

2

Elements of Human–Machine Systems

2.1 Human Factors Role in Modern Technology

In the last 30 years, technology has expanded enormously especially in scope and efficiency of the operations that can be performed by machines alone, exploiting their imbedded autonomous “decision-making” rules and mechanisms.

Similarly, roles and duties of human operators have undergone tremendous changes, and nowadays, operators are mainly supervisors and monitors of procedures carried out automatically, once these have been set up by the operators themselves (Sheridan, 1992, 1999). In such configurations of Human–Machine Systems (HMS), the design of automatic systems and the control of the interaction with human operators have become much more complex. In particular, the consequences of a “human error” or of a “misunderstanding” between human and automation can be unrecoverable and catastrophic (Nagel, 1988).

Two main factors have contributed to generating relevant concern and attention on the human factor role in safety: the *enormously improved reliability of hardware*, and the *extensive use of automation*. Advances in hardware technology have vastly reduced mechanical faults and enabled the management of plants, even in the presence of severe system faults and malfunctions. In this way, the contribution of human factors to safety analysis has been enhanced and “human error” has become the primary “cause” of most accidents in all technologically developed domains. It is nowadays very common to hear “human error” quoted as a possible or likely cause of accidents, by media and even by safety authorities, immediately after the occurrence of an accident. Unfortunately, this is only a shallow, and in many cases inappropriate, explanation of the real causes of an accident and is frequently utilised just for assigning responsibility and blame, rather than finding explanation and remedies. In some unfortunate cases, human errors of front line operators are abusively indicated as primary causes by certain managers in order to protect themselves and cover their own faults and responsibilities.

Considering the role of automation, it is widely accepted that in normal conditions modern plants are easier to operate than their predecessors. Human-centred design principles are utilised by manufacturers to varying degrees of accuracy when designing control systems and interfaces. These principles aim at maintain-

ing a central role for the operator in the management (supervisory) control loop, and require that operators are constantly “ahead” of a plant’s performance, controlling and supervising the automatic system in all its functions and procedures (Norman and Draper, 1986; Billings, 1997). However, designers do not always respect this essential requirement. Systems behave and respond via the automation and follow the rules and principles provided by their designers. These are not always totally known or familiar to front line operators. Moreover, in abnormal or emergency conditions, the dynamic characteristics of the sequence of events add to the inherent complexity of the situation and further complicate the decision-making process. If the expected response does not occur, a mismatch arises between the operator’s understanding of the dynamic evolution (situation awareness) and the automatic system. Thus, working environments are much more demanding in terms of cognitive and reasoning abilities than simple sensory-motor skills (Rankin and Krichbaum, 1998; Hollnagel, 1993; Ralli, 1993).

In such scenarios, and aiming to offer valuable and consolidated ways to improve safety and control of HMSs, the role and interplay of humans and automation is vital and needs careful consideration. This discussion leads to two main considerations. On one side, while automation is necessary, as it supports human tasks performance and can successfully replace human activity, it should also be developed with consideration for the consequences of inappropriate reasoning or misunderstandings on the part of the operators. This is particularly important when an operator’s knowledge and beliefs are deeply rooted in the social, organisational and technical context, usually called sociotechnical working context, in which they are born and developed. These inappropriate reasoning or misunderstandings are very difficult to trace and eliminate. On the other side, the occurrence of “human error” is an intrinsic characteristic of the management of any system, and it is impossible to conceive a plant that is totally “human error” free.

Consequently, the improvement of safety of a system cannot be achieved by tackling any actual inappropriate performance that has occurred or may have happened during an accident, but rather by understanding:

1. “why” operators took certain steps, and “what” are the root causes that may have generated, or may trigger in the future, inappropriate human behaviours;
2. “what” forms of inappropriate behaviour was produced, or could result, from such socio-technical root causes; and
3. “how” can systems be developed and humans be trained in order to:
 - (a) anticipate and prevent accidents and incidents initiators;
 - (b) manage accidents that still occur, and possibly recover normality; and
 - (c) limit or protect other humans and environment from accident consequences, when prevention and recovery did not happen.

In addition, the possibility for systemic and component failures remains, and it would be unwise and unacceptable to consider technical systems fully failure free and focus only on human errors.

This is why, in order to ensure safety and efficiency of modern technological systems, a much wider process of evaluation and study of human-machine inter-

action has to be developed, rather than simply tackling human inappropriate performances. Such a type of approach may be called *Human Error and Accident Management* (HEAM), and it involves the thorough development of measures at human machine system level for (a) *prevention* of conditions that favour and lead to system failures and/or human errors; (b) *recovery* of a plants' normal or safe performance, once a failure/error could not be anticipated and avoided, and an accident/incident has started; and (c) *containment* of the consequences and protection of the human beings and environment, in the case that neither prevention nor recovery succeed.

These fundamental goals of HEAM can be achieved and maintained at different stages of the development and implementation of a technical system, namely at design level, as well as during its lifetime. In this way, it is possible to grant continuous improvement of normal operations and emergency management in complete safety at all times. In particular, the consideration and analysis of human error and accident management must influence the following four areas of development and application of HMSs:

- *design* of human machine interactions and interfaces;
- *training* of operators and main actors for managing nontechnical risky states;
- *safety assessment* of systems and organisations; and
- *accident/incident investigation*.

Improving the design of Human–Machine Systems implies ameliorating the design process in order to ascertain that the basic principles of human-centred automation are respected. Improving *training*, in nontechnical issues, intends to increase the ability of operators to capture, notice, and deal with those factors and indicators of the context that favour the occurrence of errors or mismatches between human situational awareness and automation performance. Implementing accurate *safety assessments* of systems and organisations, at the design stage as well as at periodic intervals during the lifetime of a plant/system, represents the most complete method for ascertaining and maintaining high levels of safety within an organisation. Safety assessments make it possible to identify and discover at an early stage the relaxation of certain expected and critical safety measures, as well as the appearance of new factors that may favour the occurrence of accidents. Finally, *accident/incident investigation* should focus nowadays on methods by which it is possible to trace, in addition to the human erroneous performances, primarily the root causes of accidents that are deeply imbedded in the socio-technical contexts and specific working environments. Only with such a spectrum of approaches is it possible to achieve safe and efficient management of a complex human–machine system.

In this scenario, it is quite obvious that the design and the assessment of safe and effective systems and technological assets is no longer the sole responsibility of engineers, but implies the consideration of different perspectives and the contribution of a variety of specialists, especially from the human-related sciences. In particular, several disciplines must collaborate synergistically to reach such objectives, and this implies combining engineering know-how, psychology, and sociology principles, fundamentals of information technology, practical

skill in normal and emergency operations, and acquaintance with real system behaviour.

This chapter is structured around two main correlated topics: (1) elements of HEAM; (2) areas and types of application of HEAM. Firstly, the elements of complex technologies will be analysed, and a number of basic definitions for representing human-machine interaction will be developed. Particular attention will be dedicated to the concepts of human error and to the wider context of accident management. Then the two possible types of application of error and accident management studies will be considered. These are retrospective and prospective analyses. The need to preserve and ensure consistency between them will be discussed in detail.

The variety of areas of application of HEAM will then be considered. The correlation between *types of application* and *areas of application* will be dealt with in order to show which types of applications are necessary for different areas of application in order to develop consistent HMS analyses.

Finally, a methodology that can be applied in practice in different areas of application and merges the two basic types of application will be developed. This methodology is called Human Error Risk Management in Engineering Systems (HERMES) and represents a reference architecture that will be utilised throughout this book for discussing real applications of HEAM analyses.

The variety of methods, approaches, and techniques that can be applied for HEAM analyses will be described in the next chapter of the book.

2.2 Elements of Human-Machine Interaction

2.2.1 Definition of Human Factors

All complex technological systems, such as aircrafts, air traffic control rooms, chemical and energy production plants, and the like, operate in risky environments and share a number of characteristic elements, which affect their control processes (Maurino et al., 1995). In particular, the study of such systems from a human perspective implies the consideration for what is generally called the “human factor.” Moreover, all HMS can be formally analysed by approaches similar to each other for what concerns the architecture and theoretical frame adopted to describe the Human-Machine Interaction (HMI).

As this chapter refers to the elements that govern human-machine interaction, it is important to define the concept of Human Factors (HF), which embraces all the subjects discussed in this book.

Human factors may be defined as the technology concerned with the analysis and optimisation of the relationship between people and their activities, by the integration of human sciences and engineering in systematic applications, in consideration for cognitive aspects and socio-technical working contexts.

By this definition, Human Factors extends the concept of ergonomics, as the science of humans at work, beyond the workplace and behavioural performance to the cognitive and social aspects involved in human activity (Edwards, 1988).

Human Factors is conceived here as a “technology,” emphasising its practical nature rather than its disciplinary character. In this sense, the difference between human factors and human sciences is the same that exists between engineering and physics. Physics and human sciences look at the basic principles and fundamental criteria that govern their locus of interest, while engineering and human factors concentrate on the implementation in the real world and working environment of these principles and criteria. This distinction is particularly important, as it is recursively called upon for distinguishing different subject matter, especially when one looks at HMI issues from a merely theoretical or a more applied perspective.

