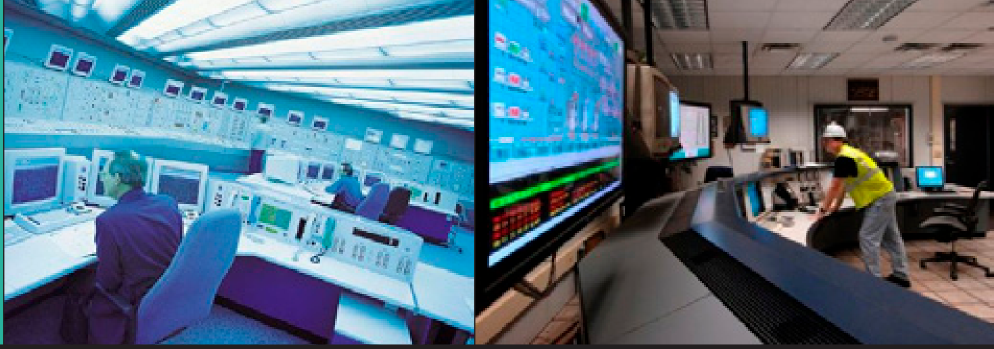
PAUL SCHERRER INSTITUT
PSI

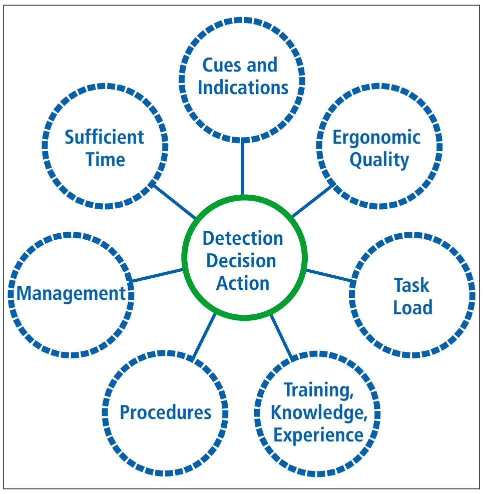


RISK AND HUMAN RELIABILITY– treating the human factor in probabilistic safety analysis

Human performance is essential to the safe and reliable operation of complex systems. The assessment of system safety must address the human element, considering how it may contribute to safety as well as risk. The expertise of the Risk and Human Reliability Group is centered on the methods for doing so, referred to as Human Reliability Analysis (HRA), and more generally on Probabilistic Safety Assessment (PSA). The overall aim of our work is increased system safety in nuclear power plants, by performing safety assessments and through the development of analysis methods. The assessment of safety for facilities outside the nuclear domain, requiring novel uses of PSA methods, is a natural extension of this activity.

The Risk and Human Reliability Group is one of the three groups of the Laboratory for Energy Systems Analysis (LEA). The core of its activities is Human Reliability Analysis (HRA), the part of Probabilistic Safety Assessment (PSA) that addresses the human factor and its role in system safety. In HRA, qualitative analyses of task requirements, the scenario context, and the performance conditions provide the basis for estimating the probabilities of the human-related events that contribute to accident scenarios.

The main research topics related to HRA are inappropriate actions, also known as errors of commission, HRA data, and simulation-based dynamic tools for HRA and PSA. These HRA activities are complemented by the application of PSA methods to assess system safety. Here, the emphasis is on novel applications that typically require adaptations of PSA methodology. The main project in this area addresses PSI's Proton Therapy Facilities (PROSCAN); PSA methods are applied to ensure the safety of patients.



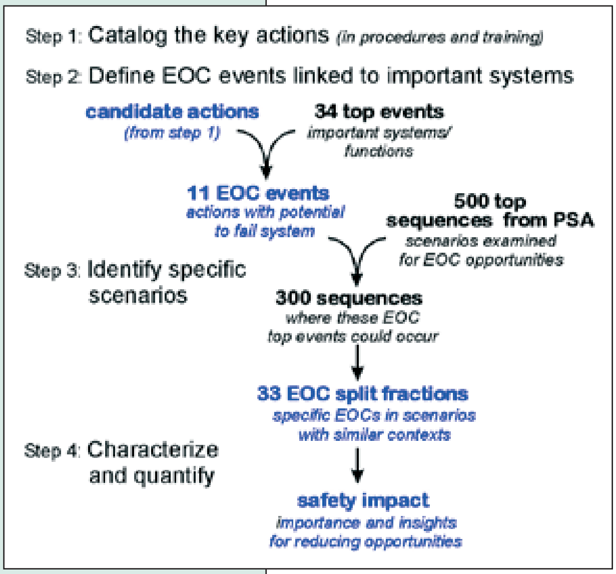
In HRA, the broad range of factors that affect human performance are examined.

