ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Risk Analysis of Highly-integrated Systems

RA III: Human Factors
Human Reliability Analysis
(AIPA, THERP, SLIM, ATHEANA, CREAM)

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Human Factors & Human – System Interface

- 2002 Ueberlingen Airplane Crash – Summary of the Event
- Consideration of Human Factors
- Human – System Interface
- Representation of Human Failures – Human Reliability Analysis
- Accident Initiation and Progression Analysis (AIPA)
- Technique for Human Error Rate Prediction (THERP)
- Success Likelihood Index Methodology (SLIM)
- A Technique for Human Event Analysis (ATHEANA)
- Cognitive Reliability and Error Analysis Method (CREAM)
- Lines of Development – Summary
- References

2002 Überlingen Airplane Crash - Summary of the Event

On 1 July at 21:35:32 (UTC time), a Tupolev TU154M flying from Moscow to Barcelona and a Boeing B757-200 flying from Bergamo to Brussels collided above Überlingen, Lake of Constance (Germany) at an altitude of approximately 10'634 m. 71 persons died and debris of both airplanes crashed on a sparsely populated area of 350 km^2.

Both aircrafts were controlled by the Area Control Centre (ACC) in Zürich.

Reconstruction of the collision based on flight data

Sequence of Events, Boeing B757-200

- The B757-200 freight carrier with two crew members took off from Bergamo at 21:06.
- At 21:21:50 the pilot announced himself to ACC Zürich while he was at flight level (FL) 260. He also requested clearance to climb at FL 360, and at 21:29:50 he reached this altitude.
- At 21:34:30 the co-pilot went to the toilet, but 12 seconds later, at 21:34:42, the on-board TCAS (traffic alert and collision avoidance system) indicated the traffic advisory “traffic, traffic”.
- At 21:34:56, the TCAS indicated the resolution advisory “descent, descent”, and the pilot started immediately to descend.
- The crew saw the other airplane and, at 21:35:10, the TCAS indicated to increase the rate of descent.
- At this time, the co-pilot was back on his seat. At 21:35:19, the crew informed ACC Zürich about the TCAS manoeuvre.
- Immediately before the collision, the control column of the airplane was at maximum inclination.

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Sequence of Events, Tupolev TU154M

- The Tupolev TU154M with nine crew members, five of them in the cockpit, and 60 passengers left Moscow at 18:48.
- At 21:30:33 the pilot announced himself to ACC Zürich, while he was flying at FL 360.
- At 21:34:42, the TCAS indicated the traffic advisory “traffic, traffic”.
- Seven seconds later at 21:34:49, ACC Zürich instructed the crew to descend because of the potential conflict, and the pilot started immediately to descend.
- At 21:34:56, the TCAS indicated the resolution advisory “climb, climb”, and the crew members started to discuss the contradiction between the indication of the TCAS and the instruction of ACC Zürich.
- At 21:35:03, ACC Zürich instructed to increase descending. ACC Zürich also pointed out the position of the other airplane, but this information about the position was wrong.
- At 21:35:24, the TCAS indicated to increase climbing.
- One second before the collision at 21:35:32, the control column was immediately moved to maximum climbing position.

Sequence of Events, ACC Zürich

Control equipment was under repair, but the dispatcher was not appropriately informed about the consequences of this work. As several functions of the system were available only in a reduced but acceptable manner, it would have been necessary to define adequate administrative measures. Neighbouring control centres were not informed about the repair work.

During the repair work, the STCA (short term conflict alert) system in the control room did not provide any visual indicator, but only an independent acoustic indicator.

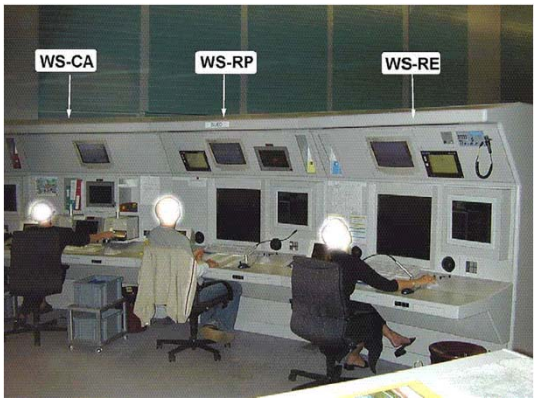
Two dispatchers were on duty – one at work, the other was relaxing in the break room. This practise was accepted by the management during low traffic periods. At about 21:10, the management operator has finished shift, and the dispatcher at work had to take over some of his duties too.