2.2.2 Human–Machine Systems

Human–machine interactions and processes always occur in realistic contexts. They are characterised by the plant or machine under control, in direct contact with the operator, and by the socio-technical working context, in which the interactions take place (Figure 2.1).

The plant interacts with the human operator through its *interfaces* and *controls*. They may be defined as follows:

- *Interfaces* are display panels, indicators, decision support tools. They transform the behaviour of the machine in visual, auditory and tactile information. These support the operator in perceiving and understanding the state and dynamic evolution of the system and in developing the strategies for its management and control.
- *Controls* are means by which it is possible to operate on the system and automation in order to implement the operator’s intention and strategy. Interventions of controls are transformed in machine information by actuators.

The socio-technical working conditions, also called *context* and *environment*, comprise of the following:

- the actual environment in which operations take place, including noise, space, light, temperature, etc.;
- other operators, cooperating directly, or collaborating at a distance, with the decision maker; and
- the social context, represented by management policies, company rules, society, and cultural climate.

The plant interfaces and socio-technical working context are the main sources of *stimuli* for the operator. They affect the operator’s allocation of resources and his or her knowledge base. They may modify the unfolding of the reasoning and cognitive processes as well as the performance of manual or control actions by, for example, causing errors or inappropriate behaviour. The loop of human machine

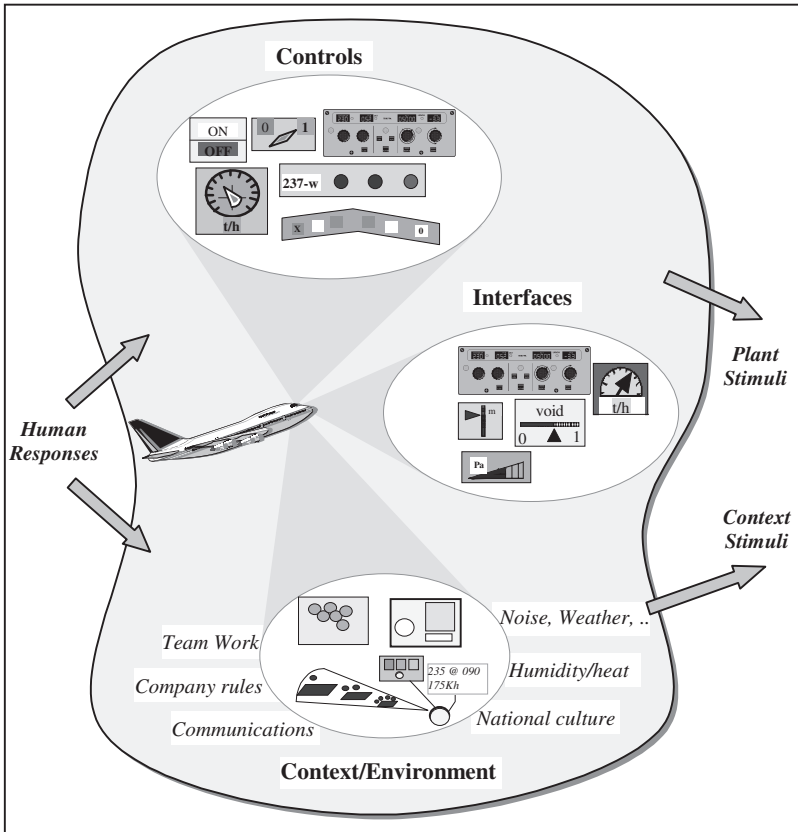


Figure 2.1 Structure of a human-machine interaction system.

interaction is then closed by the *human responses* that maintain the dynamic evolution of the interaction and generate new control actions, etc.

This structure captures and describes what may be defined as an HMS. A number of comprehensive definitions of a human-machine interaction system, or human machine system, have been proposed, as the notion of the combined human-machine element has changed over time and has become crucial for the development of all systematic safety theories. A quite complete definition of HMS can be found in the document MIL-STD-882B (DoD, 1984):

A human-machine system (HMS) can be defined as a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

This definition is deemed very appropriate, as it embraces the effects of socio-technical environment discussed above. Moreover, it looks explicitly at crucial aspects derived from the use of modern computer technology for the control and

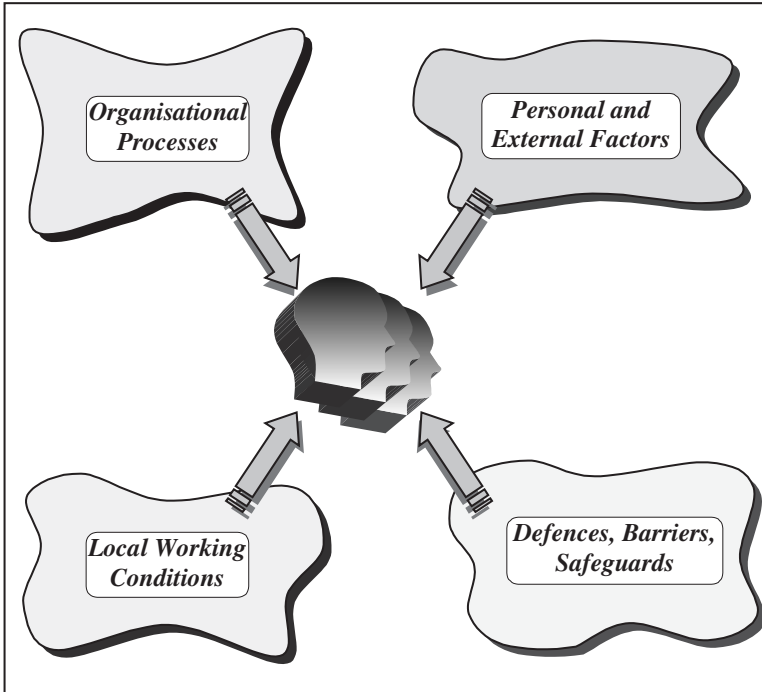


Figure 2.2 Socio-technical elements of a human–machine system.

management of plants and machines, in normal operations and emergency or transient conditions.

However, usually the terminology “system” is associated simply with the whole plant or with hardware and software components of a plant, and, thus, it represents a synonym of “machine.” In the definition of HMS adopted above, the terminology “system” is used in a much wider sense, which includes also humans, context, and environment.

2.2.3 Sociotechnical Elements of a Human–Machine System

Four main socio-technical elements influence a human–machine system and intervene in all dynamic processes characterised by human–machine interactions. These four elements are: (a) *organisational processes*, (b) *personal and external factors*, (c) *local working conditions* and (d) *defences, barriers and safeguards* (Figure 2.2).

Organisational Processes

It is now well accepted that strategic decisions have deep consequences for the way in which a system is managed. Cultural traits are the root cause of corporate

behaviour and the origin of organisational culture, which pervades all decision processes. Organisation culture is an important factor to be considered in assessing and designing the way in which certain technology is or should be managed.

A broad definition of organisation culture can be taken as (Mitroff et al., 1990):

The culture of an organisation may be defined as the set of rarely articulated, largely unconscious beliefs, values, norms, and fundamental assumptions that the organisation makes about itself, the nature of people in general and its environment. In effect, the culture is the set of “unwritten rules” that govern “acceptable behaviour” within and outside the organisation.

Organisational and cultural traits are then important factors, also called “resident pathogens” (Reason, 1990), able to play a very relevant role, affecting the safety of a system. They have to be identified and detected early, so as to ensure correct understanding of people’s behaviour and grant prompt and effective intervention when these factors combine with some system failures to generate dangerous situations.

Personal and External Factors

Personal traits and external factors are amongst the most important determinants of human behaviour. Personal traits are, by their very nature, very hard to consider and prevent, as they are linked to individual characteristics and are therefore impossible to generalise in stereotype constituents.

External factors are determined by contextual random events. Consequently, they are equally difficult to formalise and generalise, as they are directly related to human or systemic behaviours in specific environments.

However, these factors must be defined and considered in a methodological framework for the study of HMSs. They can only be approximately and imprecisely formalised by means of statistical algorithms able to capture their random nature.

The definitions of external and personal factors are proposed as follows:

External factors can be considered as all random physical or system contingencies that may alter or impinge on local working conditions and safety measures, so as to foster inadequate system performance and erroneous human behaviour.

Personal factors are individual, physical, or mental conditions that affect human behaviour, and are specific to each person. They can only be accounted for by a random variable affecting the generic behaviour of large classes or categories of people.

Personal and external factors should be considered as random variables in an overall framework of accident causal path, and their role can only be marginal in a structured analysis of an *organisation*. Their presence is anyhow considered and recognised by such random quantities.

In accident analysis, their contribution to event development and root causes is crucial in many cases, and the identification of their role needs adhoc assessment and evaluation.

Local Working Conditions

Local working conditions are “expressions” of physical and social contexts, including higher-level organisational and cultural traits. These are transmitted along various pathways of the *organisation*. They are probably the most relevant factors affecting the behaviour of front line operators, as well as people involved in decision making, as they are immediately and promptly related to the environment and dynamic evolution of the human–machine system.

