovery as a cognitive sequence composed of the following stages:

- Detection;
- Diagnosis;
- Planning or Select task;
- Execution.

In the fault tree structure, the top event is a Human Failure and is modeled by an OR gate, indicating that system failure may occur through different failure modes, in this case, potential deviations from an expected action. As shown in Figure 1, each Failure Mode is combined by an AND gate, representing the set of conditions that must occur jointly for a given failure mode to occur.

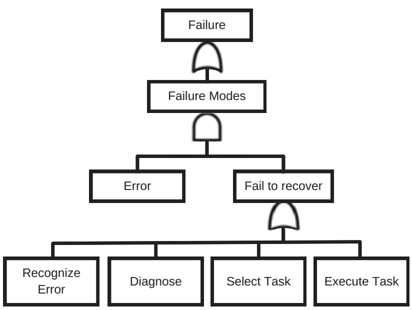

Fig. 1. Fault Tree Analysis representation of the human error recovery model.

Each Failure Mode leads to the events Error or Failure to Recover, which are the initial human error and an unsuccessful recovery attempt following that error. The Recovery model is a combination of basic events corresponding to cognitive stages: Recognize the Error, Diagnose, Plan or Select Task, and Execute Task.

This formulation represents Recovery as an ordered set of cognitive functions and supports the probabilistic evaluation of failure paths associated with incomplete or unsuccessful recovery processes.

2.2. *Task analysis*

Task analysis provides the basis for fault tree development and for the identification of human actions associated with error occurrence and recovery. For each case study, the operational or maintenance activity was decomposed into elementary tasks, stages, steps, and actions, considering normal execution, potential deviations, and associated recovery actions. This decomposition supports the identification of cognitive demands at each recovery stage and establishes traceability between task characteristics and fault tree events. The operator task is the hot metal sampling in the blast furnace. In this process, the operator uses lances to obtain samples of pig iron and slag, choosing the exact point in the bed to collect the sample. It is an environment with risks to the worker due to the proximity to high temperatures, and the consequence of an inadequate sample is the decision to consume more process inputs.

Figure 2 presents the Hierarchical Task Analysis (HTA) diagram used to support the assessment.

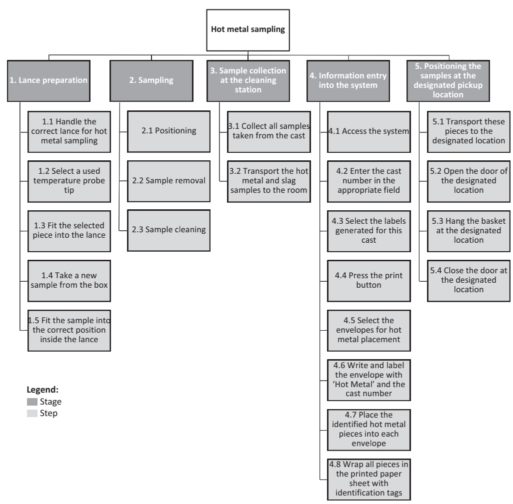

Fig. 2. Hierarchical Task Analysis (HTA) for hot metal sampling.

The maintenance task is the replacement of the planetary gear shaft of an overhead crane. In this activity, the maintenance team must lock out the system, safely access the gearbox, disassemble, clean, inspect, measure, adjust, reassemble, and test the equipment. This work is performed at heights of up to 5 meters, involving the movement of heavy loads. A service failure could lead to the shutdown of an entire production line.

Table 1 presents the decomposition of the *Gearbox drive components assembly* task into steps and actions. For each task step, common Human Factors following the HEART, SPAR-H, and Petro-HRA frameworks are assigned. To represent a risk-related measure, Severity (Se) was included, which reflects the potential consequence of task failure and assumes values ranging from 1 to 7.

Table 1. Human Factors assessment for crane gearbox assembly task, Step 5 decomposition.

ID	Step / Action	Se[1]	Cp[2]	Fam[3]	Fb[4]	Rc[5]	Index
5	Gearbox drive components assembly						
5.1	Input shaft assembly (opposite to reverse)	7	5	5	2	8	44
5.2	Input shaft assembly (reverse side)	7	5	5	2	8	44
5.3	Planetary gear assembly and tie-rod gap adjustment	7	5	5	2	7	50
5.4	Bearing housing and planetary gearbox assembly	7	3	3	4	8	252
5.5	Contact test of south and north input shafts	7	5	5	3	2	263
5.6	Removal of north input shaft and pallet placement	7	5	5	2	8	44

Note: [1]Se: Severity; [2]Cp: Complexity; [3]Fam: Familiarity; [4]Fb: Feedback; [5]Rc: Recoverability.