Due to the repair work to the standard telephone line was out of order and, additionally, due to a failure of the backup telephone system, no telephone calls from outside were possible.

Besides the TU154M and the B757-200, the dispatcher was also controlling a delayed landing of an A320 at Friedrichshafen/Germany. The communication with this airplane was on a different radio frequency.

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Because of this situation, the dispatcher had to observe two radar displays at the same time, i.e. he had to move between the two screens. He was not aware of this being an extraordinary situation, and always thought that he could master the situation.



Sequence of Events (Summarising Table)

Time	Boeing B757-200	Tupolew TU154M	ACC Zürich
18:48		Start at Moscow	
21:06	Start at Bergamo		
21:10			Management operator leaves the control room
21:13			Control equipment is put into repair conditions
21:15			Second dispatcher leaves the control room
21:21:50	Announcement at ACC Zürich, FL 260		
21:29:50	FL 360 reached		
21:30:33		Announcement at ACC Zürich, FL 360	
21:34:42	TCAS traffic advisory "traffic, traffic"	TCAS traffic advisory "traffic, traffic"	
21:34:49		Instruction from ACC Zürich to descend Pilot starts immediately to descend	Dispatcher instructs TU154M to descend
21:34:56	TCAS resolution advisory "descent, descent" Pilot starts immediately to descend	TCAS resolution advisory "climb, climb"	
21:35:03			Dispatcher instructs TU154M to increase descending
21:35:10	TCAS indicates increase descending.		
21:35:19	Crew informs ACC Zürich about the TCAS manoeuvre		
21:35:32	Collision	Collision	

Causes of the Accident

The direct causes of the accident are:

- The dispatcher realised too late that the two airplanes were at the same flight level.
- The crew of the TU154M followed the instruction of ACC Zürich, not of the TCAS.

The systemic causes of the accident are:

- The international rules published for the TCAS are not consistent; they are incomplete and partly contradictory.
- The ACC Zürich management accepted that only one dispatcher was required to be present in the control room during times of low traffic, and they accepted that he is controlling two open working items at the same time.

Court Decisions in the Law Suit against 8 Skyguide Employees

On 4 September 2007, the district court of Bülach pronounced the judgment in the law suit against 8 Skyguide employees:

- 3 executives are sentenced for multiple involuntary manslaughter to a conditional prison term of 12 months.
- The sentence for 1 project manager is a conditional fine of 90 daily rates of SFr. 150.– (SFr. 13'500.–).
- Acquittal / verdict of not guilty for 4 accused (1 project team member, 1 system manager, 1 control tower operator, 1 management operator).

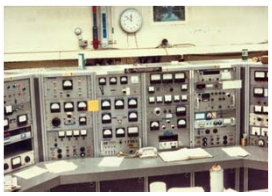
What is a Human-System Interface?

Amount of means by which people interact with a particular machine, device, computer program, or other systems.

Input: allowing the users to manipulate a system.
Output: allowing the system to produce a particular effect.

Examples:

- Screens and multi-screens.
- Control panels.
- ...



Consideration of Human Factors

Not considering human failures result in:

- Disregard of essential factors.
- Unrealistic analysis results as human factors significantly contribute to accidents in various industries.
- Analysis rejection, e.g. by regulatory body.

Human influence on operation of a system include:

- Regular operational actions.
- Maintenance actions, such as inspection and repair.
- Control or triggering of small disturbances.
- Termination of an ongoing of a disturbance, as well as mitigation of its consequences

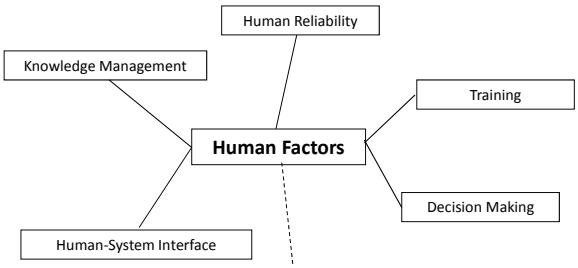
- http://www.bezirksgericht-buelach.ch/zrp/buelach.nsf/wViewContent/2B2DC865BDFACB27C125734C0056248A/$File/Mediemitteilungen%204.9.2007.pdf