The definition of local working conditions can be adapted from Maurino et al. (1995) as:

Local working conditions are the specific factors that influence the efficiency and reliability of human performance in a particular work context.

Local working conditions affect the performance of tasks by influencing either the interface between operators and control systems and/or cognitive activities. Examples of local working conditions are: workplace design, interfaces with automation, tools and instruments, protective equipment, job planning, procedures, supervision processes, workload, training, and policies.

Defences, Barriers, and Safeguards

Defences, Barriers, and Safeguards (DBS) are all structures and components, either physical or social, that are designed, programmed, and inserted in the human–machine system with the aim of making more efficient and safe the management of a plant, in normal and emergency conditions.

In general, the following definition can be adopted:

Defences, barriers, and safeguards are the measures developed by the organisation aimed at creating awareness, warning, protection, recovery, containment, and escape from hazards and accidents.

DBS are then a direct result of a high-level organisational process which includes planning, design of automation and emergency systems, definition of policies on training and procedures, and the like (Reason, 1997; Hollnagel, 1999; Polet et al., 2002). They fulfil a series of functions, namely:

- to create awareness and understanding of the hazards;
- to support the detection process of off-normal conditions;
- to support restoring normal operating conditions;
- to protect from injury;
- to contain the consequences of an event;
- to support escape in the case of loss of control or accident.

In order to offer here a formal distinction between different types and modes of DBS, the classification proposed by Hollnagel (1999) can be proposed as an example of guidelines for a safety analyst. According to this classification, DBS can be grouped into four main types:

1. *Material Barriers*. These types of DBS prevent the performance of dangerous actions or contain consequences of occurrences by physical constraints. Examples of *material* DBSs are doors, railings, fences, safety belts, filters, etc. These barriers aim at attaining their goals by simply being located in strategically relevant positions or by reacting to physical and environmental conditions.
2. *Functional Barriers*. These barriers require that a certain function occurs or that certain variables reach or are assigned predefined values to become active. In other words, a certain *function* has to be satisfied or fulfilled in order to make the barrier either effective or ineffective, depending on its purpose. Examples of *functional* DBS are air-locks, dead-man-buttons, passwords, safety codes, delays, etc.
3. *Symbolic Barriers*. These DBS are associated with a certain logic or conventional rule or habit that indicate the presence of a dangerous or safety relevant condition. In other words, *symbolic* DBS require knowledge of certain rules and regulations, or habits, and their interpretation in order to be effective. *Symbolic* DBS may not be respected or may be bypassed by users. Examples of *symbolic* DBSs are safety code sequences, instructions and procedures, signs, signals and warnings, clearances, joborders, etc.
4. *Immaterial Barriers*. These DBS are the most highly located barriers in a cognitive sense. They demand explicit interpretation by the user, as they are known but only in general form and are not present in any of the other DBS forms, i.e., symbolic, functional, or material. In general, these are the result of cultures, philosophies, or policies which develop within an organisation and are very difficult to modify or adapt to new situations and contexts. Examples of *immaterial* DBS are laws, general rules, standards, etc.

The differences that exist between these four categories are useful for supporting analysts or designers in developing DBS at different levels of depth. They are not totally independent from each other. However, the existence of certain overlapping amongst them does not affect the overall understanding and support that such classification may offer in the process of design and validation of a safety system.

2.3 Human Error and Error Management

The previous sections have considered the building blocks of organisations from a socio-technical perspective. These factors represent the underlying conditions that foster the generation of human inappropriate behaviour and human errors. While many psychologists have discussed the fundamental nature of human error in detail (Norman, 1981; Reason 1986, 1987, 1990, 1997; Reason and Mycielska, 1982; Rouse and Rouse, 1983; Rasmussen, et al., 1987; Senders and Moray, 1991), the human factors perspective adopted in this book shifts the focus of attention on the effects of errors in a technological environment.

2.3.1 Human Error in an Organisational Perspective

Definition of Human Error

A definition and classification of Human Error (HE) which can be considered “classical” has been given by Reason (1990), and may be summarised as follows:

Human error may be defined as the failure of planned actions to achieve their desired ends without the intervention of some unforeseeable event.

This failure can occur either when the plan is adequate but the actions deviate from the plan (*slips, lapses*), or when the actions conform to the plan but the plan is inadequate for achieving the desired ends (*mistakes*).

Slips are associated with attentional or perceptual failures and result in observable inappropriate actions. Lapses are more cognitive events and usually involve memory failures. Mistakes are errors made at a high cognitive level, involving processes linked to the available information, planning, judging, and formulating intentions.

Another type of error is considered in Reason’s classification: *violations*.

Violations are deviations from safe operating practices, procedures, standards, or rules. Most violations are deliberate actions, even if sometimes they can be erroneous.

Errors defined in the Reason’s theoretical framework, independently of their type, can take different modes according to the person that makes them and the role that this person occupies in the organisation. Errors made by front line operators and primary actors, in the control process of a system, emerge immediately and become very visible in the evolution of an event. These are called *active errors* and are the most obvious occurrences and the most rapidly identified human contributors in an accident.

Errors made at higher levels of the organisations, such as in the definition of policies or emergency procedures, or in remote and distant working systems such as at the maintenance level, are more complicated and difficult to spot at first sight. These errors lie inactive in the system and do not show their negative effects until specific conditions are encountered.

The higher the level of the organisation at which these errors are made, the more serious are the consequences at the front line operation. Indeed, errors of strategic nature, such as when defining company philosophies or policies, affect safety attitudes and the culture of operators and managers, creating working conditions that foster violations and inappropriate or careless performances.

These errors are defined as *latent errors* and are the most dangerous and serious errors to be tackled.

Types and Modes of Human Error

Types of Human Error

The definitions of human error discussed in the previous section concentrate on the types of inappropriate behaviour that can be identified primarily in an organisational perspective, as they identify generic manifestations of behaviour.

In this sense, *slips*, *lapses*, *mistakes*, and *violations* concern the individual behaviour, while *active* and *latent* errors are representative of the organisational perspectives in which individual behaviours are framed.

Other *types* of errors can be defined, for example, focusing on the specific performance of individual persons. In particular, a simple structuring of error types in errors of *omission* and *commission* allows the classification of a wide variety of inappropriate behaviours (Swain and Guttman, 1983). Errors of omissions are, as the definition says, simple omission actions or steps in the performance of a procedure or a well-known process. Errors of commission are all the remaining possible manifestations of inappropriate behaviour that imply the actual performance of an inappropriate action.

Modes of Human Error

When studying human-machine systems, a concrete representation of actual inappropriate behaviours is necessary.

Error types can be complemented by the identification of the forms taken by inappropriate behaviours. These can be classified as error *modes* and are associated with error types in classifying and representing the behaviour of humans interacting with machines.

Examples of modes of errors are the actual amount of delays in performing certain actions, or the inadequate amount of force applied in performing a certain operation, etc.

In practice, when classifying human errors in an accident analysis, or when considering errors in safety studies, it is necessary to:

- frame inappropriate behaviours in the socio-technical environment in which they are made (*error types*); and
- define the actual forms that errors take when performing a certain action (*error modes*).

This representation of errors allows the complete consideration of errors in any type of study or analysis.

2.3.2 Human Error in Safety Practices

These concepts of human errors are nowadays accepted by designers and analysts of many organisations and technologically advanced systems. As a consequence, error management tools are implemented in practice.

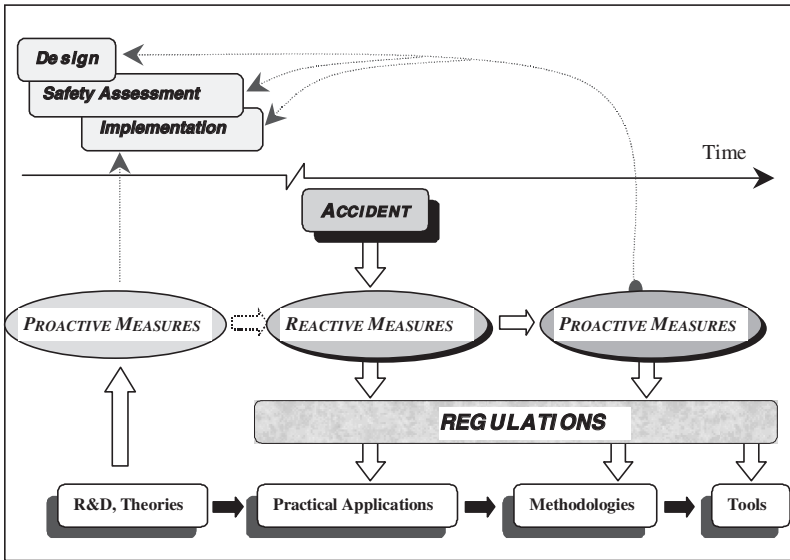


Figure 2.3 Proactive–reactive measures for safety management and accident prevention.