Complexity (Cp) reflects the number and interdependence of task elements. Familiarity (Fam) indicates the degree of operator experience with the task. Feedback (Fb) describes the availability and clarity of information confirming task execution. These factors assume values ranging from 1 to 5. Recoverability (Rc) represents the potential for error detection and correction before task completion and assumes values ranging from 1 to 8, based on HEART Error Producing Conditions (EPC) multipliers.

The index value is obtained by multiplying Severity and the Human Factors (Cp, Fam, Fb, and Rc). It is used to prioritize task steps for fault tree modeling and Human Error Probability estimation. Higher index values indicate greater criticality from a human reliability perspective and support the identification of steps that may require more detailed evaluation.

The values assigned to the Human Factors were based on expert judgment, considering task conditions, operator experience, available procedural and interface characteristics. These factors not only support task prioritization but also provide a structured reference for the application of HEART, SPAR-H and Petro-HRA. In this context, they were used to support the assignment of Performance Shaping Factors and Error Producing Conditions, and were effectively incorporated into the Human Error Probability estimation.

Recovery can reduce the index, as observed in Table 1 for Actions 5.1 to 5.3. However, when feedback is insufficient, the effect of recoverability is reduced, as illustrated by Action 5.4.

2.3. *HEP estimation using HEART and SPAR-H*

HEP associated with recovery actions were estimated using HEART and SPAR-H. For HEART, nominal error probabilities were selected according to the generic task types defined according to the HEART generic task categories presented in Table 2.

For the Hot Metal sampling task, the Generic Task selected in Table 2 was task E with HEP of 0.02. For the gearbox drive assembly task, the Generic Task selected was F with HEP of 0.003. Although this high-level task for HEP definition, in the FTA, each action had its own HEP value, and in the case of the set of actions for Recovery, the values were standardized.

For SPAR-H, HEP estimation followed the standard formulation based on nominal error rates for diagnosis and action tasks. Nominal HEP values of 1×10^{-2} were adopted for diagnosis tasks and 1×10^{-3} for action tasks. These values were

Table 2. HEART generic tasks and their HEP.

ID	Generic task	HEP
A	Totally unfamiliar task, performed at speed, with no clear understanding of consequences	0.55
B	Shift or restore a system to a new or original state in a single attempt, without supervision or procedures	0.26
C	Complex task requiring high comprehension and skill	0.16
D	Fairly simple task performed rapidly or with limited attention	0.09
E	Routine, highly practised rapid task with relatively low skill demand	0.02
F	Shift or restore a system following procedures with some checking	0.003
G	Completely familiar, well-designed, highly practised routine task, performed frequently by trained personnel, aware of failure implications	0.00004
H	Correct response to a system command supported by augmented or automated supervision	0.00002
M	Miscellaneous task not covered by other task descriptions	0.03

Source: Adapted from (Williams (1985)).

adjusted using Performance Shaping Factors reflecting task conditions, interface characteristics, time availability, and procedural guidance.

2.4. *Assumptions for HEP estimation*

The application of SPAR-H and HEART within the proposed methodology is based on the following assumptions:

- Detection, Diagnosis and Select task actions are treated as diagnosis tasks;
- Execution stage is treated as action tasks;
- PSFs are assigned based on task conditions, human–machine interface characteristics, time availability, and procedural guidance;
- A constant failure rate is assumed for human actions;
- Independence between basic events is assumed unless dependencies are explicitly represented in the fault tree.

2.5. *Integration with Petro-HRA and APOA*

The Petro-HRA framework was applied to adapt SPAR-H-based Human Error Probability estimations to operational and maintenance conditions typical of steelmaking processes. APOA was used as a complementary technique to support fault tree construction and to ensure consistency in the representation of causal relationships among human, technical, and organizational factors.

In this study, human factors defined in SPAR-H and Petro-HRA were evaluated using equivalent criteria. The cultural factor was excluded from the analysis to maintain consistency with the available data and the operational context; therefore, results are presented using a single harmonized set of parameters. Although Petro-HRA and APOA were originally developed for applications in the oil and gas sector, their structured treatment of human factors and causal relationships supports their application in industrial process analysis.

The integrated use of these methods enables the comparison of HEP estimates obtained from different HRA approaches within a unified Fault Tree Analysis structure and supports the evaluation of recovery performance across different task types.