Human Factors

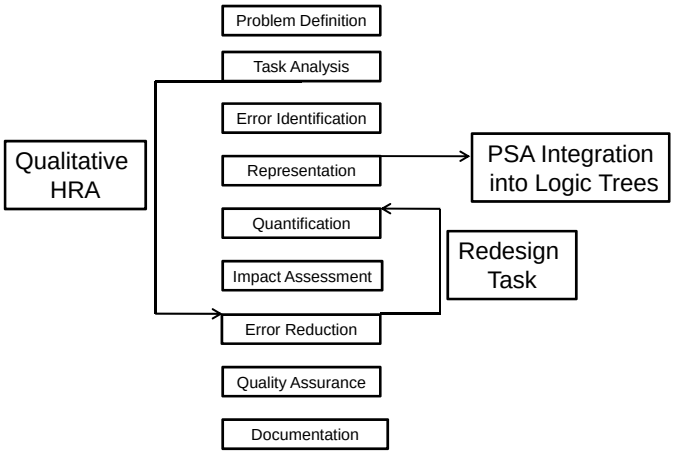
Human factors:

- Study of all aspects which can influence people and their behaviour.
- Human factors is a multidisciplinary subject (Engineering, Cognitive Engineering, Psychology, Biomechanics, Anthropometry etc...).
- Composed of different domains, including Human Reliability Analysis.

Human Reliability is usually defined as the probability that a person will correctly perform some system-required activity during a given time period (if time is a limiting factor) without performing any extraneous activity that can degrade the system.



Human Reliability Analysis Process



Representation of human failures

Human Reliability Analysis

- Identification and understanding of important factors that could affect the human performance. In particular circumstances which can lead the system into "unsafe" conditions.
- Considering the human failure as an integral part of a fault tree or event tree analysis. Part of Probabilistic Safety/Risk Assessment (PSA/PRA).

Example fault tree analysis

- Covers interactions "man-machine" (or system), explicitly and implicitly.
- Models human failures like failures of components.
- Can help identify the most important consequences of human failures to a system.

Requirements

- Detailed knowledge of the system and the required actions / duties (handbooks).
- Taking into account additional factors such as action and duty chains.

The term human error has been defined by Swain in 1989 as: "*Any member of a set of human actions or activities that exceeds some limit of acceptability, i.e. an out of tolerance action (or failure to act) where the limits of performance are defined by the system".*

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Preparation of a HRA

1. Analysis of actions and tasks

- Evaluation of required information.
- Identification of state before and after task execution.
- Identification of information transmission.
- Identification of an adequate classification.
- Identification of interconnections among staff and actions.

2. Analysis of the impact of actions on system safety

- Screening of important actions.

3. Quantification of behaviour

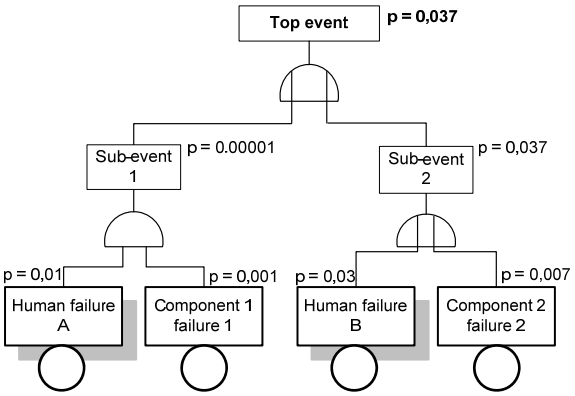
- Practice oriented methods for the identification of failure probabilities:

THERP: breakdown Breakdown of actions into simple sub-actions until estimators are available (like FTA), which consider e.g. the time sequence; consideration of interdependencies afterwards.	**AIPA: time dependent** Behaviour of the operator (s) in charge is modelled as a ratio of required and available time for correct response; consideration of stress afterwards
SLIM: context based Questioning of experts in order to assess actions influencing human failure probabilities. The identification of the probability is then based on a calibration of the expert opinions and on experience.	**CREAM** Identify those parts of the work, as tasks or actions, that require or depend on human cognition. Determine the conditions under which the reliability of cognition may be reduced.