However, in many cases they still present crucial limitations. They are implemented as “piecemeal” rather than planned interventions; they are developed as “reactive rather than proactive” measures, i.e., they result from “event-driven” rather than “principle-driven” considerations (Reason, 1997, p. 126).

Consequently, certain types of safety and error management measures suffer major drawbacks for three main reasons:

- They consider errors as causes rather than consequences of accidents.
- They focus on people rather than situations.
- They rely on punishment and blame rather than improving safety culture and attitudes.

Human errors that are immediately visible in the case of accidents are simply manifestations of inappropriate behaviour. They require an explanation as much as the accident that is related to them. It is necessary to understand the context in which errors have occurred, the socio-technical and organisational environment and, sometimes, also the personal factors that have fostered them. Finally, the results obtained by the “blame, exhortation, and disciplinary” sanctions are small when compared with the development of a (safety) culture through personal conviction.

In practice, the application of a safety method and the development of measures, including approaches for error reduction and containment of consequences, usually follow an evolutionary process (Figure 2.3). Safety methods are originally generated at the research and development (R&D) level, as proactive measures for improving safety. However, they have a limited impact on design, safety assessment, and implementation, and they are rarely immediately transformed into practically applicable tools. Only later, during system operation and lifetime, and

following the occurrence of a severe accident, (reactive) measures are developed, as a reaction aimed at avoiding the repetition of the causes and circumstances of that specific accident. These are then further expanded into sound methods and are introduced as (proactive) mandatory measures by safety and regulatory authorities, with the precise aim of accident prevention and limitation (Cacciabue and Pedrali, 1997; Cacciabue, 1999).

2.3.3 An Expanded View on Human Errors

The definitions of human error discussed in previous sections, and the various types of errors that derived from them, fit very well the socio-technical elements of a human-machine system. They encompass the logical and strict connections between manifestations of erroneous performances and organisational and environmental factors that may be at their origin.

In many cases, however, certain behaviours, which are later identified as erroneous or inappropriate, are completely reasonable, unavoidable or even necessary, given the contextual conditions and the operator's appraisal of the situation ("situational awareness") at the time of their occurrence.

Therefore, studying safety and simply discussing in terms of human errors is not an effective way forward, while it is much more important to understand and analyse the overall human-machine conditions and the context in which accidents and human behaviour develop. Moreover, it is obvious that it is impossible to eliminate all errors or inappropriate behaviours that may occur during the management of a plant, especially in those cases where certain decisions and choices are made as a consequence of special contextual conditions. Therefore, it is equally important to accept that "errors" occur and to also consider and develop, in addition to preventive measures, adequate means for ensuring prompt errors recognition and recovery or even protection for humans and environment in case of accidents.

Following this line of thought, we will frame the human contribution to accident causal paths in a perspective that considers the "human error" not as the cause but as the consequence of other factors that reside at different levels of the organisation, as well as in the contextual and dynamic circumstances of the specific occurrence. These are the important causal elements, or root causes, that need to be identified and removed from the system, or at least minimised, in order to prevent their occurrence and their negative effects or to ensure their effective control and recovery or, eventually, protection in the case of an accident.

The safety of any system depends indeed on a combination of technical and social factors, which are deeply correlated and cannot be separated and dealt with independently from one another. They must be tackled by appropriate methodologies of human-machine interaction and human-machine system for the identification of "*safety critical factors*" and "*safety levels*" that enable evaluation of the safety state of a system and its "distance" from dangerous or unsafe conditions.

Any system, starting from its design stage and then, following its practical implementation and during its entire operating life, detains and attains different safety levels and develops a variety of new safety-critical factors. The safety of a system depends on these factors and levels. They must be determined and evaluated at the design stage, as well as during the life of the system, for ascertaining its operability and possibly discovering the need for improvements and/or new safety measures.

In practice, it is necessary to accept that human errors occur and cannot be totally prevented or eliminated. Consequently, the way to improve the safety levels of complex systems concentrates on three different means of intervention: (1) by *prevention* of risky or inappropriate circumstances; (2) by offering adequate ways of *recovery*, when prevention has not been possible; and (3) by *containment* and limitation of consequences, when neither prevention or recovery has been successful. To ensure maximum safety it is necessary to define or identify indicators or safety critical factors. These allow to “measure” the level of safety attained by a system at any time of its life and to “confront” these indicators with acceptable values, possibly for all three types of means of intervention.

This implies developing adequate human–machine interaction management, or human error and accident management, approaches within an organisation.

2.4 Human Error and Accident Management

Given the above discussion, the definition of Human Error and Accident Management (HEAM) that is adopted is as follows:

Human error and accident management is the variety of methods and measures designed to reduce inappropriate and risky human–machine interactions at different stages of a system lifetime, by offering means and ways to recognise and prevent them, to control and recover from those that still occur, and to contain and escape their adverse consequences, when full recovery is not possible.

The clear understanding of the above definition and of the goals of HEAM is the *first fundamental standpoint* in the development of human–machine systems and effective safety measures.

The definition of HEAM is strictly coupled with the definition, developed in the previous section, of “human error” as inappropriate performance/behaviour, dependent on the context and dynamic contingencies and imbedded in a specific socio-technical environment. This definition of “human error” is integrated in a more general representation of HMI and modelling of human behaviour, which embraces all types of interactions, either adequate or inappropriate.

The understanding of the concept of human error in terms of a human–machine interaction process and the adoption of a model of HMS that considers humans and machines at the same level, in a sort of a “joint cognitive system,” represents the *second fundamental standpoint* in the development of effective HMS and HEAM measures.

The objective of this book lies precisely in the structuring and in offering guidance to the application of methods for developing and implementing HEAM means and measures that can be proactively implemented within an organisation, to minimise the occurrence and to control human-machine related accidents.

2.4.1 Types of Analysis for HEAM

Prospective and Retrospective Analyses

Human error and accident management should be conceived as a set of proactive measures that improve the safety standards of an organisation. Proactive measures may be developed on the basis of creative thinking and safety-oriented attitudes of analysts who are able to imagine safety-critical scenarios and study appropriate ways and measures to prevent their occurrence, recovery normal system functions when they still happen, and protect humans and environment in case of accident. These analyses are performed with a prospective view of what may happen during an abnormal situation.

At the same time, proactive measures must be associated to the real socio-technical contexts in which they are applied. They require, therefore, a thorough assessment of the *local working conditions*, and *organisational processes*, including their dynamic and evolutionary aspects, and their history, in terms of past incidents and accidents that have involved failures of *defences, barriers, and safeguards* and *personal and external factors*. The studies of these socio-technical elements of HMS are basically retrospective analyses by which it is possible to learn the lesson from past experience and to understand the actual working conditions in which HMI takes place.

There are, therefore, two major types of analyses that support the development of HMS and HEAM measures, namely, *retrospective* and *prospective analyses*. They are complementary to each other, and contribute equally to design and safety assessment processes.

In a wider context of human-machine interaction studies, prospective and retrospective types of analyses can be defined as follows:

Retrospective analyses consist of the assessment of events involving human-machine interaction, such as accidents, incidents, or “near-misses,” with the objective of a detailed search for the fundamental reasons, facts, and causes (“root causes”) that fostered them.

Prospective analyses entail the prediction and evaluation of the consequences of human-machine interaction, given certain initiating events and boundary configurations of a system.

The clear understanding and consideration of the difference and synergy between prospective and retrospective analyses is the *third fundamental standpoint* in the development of effective HMS and HEAM measures. To make these concepts more clear a detailed discussion will now follow.

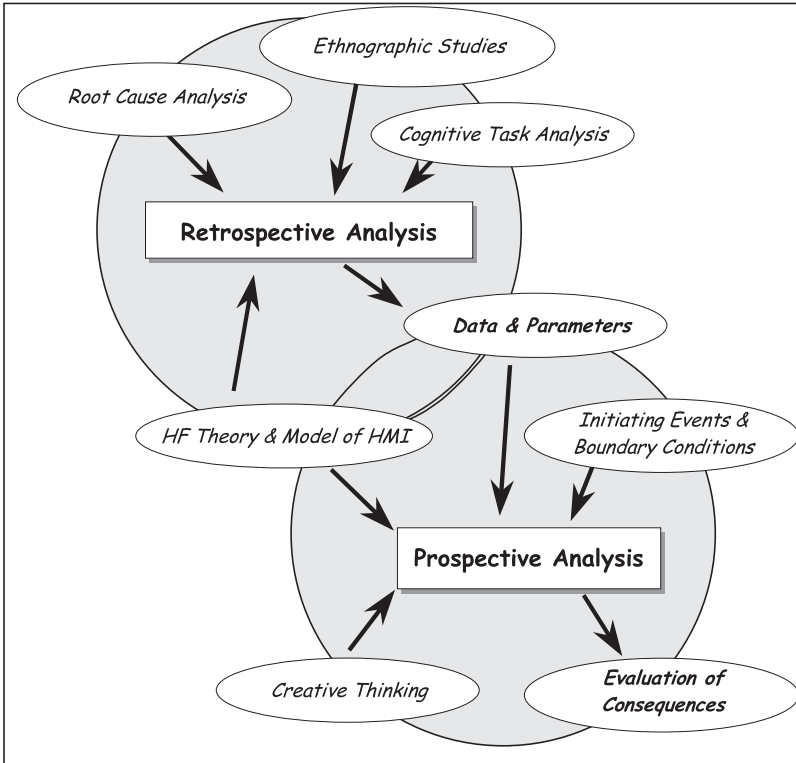


Figure 2.4 Prospective and retrospective analysis.