3. Results

Human Error Probabilities were estimated using HEART and SPAR-H to assess recovery under operating conditions. The results are presented for two case studies modeled through Fault Tree Analysis: hot metal sampling in the blast furnace and the replacement of the planetary gear shaft of an overhead crane.

3.1. *Fault Tree models*

Two fault trees were developed to represent the logical structure of human error recovery for the selected case studies. In both models, recovery failure is defined as the top event and is represented as the logical combination of failures in the recovery stages of detection, diagnosis, planning or select task, and execution.

The fault tree developed for hot metal sampling in the blast furnace is presented in Figure 3. The fault tree corresponding to the replacement of the planetary gear shaft of an overhead crane is presented in Figure 4.

3.2. *HEP estimation results*

The HEP estimated from the FTA for the two case studies is summarized in Table 3. The table presents the probability of failure to recover associated with each activity, together with the corresponding frequency of task execution assumptions.

As can be verified in Table 3, the HEART technique results were lower than SPAR-H results. However, the results are proportional for each task analyzed. Although the distance between results, for Human reliability assessment is not uncommon.

3.3. *Comparison between HEART and SPAR-H*

HEART and SPAR-H are based on different modeling assumptions and adopt distinct nominal Human Error Probability values. Consequently, differences in the estimated HEP values are ex-

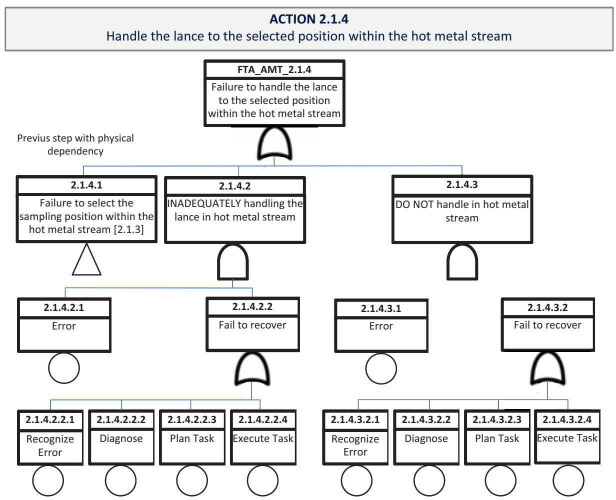

Fig. 3. Fault Tree Analysis representation of the human error recovery model for hot metal sampling.

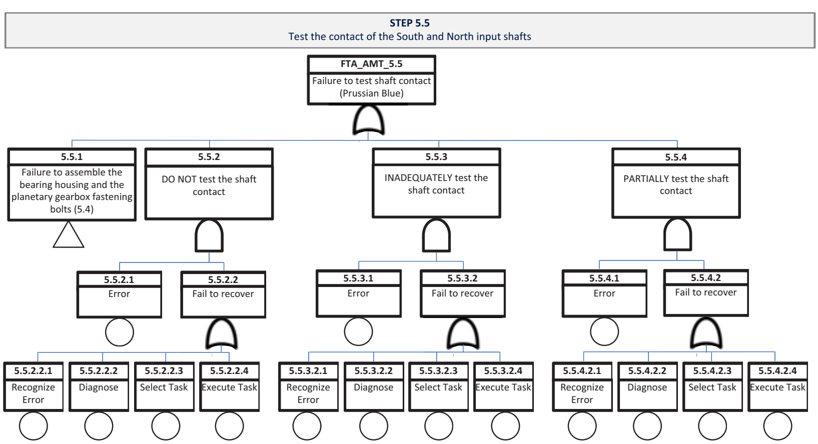

Fig. 4. Fault Tree Analysis representation of the human error recovery model for replacement of the planetary gear shaft of an overhead crane.

Table 3. Human Error Probability estimates from the Fault Tree Analysis.

Case study	Failure (%)	Frequency
SPAR-H		
Planetary shaft replacement	0.1922	0.5 / year
Hot metal sampling	0.1302	3650 / year
HEART		
Planetary shaft replacement	0.1101	0.5 / year
Hot metal sampling	0.0682	3650 / year

Note: Frequencies correspond to typical maintenance and operational activities.

pected. While absolute probability values may vary between techniques, the analysis establishes a comparable range of failure probabilities for the assessed tasks.