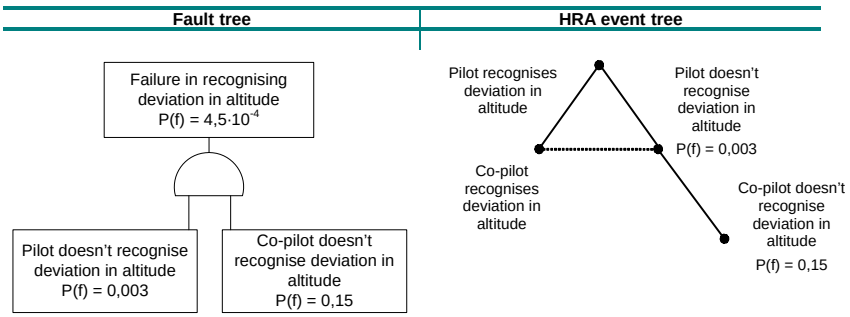
4. Representation of the behaviour within a logical framework

• Creation of a quantitative fault / event tree with component failures and human action failures.

Fault tree



Fault Tree and HRA Event Tree



Accident Initiation and Progression Analysis (AIPA)

Approach

• The operator (individual or team) does not immediately react on a demanded action because of control room displays.
• Given enough time, the operator will most likely take measures that will not aggravate the situation. This is particularly so when the measures taken are well-known and have been trained.
• If the operator recognises that the actions taken do not result in the desired system state he will take further measures.

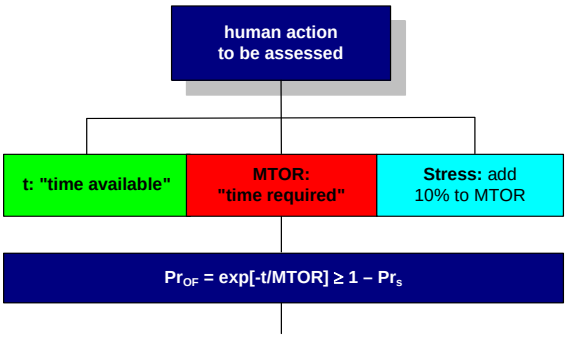
Model Equation

$$\Pr_{OF} = \exp\left[-\frac{t}{MTOR}\right] \quad and \quad \Pr_{OF} \geq 1 - \Pr_{s}$$

where:
$\Pr_{OF}$: Operator failure probability.
t : Available time, from technical characteristics of system.
MTOR : Mean time to a correct operator response (experts' judgment).
Pr_s : Cut off success probability (between 0.99 and 0.9999; individually defined by an evaluator for each action).

Influence of stress : If stress exceeds the usual level, add 10% to MTOR.

Assessment



Failure Probability
General, boundary condition: $10^{-4} \leq \Pr_{OF} \leq 1$

The AIPA Model is characterised by its easy applicability.

Example

In a pump system a storage tank is filled in 10 min and emptied in 50 min. Overfilling the storage tank by more than 30 % leads to the rupture of a disc and the medium is released into the environment. The probability of a control-room operator to respond inappropriately to this situation is given as $3 \cdot 10^{-4}$ (optimum in this situation). According to the describtion of the facility, the operator has 3 min to open the switches, the task requires 30 seconds. The fast closing of the switches will put the operator under additional stress since a release can lead to severe losses.

Setting up the equation: $Pr_S = 1 - 3 \cdot 10^{-4} = 0{,}9997$
$t = 3$ min; $MTOR = 0{,}5$ min

$$\Pr_{OF} = \exp\left[-\frac{3}{0.5 \cdot (1+0.1)}\right] = 4.3 \cdot 10^{-3}$$

Fulfilled boundary conditions: $\Pr_{OF} \geq 1 - \Pr_s$ *and* $10^{-4} \leq \Pr_{OF} \leq 1.$

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Technique for Human Error Rate and Prediction (THERP)

Technique for Human Error Rate and Prediction (Swain & Guttmann, 1983) is probably the best well-known of the first generation HRA methods. The aim of THERP is to calculate the probability of successful performance of the activities necessary for the accomplishment of a task. The calculations are based on pre-defined error rates (called HEPs) and success is defined as the complement to the probability of making an error. THERP involves performing a task analysis to provide a description of the performance characteristics of the human tasks being analyzed. The results of the task analysis are represented graphically in a so-called HRA event tree that is a formal representation of the required sequence of actions.