Retrospective Analyses

In practice, retrospective analyses are oriented to the identification of “data and parameters” associated with a specific occurrence and context.

They can be carried out by combining four types of methods and models that are extensively formalised and discussed in the literature, namely (Figure 2.4):

- root cause analysis;
- ethnographic studies;
- cognitive task analysis; and
- HF theories and models of HMI.

Human factors theories and models of HMI consider several reference paradigms that can be applied in studying a specific contextual environment. These are generic models and architectures of human–machine interaction that must be adapted to the specific context and system.

In order to select and apply the most appropriate HMI model, an analyst must primarily study objectives, formal plans, and procedures for operating processes. This

is done through the evaluation of tasks and goals assigned to operators for managing normal and emergency conditions, i.e., by task analysis. Given that cognitive and decision-making processes are nowadays more relevant than actual actions, the standard task analysis has been further developed in “cognitive task analysis” (CTA) that focuses on the cognitive rather than behavioural aspects of human activity.

In addition to the formal process of CTA, it is essential to analyse and evaluate the outcome of past events in terms of accidents/incidents and, especially, near misses with the objective of identifying the causes and reasons of specific behaviours and HMI in general. This is performed by Root Cause Analysis (RCA) methods.

Finally, in order to fully understand why and how events and interactions take place in a specific context, it is essential that the analysts become familiar with the working environment and practices of system management. This is a crucial process in the implementation of any formal method to a specific real case, and it is performed by field observation and assessment of working practices and habits, i.e., by ethnographic studies.

These four types of methods and approaches contribute and integrate their outcome for the identification of data and parameters that characterise a specific context. These data allow the performance of sound and realistic prospective studies and analyses.

The application of well-qualified and experimented models and techniques, and the performance and integration of the results of all steps in a retrospective study, represent two necessary processes to be performed almost normatively in order to obtain a clear picture of the existing context and socio-technical working environment, as well as consistent sets of data and parameters for predictive studies.

Prospective Analyses

Prospective analyses aim at the “evaluation of consequences” of HMI scenarios, given a selected spectrum of (Figure 2.4):

- HF theories and models of HMI,
- data and parameters,
- initiating events and boundary conditions, and
- creative thinking.

The HF theories and models of HMI that sustain prospective analysis must be the same as those applied for retrospective analysis. The same conditions apply with respect to the generality of paradigms and specificity of domains of application. The models selected for application need to be transformed into simulations that can be practically implemented in (computer) programs and adapted to specific contexts in order to perform previsions and estimates of the likely consequences of accidents or prediction of special situations that develop from certain initiating/boundary conditions and HMI.

The data and parameters that sustain such models and simulations, as well as their validity and applicability, are the outcome of retrospective studies and strictly depend on the accuracy of the (retrospective) analyses that produce them.

The initiating events and boundary conditions give the spectrum of situations that are analysed by the prospective study and are developed by the analyst on the basis of his/her experience, expertise, knowledge and, specifically, creative thinking.

The latter is a fundamental component of any speculative and perspective type of analysis and plays a clear role in the selection of models, variables, data, and all other elements that combine in a prospective study. Creative thinking is the necessary condition for the development a “human-centred” prospective analysis, which is an essential contribution to any type of study where novelty and imagination are governing components, aiming at anticipating and predicting possible HMS behaviours and HMI.

As for the case of retrospective analyses, the application of a prospective study must be structured and formalised in order to develop a consistent methodology that may be recursively and effectively applied. The reliability of a methodology for prospective analysis can be observed through the evaluation of the consequences of HMI. These are the ultimate outcome of a prospective safety study, and represent the values and quantities that allow an analyst to draw conclusions and evaluations about the safety state and safety level of a system.

Differences and Commonalities Between Prospective and Retrospective Analyses

The procedures for developing prospective and retrospective analysis bear certain commonalities, but also contain important differences. The differences consist in the basic objectives of the two approaches. In prospective studies the analyst must look ahead and speculate in a creative way. In retrospective assessments the focus lies in understanding and extracting the lesson from past events and occurrences.

The commonalities between the two approaches lie in human factors theories and human–machine interaction models and sets of data and parameters. The same basic HF theory must be considered for prospective and retrospective studies and, consequently, coherent human behaviour and error models must be applied. In this way, data and parameters derived from retrospective studies of real events and evaluation of working environment can be consistently and coherently applied for prospective analyses. These common elements should be well identified, as they represent logical links between the two approaches.

In other words, to make prospective and retrospective analyses consistent with each other, it is essential that identical, or at least coherent, HF theories and HMI models should be utilised for both types of analysis. In this way, data and parameters derived from retrospective studies may be applied in prospective assessments without having to make inferences and judgement, which introduce further and unnecessary uncertainties on the evaluation of consequences.

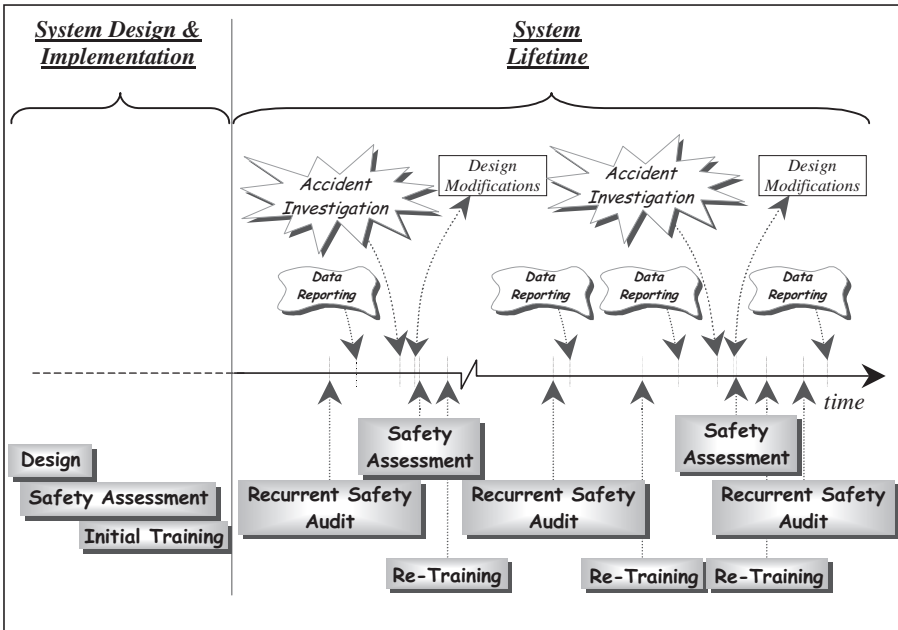


Figure 2.5 Safety evaluations during design, implementation, and lifetime of a system.

2.4.2 Areas of Application of HEAM

According to the definition of human error and accident management, the measures that ensure safety and prevent risky interactions within a human-machine system are considered and dealt with at different stages of the system lifetime (Figure 2.5).

This implies that before the actual implementation and installation of a system, i.e., during the *design* stage and *preliminary safety assessment*, the possible occurrence of incidents and human inappropriate behaviours have to be considered, and suitable defences, barriers, and safeguards must be devised in order to prevent them, control them, and minimize their consequences.

Similarly, the same conditions have to be considered for the development of *initial training* (before system installation) and *retraining* (during system lifetime), which should strengthen human perception and promote adequate reaction in the case of appearance of contextual conditions that may favour and generate inappropriate behaviours and possible incidents and accidents.

Moreover, during the operational life of a system, it becomes essential to learn the lesson that may be drawn from the occurrence of incidents, accidents, and near misses, as well as to be prepared to evaluate the dynamic evolution of the safety levels of the system. This implies that appropriate HEAM approaches have to be considered that favour *data reporting* and *collection*. These data support the *acci-*

Table 2.1 Application and basic requirements for HEAM

Area of application	Type of assessment
Design	<ul style="list-style-type: none">• Design of control, emergency, and protection systems• Design of human–machine interfaces• Development of standard and emergency operating procedures
Training	<ul style="list-style-type: none">• Classroom human factors training• Human factors training in simulators
Safety assessment	<ul style="list-style-type: none">• Human contribution to design basis accident• Human contribution to quantitative risk assessment• Evaluation of safety levels of an organisation by recurrent safety audits
Accident investigation	<ul style="list-style-type: none">• Human contribution to accident etiology and identification of root causes

dent investigation and *recurrent safety audits*, which consent to ascertain whether the conditions for safe and effective operations still exist, or some changes and improvements are needed in order to reestablish adequate levels of safety condition and operability.