Human Reliability Analysis (HRA)

The safety of complex, human-technical installations is based on combining reliable hardware, automatic and computer-controlled systems, and human performance. The role of HRA methods is to identify the personnel actions critical for safety, to analyze the performance conditions and the scenario context that influence performance, and to estimate the probabilities of the human-related failure events in the modeled accident scenarios.

Today PSAs principally address the omission of actions that are required to bring a facility to a safe state or to mitigate the consequences of an accident. An important issue is to understand the risk associated with inappropriate actions or errors of commission (EOCs). What are some actions that must not be done? Are there scenarios with cues that could suggest inappropriate actions? How likely are these scenarios?

The number of potential inappropriate actions is very large in contrast to required actions. The Commission Errors Search and Assessment (CESA) method, developed for the identification of EOCs, narrows the search by prioritizing actions on key systems and functions and examining the conditions under which they could erroneously appear to be appropriate.


Step 1: Catalog the key actions (in procedures and training)
Step 2: Define EOC events linked to important systems
candidate actions
(from step 1)
34 top events
important systems/ functions
11 EOC events
actions with potential to fail system
500 top sequences from PSA
scenarios examined for EOC opportunities
Step 3: Identify specific scenarios
300 sequences
where these EOC top events could occur
33 EOC split fractions
specific EOCs in scenarios with similar contexts
Step 4: Characterize and quantify
safety impact
importance and insights for reducing opportunities

The CESA method limits the search space by prioritizing EOCs associated with important systems.

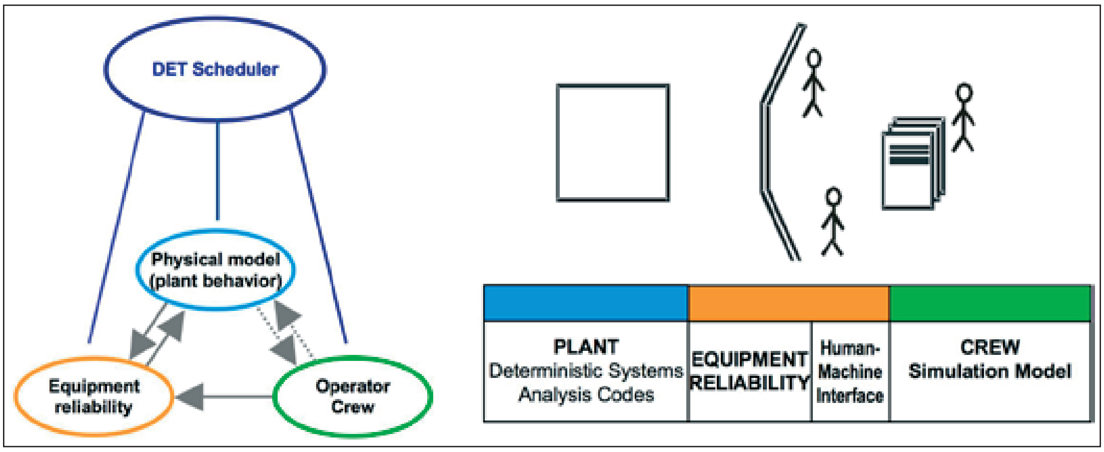
Ref.: Reer et al., Rel. Eng. Sys. Safety 83(2) 187-205(2004).

To determine the risk significance of human failure events and EOC situations, failure probabilities are needed. The CESA-Q (for quantification) is being developed as a foundation for the estimation of the failure probabilities associated with decision-making, typically an important element of EOCs.

Dynamic PSA and Operator Modeling

A comprehensive understanding of how situations present themselves to the operators is an essential input for HRA analysis. These performance conditions make up the context for the personnel's actions; at the same time, this context is changed by these actions. Consequently, characterizing these conditions requires analyzing how plant behavior, the automatic control and safety systems, and the operators' response affect each other.