The **THERP** consists of the following steps:

1. Decomposition of tasks into simple sub-actions until estimators are available.
2. Assigning nominal HEPs to each sub-action.
3. Estimation of effects of performance influencing, shaping factors on each sub-action.
4. Modeling in an HRA event tree.
5. Quantification of total Human Error Probability.

Example: Diagnosis of an "Abnormal" Event:

- The failure of the main feed water supply and – in addition – the emergency water feed of a steam generator is assumed.
- Control room staff has to diagnose this event correctly and trigger recovery reactions within 20 min.
- The staff has to be aware that a corrective action must be in time; otherwise the so-called "feed & bleed cooling" has to be initiated. Inadequate reactions may result in core meltdown.

Assessment of probabilities:

- The assessment of human error probabilities (HEP) needs "models and rules".
- Assessment: if rule 2a (see next table), is applied to the given situation then probability of wrong diagnosis is given by Pr(F) = 0.01.
- Many additional situations and human dependencies are regarded in THERP.

Guidelines for adjusting nominal HEP:

1.Use upper bound of Fig. A if:
The event is not covered in training **or** the event is covered but not practised except in initial training of operators for becoming licensed **or** the talk-through and interviews show that not all the operators know the pattern of stimuli associated with the event.

2. Use lower bound of Fig. A if:
The event is a well-recognised classic (e.g., Three Mile Island incident, 1979), and the operators have practised the event in the simulator qualification exercises **and** the talk-through and interviews indicate that all the operators have a good verbal recognition of the relevant stimulus patterns and know what to do or which written procedures to follow.

3. Use nominal Human Error Probability (HEP) of Fig. A if:
The only practise of the event is in simulator re-qualification exercises and all operators have had this experience **or** none of the rules for use of upper or lower bound apply.

Nominal Model of Estimated HEP for Diagnosis within Time t of an Abnormal Event by Control Room Staff

The probability of a false diagnosis Pr(t) by the operation staff in dependence of the time t [3] after the recognition of an exceptional event. The diagnosis contains the interpretation and, if necessary, the decision making: determination of the causes of the event to find out the system and/or components capable of reducing or eliminating the occurred problems. The given probabilities are not appropriate for a single operator. They already include the redundancies of a typical operator team.

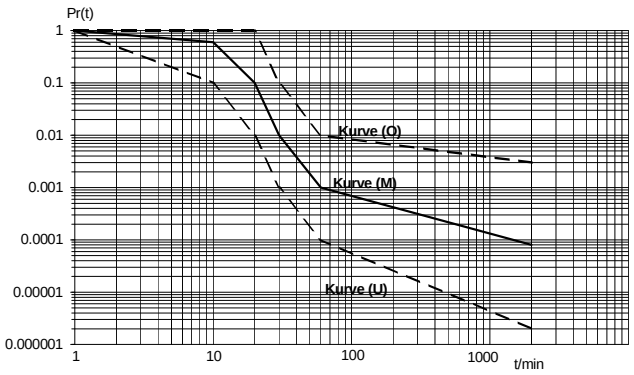
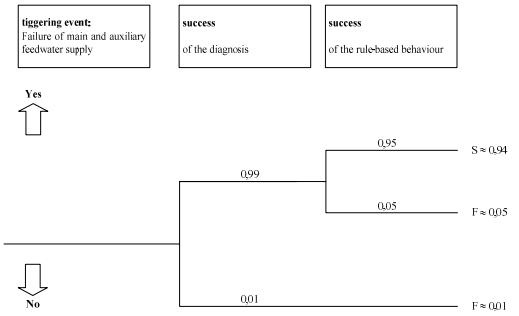


Fig. A: time t in minutes after a compelling signal of abnormal situation.

Overall assessment of human actions

To assess the human actions the "diagnosis" and "behaviour" are combined. Rule based behaviour is also quantified by the application of tables.