In other words, HEAM approaches should be applied at four stages of the development and operation of a technological system, namely, *design*, *training*, *safety assessment*, and *accident investigation* (Table 2.1). The consideration of HEAM measures in these four areas of application requires recursive utilisation of appropriate methods for the evaluation of the safety level of an organisation in order to ensure the preservation of adequate safety levels throughout the lifetime of a plant or system.

Each of these four areas of application encompasses specific types of assessment. These will be briefly discussed in the following sections, while a complete analysis of specific tools and detailed procedures for application will be performed in the next chapter of this book.

The *fourth fundamental standpoint* in the development of effective HEAM measures lies in the appreciation that before and during the lifetime of a system a variety of tools and approaches must be applied for the continuous verification that adequate safety conditions exist and are maintained. These tools aim at sustaining and ensuring affective applications in the four areas of application of *design*, *training*, *safety assessment*, and *accident investigation*.

In performing safety evaluation of a system and in devising measures for prevention, recovery, and protection from accidents it is essential that adequate *indicators* and *markers* are identified that allow the measurement of the safety level of a system. Only generic indicators can be defined according to types of system. The definition of what *indicators* and *markers* are important and constitute valuable measures of safety for a specific system can be defined only by the individual organisations responsible for the management of the system, or family of systems. Therefore, a set of methods and approaches must be applied for the adaptation of

generic indicators and for the definition of appropriate safety levels for each specific plant.

The appreciation of the importance and role of *safety indicators* or *markers*, and their specific values associated to each plant, working context, and organisation, represents the *fifth fundamental standpoint* in the development of effective HMS and HEAM measures.

Design

At the design level, HEAM can be tackled by developing *control, emergency, and protection systems* that are effective and useful. These systems are always coupled to appropriate *procedures* and *interfaces* (Stokes and Wickens, 1988; Degani and Wiener, 1994a). Applying models and numerical simulations of human-machine interaction, different procedures and interfaces can be designed, compared, and tested for a large variety of initial and transitory conditions generated by plant malfunctions, emergencies, and normal operations. The study of procedures and interfaces, for diverse human behaviours, is a typical application of prospective HMI methods.

Training

Training human factors insight has nowadays become common practice for highly specialised operators, such as nuclear power plant operators, pilots, air traffic controllers, etc. This type of training is performed in addition to, and is complementary to, the more classical training of technical skill and plant control performance. Therefore, it is usually called human factors, or “nontechnical,” training, so as to distinguish it from the more classical formal training of ability to manage and control the plant from the physical and technical viewpoint.

In some cases, such as in civil and military aviation, regular and recurrent training procedures in human factors are already formalised by regulatory bodies and authorities and are integral part of the overall curriculum of expertise development. Two specific types of human factors training are considered: *classroom* and *simulator*. Classroom (human factors) training consists in introducing the concepts of human behaviour, human-human and human-machine interaction in very specialised discussions and lectures, as part of the standard and recurrent training (Wiener et al., 1993).

Simulator (human factors) training is carried out during practical, hands-on, sessions at a “full-scale replica” simulator. Operators are trained in these sessions with the objective to develop their “technical” skill in controlling and supervising the machine during abnormal conditions, but also to manage critical situations and exploit human competence and potentialities at their best, especially when working as a team.

In both these cases, i.e., classroom or simulator training, the instructor or facilitator must master different paradigms of human behaviour in order to be able to describe, review, and characterise different human performances.

Safety Assessment

A Safety Assessment study can be performed from three quite different perspectives: *Design Basis Accident (DBA)* analysis, *Quantitative Risk Assessment (QRA)*, also called Probabilistic Safety Assessment (PSA) or Probabilistic Risk Assessment (PRA), and *Recurrent Safety Audit (RSA)*.

Design Basis Accident

Design basis accident analyses consist in safety studies of specific accidents. The boundary and initial conditions are prespecified by the designer and are believed to represent the set of worse possible accidental scenarios, which encompass all other conceivable accident configurations.

Safety measures and protection devices are designed and dimensioned on the basis of the results of DBA studies, which imply the evaluation of all engineered safety devices, standards, procedures, and training, including human interactions and plant performances, in such worse possible conditions.

Quantitative Risk Assessment

Quantitative risk assessment methods evaluate the frequencies of occurrence, or probabilities, associated with certain accidents, in relation to predefined selections of initiating events. As basic methodologies for systematic safety analysis, they combine classes of erroneous behaviour and system reliability data, i.e., failure rates, in structured representations of events (Hollnagel, 1993; Parry, 1994; Cacciabue, 1997).

Quantitative risk assessment studies are essentially prospective types of analysis, as the analysts define hypothetical initiating events and failure/error probabilities and calculate the frequencies of a spectrum of consequences derived from different paths of accidents. In particular, the probabilities associated with human erroneous actions are needed to perform the evaluation of human interaction processes and to quantify success/failure of a performance of certain tasks or procedures.

The final objective of a QRA is the quantification of the risk associated with certain events and the evaluation of whether such risk falls within the limits set by regulations and standards. When this does not occur, new or more reliable safety measures must be considered in order to contain further the risk and improve safety.

Recurrent Safety Audits

The constitutive elements of complex technologies have been identified in the presence and interconnection of organisational and cultural traits; working conditions; defences, barriers; and safeguards; and personal and external factors. The assess-

ment of the safety level throughout a system and an organisation requires that these factors be evaluated at periodic intervals, i.e., recursively, in order to examine the state and possible evolution of the system/organisation towards different levels of safety/risk conditions.

These types of evaluations focus on data, critical system functions, and specific human-machine characteristics that require particular attention and need to be evaluated in relation to each specific system/organisation.

Recurrent Safety Audits (RSA) of organisations attempt to evaluate the safety state (level) of an organisation with respect to a variety of safety indicators and markers associated with the current state of the constitutive elements of a system, i.e., organisational and cultural traits, working conditions, personal and external factors, and, above all, defences, barriers, and safeguards.

The recurrent assessment of the safety level of an organisation requires a methodological framework where different methods and approaches are combined and integrated for considering HMI. RSA of organisations are critical and essential key processes for preserving systems integrity and for preventing and protecting from accidents.

The absence or a poor practice in the application of RSA has been recognised as a major deficiency in organisations that have experienced serious accidents, which, in some cases, have led to lethal consequences for an entire technological domain (Cacciabue et al., 2000).

Accident Investigation

Accident investigations are oriented to the identification of the root causes of an accident, either related to human errors and mishaps and/or to system failures and malfunctions. From the human factors viewpoint, a method for accident analysis requires a methodological framework that comprises models of cognitive processes and organisations. These models lead to classification schemes, or taxonomies, that allow the categorisation of observed behaviours (ICAO, 1987, 1993; Hollnagel, 1991, 1998).

Accident studies and investigations are reactive types of study, as they usually point towards the definition of preventive measures against future events of the same type. Sometimes, however, accident investigations stop at the identification of root causes and correlations between causes-effects-consequences within the human-machine system. In this case, the reactive approach is limited at the level of retrospective analysis with no proposition for system improvements and feedback modifications.

It is important to distinguish between “accident investigation,” or “accident analysis,” and “root cause analysis (RCA) of events.” The former represents a much wider type of study that embraces the study of previous events that have occurred within an organisation, and the assessment of all root causes of the accident under examination, both human and system related. On the other hand, “root cause analysis” implies a more focused technique on evaluation of causes and effects of a specific

event that occurred. Consequently, “root cause analysis” is only one of the elements that constitute an “accident investigation.”

In the case of human factors, the RCA of an event involves the evaluation of reasons and causes associated with a single inappropriate performance or error. On the other hand, the contribution of human performance during an accident demands the consideration of many events and interactions (positive as well as negative), which contribute to the dynamic evolution of the accident. This distinction is important and will be discussed in much more detail in later sections of this book.

2.5 Integration of Prospective and Retrospective Analyses: The HERMES Methodology

The need to integrate and ensure consistency between prospective and retrospective studies has been discussed earlier in this chapter and represents a fundamental standpoint for developing effective HMS and HEAM measures. Similarly, the approaches and methods for prospective and retrospective studies must be integrated during different stages of design, assessment, training, and accident investigation of a HMS.

The need to correlate prospective and retrospective studies in a logical analytical process that can support the consideration of sound HMI approaches in different areas of application, has led to the development of a methodology that respects all requirements and basic conditions for their integration and mutual correlation.

This methodology is called Human Error Risk Management for Engineering Systems (HERMES).

HERMES is structured in a number of steps that may be applied in order to follow and preserve the basic requirements of congruence and consistency between retrospective and prospective studies, as well as to underpin the correspondence between recurrent HMI analyses and system safety and integrity, which changes during the lifetime of a system (Figure 2.6).

2.5.1 Human Error Risk Management for Engineering Systems

As already discussed, both types of retrospective and prospective analyses rest on a common empirical and theoretical platform: the evaluation of the socio-technical context, and the theoretical stand with respect to modelling human–machine interaction.