The aim of dynamic scenario and operator modeling is to help HRA and PSA analysts analyze these interactions by means of a joint simulation of the plant behavior, systems, and operators. A framework for building such simulations is the discrete dynamic event tree; it combines continuous simulation and stochastic (probabilistic or random) events.

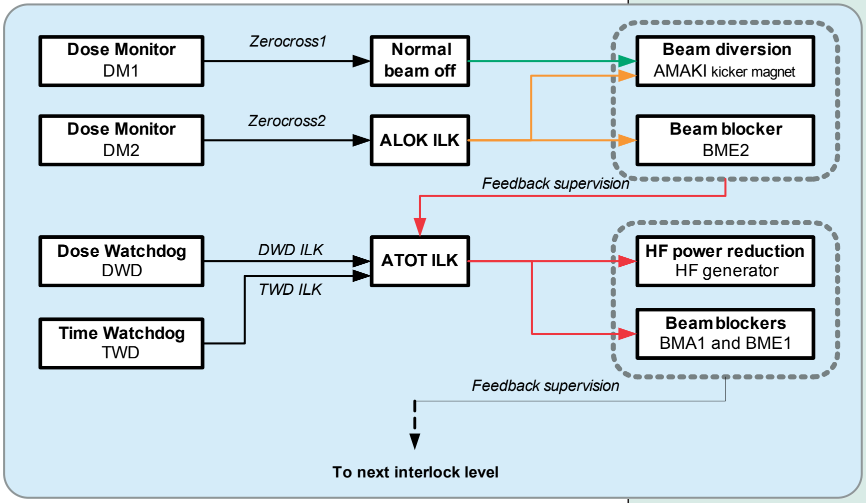


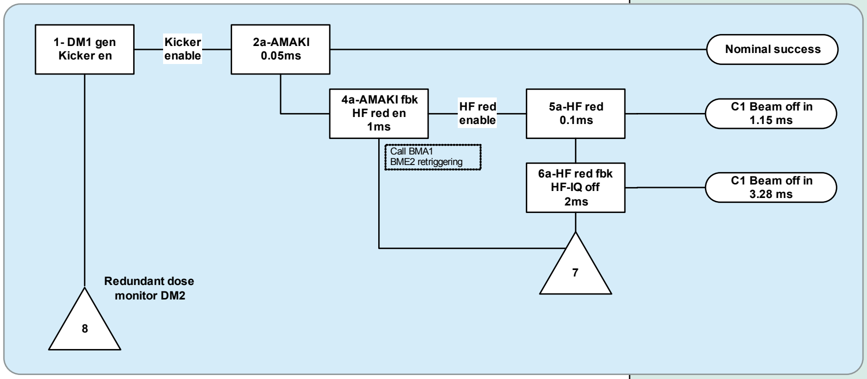
In dynamic, simulation-based safety assessment, the Dynamic Event Tree scheduler coordinates the interactions of the models.