Example:
- Probability of false diagnosis: p50 = 0.01
- Probability of false behaviour: p50 = 0.05



⇒ Sum of probabilities of failure paths: Pr_{50} = 0.06

⇒ Pr(system failure) = Pr(triggering event) · 0.06

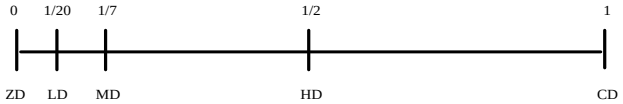
S – success paths

F – failure paths

Dependence of human actions in the THERP-model

Problem: Determination of probability of failure/success of a task may be related to failure/success of other tasks. Application to specific degrees of dependencies:

Degree of coupling	Median
ZD: Zero Dependence (no coupling)	x
LD: Low Dependence (weak coupling)	(1+19x)/20
MD: Moderate Dependence (medium coupling)	(1+6x)/7
HD: High Dependence (strong coupling)	(1+x)/2
CD: Complete Dependence (complete coupling)	1
x: base value of the failure- or success probability	



THERP's advantages:
- It is an overall, well-used in practice methodology.
- It offers a powerful methodology which can be made auditable by the assessor.

It is performed well in terms of accuracy.

Disadvantages:
- It is relatively unstructured.
- It is highly judgmental based on assessor's experience.
- Its interaction between certain PSFs is unknown, therefore can be given no guidelines for possible combinations.

Success Likelihood Index Method (SLIM)

Success Likelihood Index Method (SLIM), (Embrey and Hall,1981), is used for the purposes of evaluating the probability of a human error occurring throughout the completion of a specific task. SLIM is a decision analytic approach to HRA which uses expert judgment to quantify Performance Shaping Factors (PSFs). Such factors are used to derive a Success Likelihood Index (SLI), a form of preference index, which is calibrated against existing data to derive a final Human Error Probability (HEP). The PSF's which require to be considered are chosen by experts and are namely those factors regarded as most significant in relation to the context in question.

The SLIM methodology, lists the following steps in deriving the SLI for each task and converting it to a probability:

1. The selection of the expert panel.
2. The definition of situations and subsets.
3. The elicitation of PSFs.
4. The rating of the tasks on the PSF scale.
5. The ideal point elicitation and scaling calculations.
6. Independence checks.
7. The weighting procedure.
8. The calculation of SLIs.
9. The conversion of SLIs into probabilities.

Typical Performance Shaping Factors, used in SLIM are listed below:

- Time pressure or stress levels.
- Quality of information or of the interface.
- Quality of procedures.
- Level of a task's complexity.
- Consequences as perceived by operator.
- The amount of teamwork required.
- Whether or not there is adequate training or adequate level of competence.

Step 4: PSF Rating

Definition: This example of PSF represents the extent to which operating instructions enhance the ability of an operator to conduct a certain "action".	
Scaling guidance r_k	
Rating	**Example of a fictitious process with the following rating:**
0	Instructions are precisely defined. Operators are able to easily follow the instructions.
1	-
2	Instructions are precisely defined. Operators are able to easily follow the instructions but the clarity could be affected by prior changes or modifications.
3	-
4	-
5	Instructions are available. Some interpretations by the operator are necessary to take certain "actions".
6	Several steps in the procedure may require the operator to return to a previously completed step (e.g. continuous "actions" or keeping ahead skipped tasks).
7	Instructions are being used but due to an urge to act the operator is only capable to use them as check-up.
8	The "action" is a coincidental event for which the instructions can only give a vague advice.
9	Instructions are poorly composed and may lead to wrong actions.
10	No instructions exist for this "actions".

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Step 7: PSF Weighting

PSF "plant-human-machine interface and gauges system": scaled on the possibility of a human-machine interface to provide informatios to succesfully take an "action".	
Weighting w_k	**Example of a fictitious process**
0: insignificant	Other factors are so dominating that I do not care about how good or bad these indicators are because they will not change the human error probability of this specific "action"
1: low	This is an "action" based on the experience of responding to many alarms that require little or no diagnosis. I can easily prove the correctness of my "action" in various ways.
2: normal	Patterns of indicators absolutely force an "action" and check the correct response of the facility but they do not require a thorough checking or assessment.
4: high	A successful "action" is not possible without an adequate response to the facility's gauges. We have to consider specific parameters to diagnose the problem and/or checking the facility.