The evaluation of socio-technical context represents an essential condition that leads to the definition of data and parameters for prospective studies, and supports the analyst in identifying the conditions that favour certain behaviours, which may foster accidents.

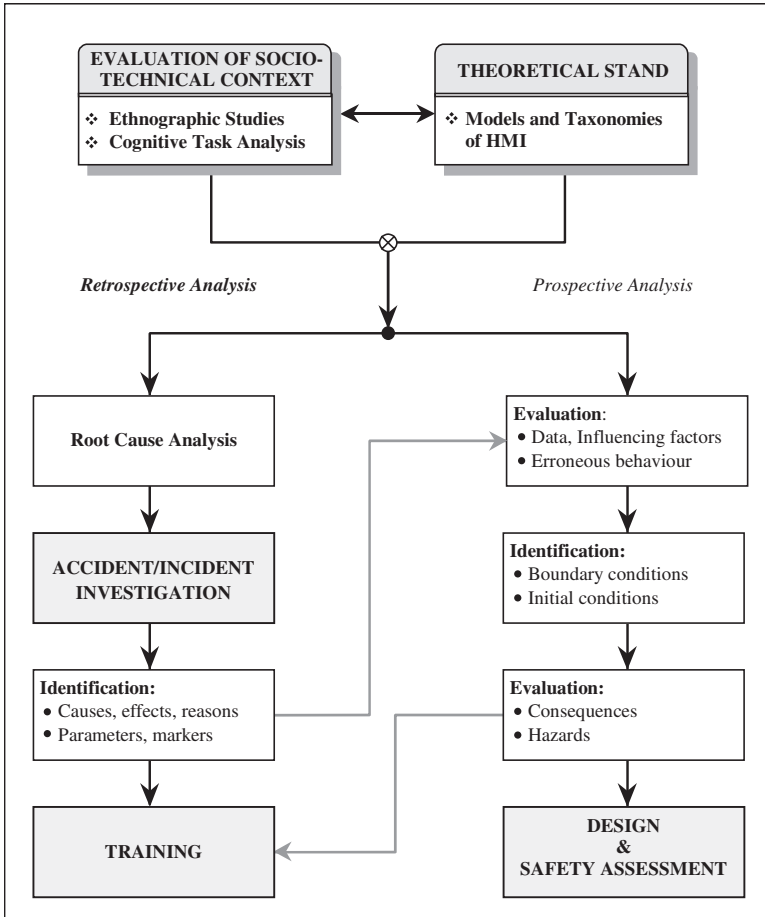


Figure 2.6 Methodology for human error risk management for engineering systems (HERMES).

The study of socio-technical contexts is performed by theoretical evaluation of work processes, i.e., “Cognitive Task Analysis” (CTA), and by field studies, such as interviews with operators, observations of real work processes, application of questionnaires, and analysis of simulator sessions. These represent a set of empirical methods that can be classified as “Ethnographic Studies” (ES).

The selection of a joint cognitive model of HMI and related taxonomy is equally important, as they define the correlation between humans and machines that are considered in order to structure formally the HMS and HMI in prospective studies. At the same time, in retrospective studies, taxonomies are essential in identifying items of HMI that affect incidental conditions. These two forms of assessment of HMS are correlated by the fact that all empirical studies and ethnographic evaluations can be implemented in prospective and retrospective applications only if

they can feed their observations in a formal structure offered by the HMI model and taxonomy.

These initial common elements of the methodology, ensures coherency in performing either an accident investigation, a safety study, a design, or a training course for a certain system or organisation. Moreover, the performance of prospective and retrospective studies requires further correlation and exchange of data between the two types of analysis.

These commonalities and correlated steps can be discussed as follows:

- The investigation on past events and accidents requires that they are described according to the temporal sequence of events. With reference to each event, it is then necessary to identify human behaviours and/or organisational factors that may be considered inappropriate for the circumstances or systemic failures. Root Cause Analysis (RCA) governs this process.
- The combination of series of RCA leads to the identification of causes of accidents, as well as data and parameters that combine to generate the overall accident investigation or accident analysis.
- From the accident analysis it is possible to derive valuable information applicable for correlated prospective studies. In particular, it is possible to derive:
 - causes, effects and reasons of errors; and
 - parameters, indicators, and markers of erroneous behaviours.
- These data and parameters, derived from retrospective analysis, are the basis for the evaluation, in a prospective analysis, of:
 - data and factors influencing performance; and, in general,
 - possible forms of erroneous behaviour.
- These generic types and forms of behaviour are then further elaborated, in a perspective analysis by experience, expertise, and creativity of the analyst, in order to *identify* specific:
 - boundary and initiating conditions.
- Using these data, parameters, boundary and initial conditions in combination with the selected human behaviour model and error taxonomy, it is possible to apply risk methods to evaluate safety margins and outcomes of potential accidental scenarios. These represent the consequences and hazards associated to certain inappropriate human behaviours and systemic failures.
- The outcome of these perspectives analyses can then be further utilised for generating possible accidental scenarios useful for training purposes.
- In this way, coherence between retrospective and prospective analyses is preserved. Moreover, the synergism and correlation that exist between them may be adequately exploited for:
 - performing design evaluations and safety assessments, in order to develop, maintain, audit, and ensure safety standards of an organisation throughout its entire lifetime; and for
 - defining contents and objectives of nontechnical training of operators, permanently linked to the evolution of a system and organisation.

In the following section, we will show how the HERMES methodology enables, in a less formalised structure, to associate goals and methods for prospective and retrospective types of studies with the areas of application of human error and accident management measures.

2.5.2 Analyses and Areas of Application

This section considers the general connections existing between areas of application and types of analysis.

It has been argued that the distinction between prospective and retrospective analyses is only apparent, as they both are important and synergetic representations, in their own way, of a human-machine system. They are indeed the two sides of the same coin, as they must be coherently and consistently applied for obtaining sound results in terms of safety.

What matters is that the theoretical models applied for prospective and retrospective analysis are identical, or at least they are based on the same paradigm of joint cognitive HMS and HMI, so as to ensure complete correspondence and maximum feedback from one type of analysis to the other. Moreover, it is important that realistic and consolidated bodies of data and parameters can be drawn from retrospective analyses that can be consistently applied for prospective studies. This serves the purpose of granting reliability and coherence of results of prospective studies.

However, when different areas of application are considered, it turns out that different types of analysis are better suited than others to satisfy the requirements of each specific area (Figure 2.7). In particular, a number of considerations can be made in respect of each type of area.

Design

Design methods tackle all basic objectives of safety systems, namely: prevention of errors and accidents, recovery from malfunctions and safety critical conditions, and protection from hazards to humans and environment due to an accident.

Design methods are always applied in a prospective oriented view. Designs of control, emergency and protection systems, as well as interfaces and procedures that govern human interaction with systems, are always performed by estimating possible scenarios of application.

However, these are not developed in isolation and need reliable and consolidated data obtained from past experience and engineering knowledge.

This is the “normal” correlation that exists between prospective and retrospective analyses.

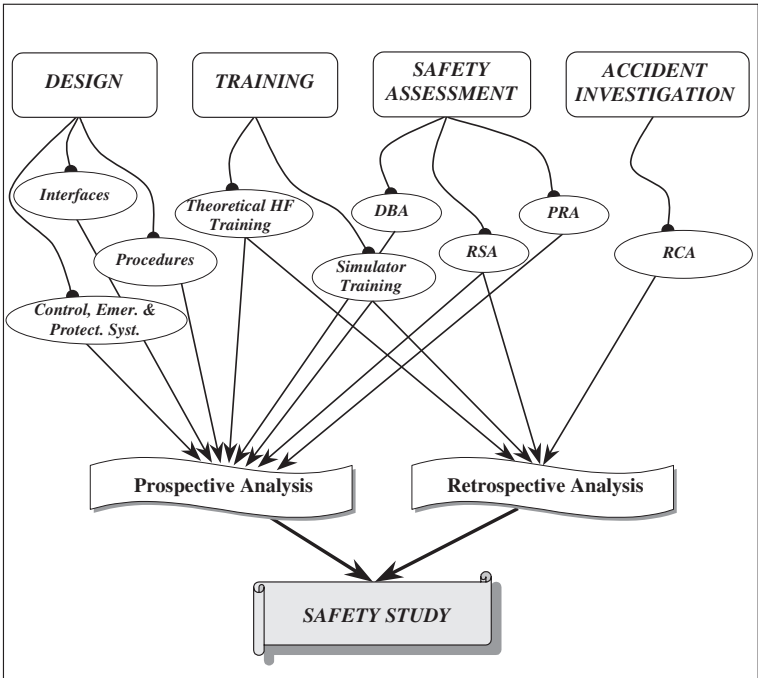


Figure 2.7 Types of applications, types of analysis, and types of simulation of human–machine systems.

Training

Training approaches aim at generating a safety culture and practices that are essential for accident prevention and management by improving and developing relevant technical and nontechnical skills in most technological environments.

This is particularly true in the aviation domain, where the very high reliability of components and the complexity of control tasks make the occurrence of malfunctions and faults very rare. This makes extremely difficult the prevention and management of emergency situations.