Probabilistic Safety Assessment for PSI's Proton Therapy Facilities

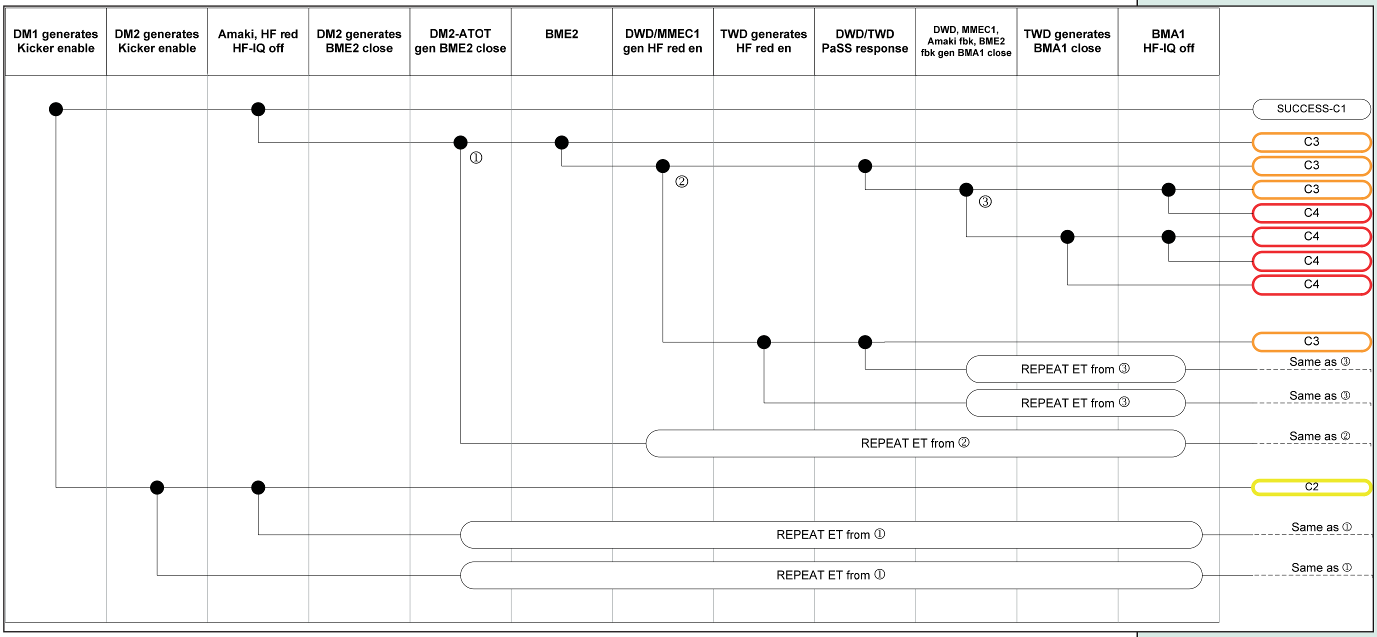
The application of PSA to PSI's Proton Therapy Facilities examines the systems' design and operation in terms of patient safety. The aim of these studies is to complement the facilities' safe operating record by assessing the residual risk and identifying possible measures to reduce the residual risk further. An earlier study of the Gantry 1 facility produced safety insights that were incorporated as upgrades, for instance, the diversification of checks for some components. An on-going study deals with the current configuration, with the dedicated medical accelerator, and work has been initiated for the upcoming Gantry 2, where advanced scanning techniques will be applied, and for multi-area facility operation.

In addition to the human factor, the role of software and electronics pose challenges for the analysis of PSI experimental facilities. In these risk assessments, PSA techniques comprise a systematic methodology to model the facility's safety design implemented with multiply redundant and diverse electronic and software systems.





Starting with a schematic of the safety logic (a), an event sequence diagram (b) shows the scenarios resulting from the failure of required functions. Next, an event tree (c) is based to represent the accident scenarios. Subsequently, fault trees are used to analyze the potential contributions to the failure of a function.



Services

Much of this research is supported by the regulatory research program of the Swiss Federal Nuclear Inspectorate (HSK). In addition, the group provides HRA-related technical support to the Inspectorate. It performs reviews of the licensee HRAs, assesses current developments, and provides recommendations on human performance and HRA-related issues.

Work for other organizations has included peer review of HRA research and applications of PSA to experimental facilities.

Joint Projects and Partners

International HRA Empirical Study – OECD Halden Reactor Project
An international evaluation of HRA methods based on comparing HRA analysis predictions with crew performance in simulated scenarios. Empirical study partners – US NRC, EPRI, EDF, IRSN, KAERI, VTT, and others.

Human Reliability Analysis Data Collection and Exchange – Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations, Working Group on Risk Assessment (CSNI WGRisk)
An initiative to develop and exchange human performance and reliability data based on simulator studies.

ADS Dynamic Event Tree software tool – University of Maryland, College Park
The Accident Dynamic Simulator (ADS) is a software for safety analysis based on dynamic event tree simulation.

Computational Intelligence for HRA and Risk Assessment – Polytechnic of Milan (Polimi)
Applications of fuzzy logic and Bayesian Belief Nets to analyze dynamic event tree scenarios and to support expert judgment.

Contacts
Risk and Human Reliability
Dr. Vinh N. Dang
Tel. +41 (0) 56 310 29 67
Fax +41 (0) 56 310 21 99
vinh.dang@psi.ch
http://safe.web.psi.ch/

Laboratory for Energy Systems Analysis
Dr. Stefan Hirschberg
Tel. +41 (0)56 310 29 56
Fax +41 (0)56 310 44 11
stefan.hirschberg@psi.ch
http://lea.web.psi.ch

PAUL SCHERRER INSTITUT
PSI

Paul Scherrer Institut, 5232 Villigen PSI, Switzerland
Tel. +41 (0)56 310 21 11, Fax +41 (0)56 310 21 99
www.psi.ch