Summary of the Weighting

Failure Likelihood Index (FLI):

$$\mathrm{FLI} = \sum_{k=1}^{n} w_k \cdot r_k$$

whereas
k= PSF (k=1, 2, …, n) w_k: weighting, r_k: rating.
• w_k and r_k are averaged expert opinions.

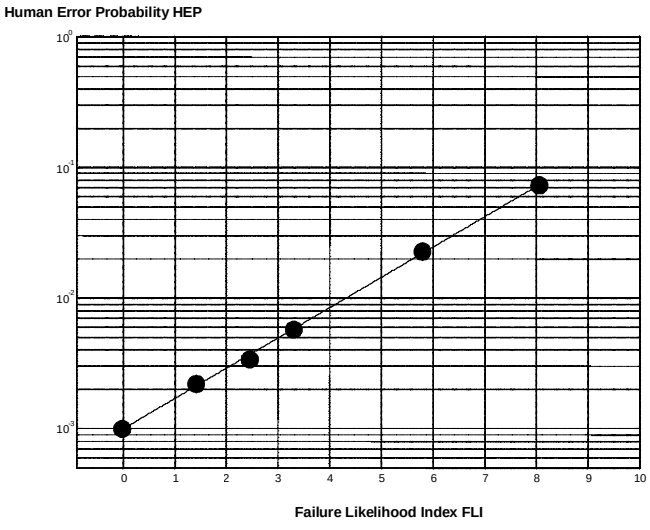
Calibration and Transformation

Transformation of FLI (= relative human error probabilities) in the requested HEP: the calibrated FLI scale is a quantitative relationship between FLI scale and the human error probabilities HEP:

$$\log_{10}(\mathrm{HEP}) = a \cdot \mathrm{FLI} + b$$

whereas
a: slope, *b:* intersection of axes.

Example of a Calibrated Scaling



SLIM's advantages:
- It is a flexible technique and a good theoretical method.
- It is able to deal with the total range of human error forms.
- it does not need task decomposition (task analysis and error taxonomies).

Disadvantages:
- It is a complex method that needs intensive resource.
- PSFs choosing is quite arbitrary.
- It is a subjective method, something that reduces its reliability and consistency.
- Some times there are problems regarding experts' group synthesis.
- There is a lack of valid calibration data (known values).

A Technique for Human Event Analysis (ATHEANA)

A Technique for Human Event Analysis, or ATHEANA, is a human reliability analysis methodology designed to support the understanding and quantification of Human Failure Events (HFEs) in nuclear power plants and it belongs to second generation HRA methods.

ATHEANA's main target are HFEs that occur when the operators are placed in an unfamiliar situation where their training and procedures are inadequate or do not apply, or when some other unusual set of circumstances exists. ATHEANA is an HRA methodology designed to search for situations with one or more of the above characteristics, and estimate the probability of making an error in such situations for use in a probabilistic risk or safety assessment. Such situations are said to have an error-forcing context (EFC) in ATHEANA terminology.

Working Steps:

1. Define and interpret the issue.
2. Define the scope of the analysis.
3. Describe the PRA accident scenario and its nominal context.
4. Define the corresponding HFE which may affect the task in question.
5. Assessing human performance relevant information and characterizing factors that could lead to potential vulnerabilities.
6. Search for plausible deviations of the PRA scenario.
7. Evaluate the potential for recovery.
8. Estimate the HEPs for the HFEs.
9. Incorporate each HFE and corresponding HEP into the PRA.

ATHEANA's advantages:
- It is a focused prediction of the specific error that might be made and the most influential factors affecting that specific error.
- It increases assurance that the major risk associated with the HFE has indeed been captured.
- It is able to estimate HEPs for all sorts of combinations of factors and various conditions.
- It increases the guarantee that the key risks associated with the HFE in question have been identified.

Disadvantages:
- The primary shortcoming of the technique is that from a Probability Risk Assessment (PRA) stance, there is no HEP produced. As a result, the ease with which this analysis can be fit into a predictive quantitative risk assessment is reduced.
- Also, while the method is apparent in categorizing the human factors contributing to an incident, it fails to prioritize or establish details of the causal relationships between these factors. Thus, further work is required to be performed in order to establish the root causes of an incident from a HRA perspective.
- The outcomes of the human errors under consideration are constrained by previously defined sequences of PRA accidents.