SPAR-H does not include a specific Performance Shaping Factor to explicitly account for recovery; therefore, the representation of recovery relies on the structure of the Fault Tree Analysis. In contrast, HEART does not define generic task types specifically for recovery scenarios but incorporates recovery-related aspects through Error Producing Conditions. In this context, FTA supports SPAR-H by providing a structured representation of recovery paths, whereas in HEART it complements the analysis by guiding the selection of appropriate EPCs.

In both approaches, the integration with FTA extends the capability of the techniques to represent recovery processes, enabling a consistent treatment of recovery scenarios within the probabilistic framework.

4. Conclusions

This study presented a methodology that integrates Fault Tree Analysis with the HRA techniques HEART, SPAR-H, Petro-HRA, and APOA to model human error recovery in operation and maintenance tasks in steelmaking processes. Recovery is represented as a sequence of cognitive stages comprising detection, diagnosis, planning or select task, and execution, explicitly modeled within a fault tree structure.

The application of the methodology to two steelmaking case studies showed that the proposed framework enables the representation of recovery as a structured and traceable process. Differences observed between Human Error Probability estimates obtained using HEART and SPAR-H are consistent with their underlying assumptions, particularly regarding the treatment of recovery, which is addressed through Error Producing Conditions in HEART and through fault tree structure in SPAR-H.

The integration of HRA techniques with Fault Tree Analysis supported the identification of tasks and deviations that influence recovery effectiveness. The combined use of task analysis and fault tree modeling enabled the explicit linkage between human actions, contextual factors, and recovery stages, allowing the evaluation of their contribution to the overall probability of failure.

The proposed methodology is applicable to other human-centered activities in industrial processes. Its compatibility with established HRA techniques and its explicit representation of recovery support its use in reliability and safety assessments that require structured modeling of human error recovery.

References

Bye, A., K. Laumann, C. Blackett, M. Rasmussen, S. Øie, K. V. D. Merwe, K. Øien, R. Boring, N. Paltrinieri, I. Waerø, S. Massaiu, K. Gould, J. E. Farbrot, and M. Fernander (2022, 1). The petro-hra guideline. Technical Report IFE/E-2022/001, Institute for Energy Technology, Kjeller, Norway. 9788270179374.

Cai, B., Y. Liu, Y. Zhang, Q. Fan, Z. Liu, and X. Tian (2013, July). A dynamic Bayesian networks modeling of human factors on offshore blowouts. *Journal of Loss Prevention in the Process Industries 26*(4), 639–649. 10.1016/j.jlp.2013.01.001.

Elidolu, G., S. I. Ahn, S. I. Sezer, R. E. Kurt, E. Akyuz, and P. Gardoni (2023, 8). Applying evidential reasoning extended spar-h modelling to analyse human reliability on crude oil tanker cargo operation. *Safety Science 164*. 10.1016/j.ssci.2023.106169.

Gertman, D. and H. Blackman (1994). *Human Reliability and Safety Analysis Data Handbook*.

New York: Wiley. 9780471591108.

Gertman, D., H. Blackman, J. Marble, J. Byers, and C. Smith (2005). The spar-h human reliability analysis method. Technical Report NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Washington, D.C. Technical report.

Kim, Y. et al. (2018). Estimating the quantitative relation between psfs and heps from full-scope simulator data. *Reliability Engineering and System Safety 173*, 12–22. 10.1016/j.ress.2018.01.001.

Kirwan, B., W. H. Gibson, and B. Hickling (2008). Human error data collection as a precursor to the development of a human reliability assessment capability in air traffic management. *Reliability Engineering and System Safety 93*(2), 217–233.

Preischl, W. and M. Hellmich (2013). Human error probabilities from operational experience of german nuclear power plants. *Reliability Engineering and System Safety 109*, 150–159.

Swain, A. D. and H. E. Guttmann (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications (therp). Technical Report NUREG/CR-1278; SAND80-0200, U.S. Nuclear Regulatory Commission, Washington, D.C. Technical report.

Taylor, C., S. Øie, and K. Gould (2020, 2). Lessons learned from applying a new hra method for the petroleum industry. *Reliability Engineering and System Safety 194*. 10.1016/j.ress.2018.10.001.

Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl (1981, 1). *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission. NUREG–0492.

Williams, J. (1985). Heart–a proposed method for achieving high reliability in elsevier. process operation by means of human factors engineering technology in proceedings of a symposium on the achievement of reliability in operating plant. *Safety and Reliability Society*.

Øie, S., M. Fernander, E. C. Bech, J. T. Ludvigsen, and M. Hauso (2023, 8). Analysis of pre-accident operator actions (apoa). Technical report, DNV Netherlands B.V. 9788251503259.