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Cognitive Reliability and Error Analysis Method (CREAM)

CREAM (Cognitive Reliability and Error Analysis Method) is a second generation HRA and enables an analyst to achieve the following:
- Identify those parts of the work, as tasks or actions, that require or depend on human cognition, and which therefore may be affected by variations in cognitive reliability.
- Determine the conditions under which the reliability of cognition may be reduced, and where therefore these tasks or actions may constitute a source of risk.
- Provide an appraisal of the consequences of human performance on system safety which can be used in a Probabilistic Safety Analysis (PSA).
- Develop and specify modifications that improve these conditions, hence serve to increase the reliability of cognition and reduce the risk.

The first three steps are the core of CREAM, while the last aims at ensure that the proper conclusions are drawn from the analysis, and that the necessary changes to the system are correctly specified.

CREAM can be used in several different ways as:
- A stand-alone analysis method, for either retrospective or prospective analyses, using a consistent taxonomy for error modes and error causes.
- Part of a larger design method for complex, interactive systems.
- A HRA in the context of an Integrated Safety Analysis (ISA) or Probabilistic Safety Analysis (PSA).

CREAM provides the core functionality of these services, i.e., the concepts, the classification system, the cognitive models, and the methods. In order to be properly used it is necessary to supplement with application or plant specific information, e.g. in the form of values for specific performance parameters, detailed operational and process knowledge that defines the context, etc.

Human Reliability Analysis Methods Comparison

Methods	Strengths	Weaknesses
THERP	▪ overall, well-used in practice ▪ powerful methodology which can be made auditable by the assessor ▪ quite accurate	▪ highly judgmental based on assessor's experience ▪ relatively unstructured ▪ interaction between certain PSFs is unknown
SLIM	▪ flexible technique ▪ good theoretical method ▪ need no task decomposition ▪ deal with the total range of human error forms	▪ complex method ▪ arbitrary PSFs choice ▪ subjective method ▪ lack of valid calibration data
ATHEANA	▪ able to estimate HEPs for all sorts of combinations ▪ increases assurance risk has been captured ▪ focused prediction of the specific potential error	▪ no HEP produced ▪ fails to prioritize or establish details of the causal relationships ▪ outcomes of human errors are constrained by previously defined sequences of PRA accidents
CREAM	▪ allows assessor to tailor to the context ▪ easily applicable into overall safety process ▪ provides an accurate sense of reliability	▪ does not cover collaborative work to great extent ▪ can be time and resource intensive ▪ need expertise in HF (subjective judgment)

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

References

1. Kirwan, B., *A Guide to Practical Human Reliability Assessment*. 1994, London: Taylor & Francis.

2. Swain, A.D. and H.E. Guttmann, *Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report)*. 1983, U.S. Nuclear Regulatory,: Washington D.C. p. 1-554.

3. Khramenkov, S.V. and O.G. Primin, *Operational Paper - Ensuring the reliability of the water piping of the Moscow water supply system.* Journal of Water Supply, 2005. 52(2): p. 127-131.

4. Reason J., Human error, Cambridge University Press, 1990.

5. Gertman D. I. and Blackman H.S., Human reliability and safety analysis data handbook, Wiley, 1994.

6. A study regarding human reliability within power system control rooms, Laboratory for Safety Analysis, ETH Zurich, 2009.

7. Kirwan B., A guide to practical human reliability assessment, Taylor & Francis, London, 1994.

8. Kröger W., "Risk Analysis of Highly-Integrated Systems," Lecture Notes, Zurich, 2007.

9. Hollnagel E., Cognitive Reliability and Error Analysis Method CREAM, Elsevier, Oxford, 1998.

10. Forester J. and Kolaczkowski A., "ATHEANA User's Guide ", Division of Risk Assessment and Special Projects. Office of Nuclear Regulatory Research (ed.), U.S. Nuclear Regulatory Commission, Washington, 2007.

11. Forester J., A. Kolaczkowski, E. Lois, and D. Kelly, "Evaluation of Human Reliability Analysis Methods Against Good Practices," Division of Risk Assessment and Special Projects. Office of Nuclear Regulatory Research (ed.), U.S. Nuclear Regulatory Commission, Washington, 2006.

12. "Aircraft Crashes Record Office,"<http://www.baaa-acro.com/>.

13. "Health and Safety Executive (HSE),"<http://www.hse.gov.uk>.