Moreover, the human factors contribution to accidents has been shown to be extremely relevant. Consequently, it becomes important to train operators to recognise and anticipate HF problems, and to deal with them as soon as they appear.

This is done in real simulators as well in classroom training sessions, making predictions and estimations of possible anomalous and emergency circumstances and occurrences. These are typical prospective estimates of scenarios.

At the same time, past accidents serve as a reference for the selection of possible training sessions. In such cases, it is possible to evaluate generic behaviours and attitudes related to distributed and shared organisational and national cultural factors in circumstances that have already been encountered in the past.

Consequently, training session can be considered also retrospective type analyses of past events. In any case, consistent knowledge of root causes and experience, derived from past events, is an essential contributor to effective non-technical training.

Safety Assessment

Safety assessment methods are initially applied in connection with design, in order to evaluate the adequacy of safety systems and procedures to cope with abnormalities, malfunctions, and accidents.

Design Basis Accident (DBA) and Quantitative Risk Assessment (QRA) methods are directly connected to the design process and, consequently, they are prospective approaches demanding estimations of possible malfunctions and errors.

However, the application of RSA during the lifetime of a system requires the evaluation of the history and modifications that have occurred and have been made on the system and may have hindered or reduced its safety level. In this sense, an appropriate RSA requires the development of retrospective analysis of past events, enabling the analyst to generate a clear picture of the state of the system. This analysis and audit combine with the estimation of adequate safety indicators and the consideration of possible malfunctions and errors that may occur and must be managed for the overall evaluation of the safety level of an organisation. This is why RSA can be considered a retrospective as well as prospective type of analysis.

In all cases, DBA, QRA, and RSA are effective only if supported by well-correlated prospective and retrospective analyses and by coherent data derived from studies of past event and occurrences. Once again, this is the essential requisite of coherent and sound safety studies.

Accident Investigation

This area of application can be considered as the prototype of the retrospective type of analysis.

Indeed, the objective of all accident investigation approaches is dedicated to the identification of root causes and reasons of accidents. In this sense, accident analysis methods offer a substantial contribution to defining the set of data and parameters that can be derived from past experience and field observation.

As already discussed, the performance of an accident investigation demands that the analyst acquires valuable and complete information of the socio-technical environment in which the accident developed. This offers the possibility to analyse human erroneous behaviours as consequences of other reasons deeply rooted in the organisation.

Moreover, even though accident investigations are substantially retrospective-type studies, their outcomes are used and exploited in prospective application for accident prevention and containment. Therefore, it is necessary that theoretical

grounds and techniques, on which accident investigations are based, are coherent and consistent with the methods and techniques applied for prospective analyses. This is the “normal” correlation that exist between prospective and retrospective studies for ensuring consistency, seen this time from the side of retrospective analysis.

2.6 Ecology of Human–Machine Systems

The need to develop methodological frameworks for considering human–machine systems and human interactions in a consistent and coherent fashion with their working context has already been well recognised in the past.

The literature of the last decade is rich in approaches and methods that focus on this subject. An excellent comprehensive and short review of methodological approaches and theoretical construct has been given by Moray (1997), covering the last 30 years of research and development in the field of human factors applied to different domains and industrial settings.

In particular, the concept of ecology of human–machine systems has become of great relevance in human factors, as it embeds in a single expression a wide variety of contributors and influences on human behaviour, mostly related the role of situation and context.

In general, ecology concerns the dependence that exists between the different actors, human or animal, and the environmental constituents and peculiarities in which they live. This creates interdependence, primarily at natural level, that leads to establishing a dynamic equilibrium and explains the evolution of life and is essential for understanding, analysing, and designing artefacts that are to be utilised by human being to operate in the world.

Nowadays, looking more closely at the working contexts of modern technology and industrial systems, one can consider different *forms of ecology* (Rouse and Sage, 1999):

- *Information ecology*, which involves the context and impacts of “information technology” on people and organisation. This is primarily the role of computer and automation on everyday life.
- *Knowledge ecology*, which considers the way in which contingency and practical experience affect adaptation of information and normative systems to real-world application.
- *Industrial ecology*, which is the effective system engineering and management of industrial processes aimed at developing sustainable products and services. This requires adaptation of personal attitudes and cultures to higher demanding organisational goals and philosophies.
- *System ecology*, which affects planning and defining systems requirements and specifications in adequate considerations for human–machine interactions as a whole.

Designing or studying a human-machine systems is therefore recognised as an endeavour that covers many different domains and must be carried out in consideration of “ecological” aspects involving the interplay and interaction of individuals with other human beings and socio-technical working contexts.

2.6.1 Ecological Approaches to Cognitive Ergonomics

In cognitive ergonomics, a vast movement of research and development has been based on the ecological approach to psychology, derived from the original work of Brunswik (1956) and further developed by Gibson (1966, 1979).

The essence and global perspective of the ecology of HMS are contained in two milestone reference books for human factors analysts that describe the theoretical “global perspectives” (Flach et al., 1995) and show practical implementation of ecological approaches, in different industrial contexts and applications (Hancock et al., 1995).

In particular, the concept of *affordance* strongly affects these ecological approaches to human machine system (Gibson, 1979). *Affordance* implies that mutuality exist between the environment (object, substances, etc.) and the individual. *Affordances* are material properties of the environment that support and limit the potential activity and intentions of the individual. Thus they are measurable quantities, but can be considered only in relation to the individual.

In a modern socio-technical perspective, the concept of *affordances* needs to cover also more immaterial properties of the “work environment” that include cultural and social relations affecting human behaviour. These have to be associated with environmental properties that can be “measured” by identifying material indicators that give a quantifiable size of such immaterial dimensions, which are extremely relevant in bounding and characterising human activity (Zaff, 1995).

Another relevant concept and guiding principle pertaining to ecological approaches is the requirement that a “good psychological theory is an essential aid to design” (Kirlik, 1995), as it represent the reference notion and paradigm for human factors that are equivalent to the basic conservation principles for engineering design. An approach based on cognitive psychology that is capable of predicting environmentally situated behaviour is essential. This is particularly true in a “macroscopic” perspective that aims at enabling the representation of actual human behaviour in a working context, rather than focusing on the (“microscopic”) description of the neural processes and personality aspects that develop in a human brain (Cacciabue and Hollnagel, 1995).

This perspective was already considered by Brunswik (1952) in the lens model (Figure 2.8), where the interplay of environmental structure and cognitive properties is critical for describing behaviour. In particular, in the lens model, there exist in our society and working contexts certain sets of *cues* (X_i) which bear specific relations and may take different values of ecological validity ($r_{e,i}$) with respect to the environment. The utilisation of such *cues* by the organism ($r_{s,i}$) depends then

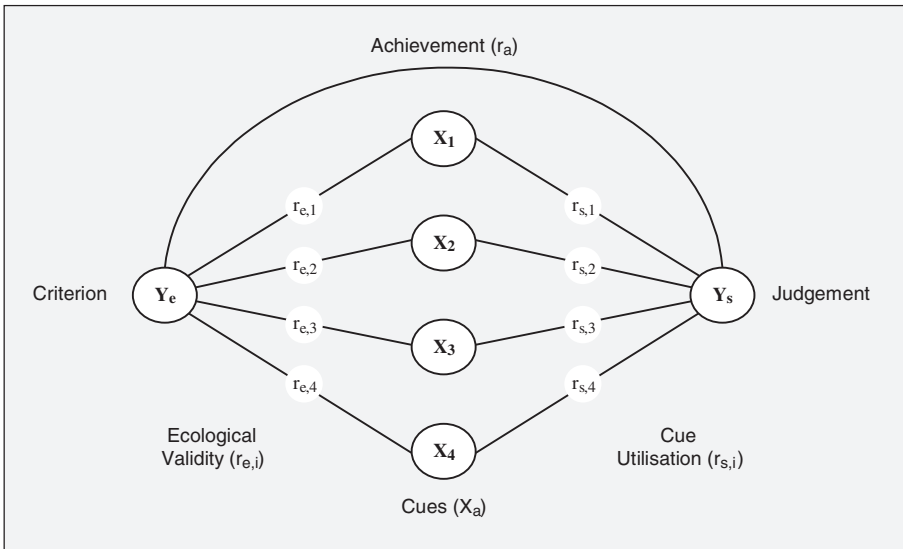


Figure 2.8 The lens model of Brunswik.

on the cognitive counterpart of the environment and leads to the actual implementation of performances in terms of achievements.

As in the case of “affordances,” the symmetry identified by Brunswik between perception/judgement and action with respect to cognition and environment, expands, in modern research, to perception and learning of multiple cues of an environment affected by policies and organisational cultures, and by socio-technical aspects such as risk perception, collaborative or cooperative teamwork, communications, and interpersonal relations.

From a general perspective, all ecological approaches to cognitive ergonomics share the fundamental requirements associated with the need to integrate human activities, at the mental and physical level, with the socio-technical environment in which they are embedded. Consequently, the general label of “ecological approach” can be assigned to any HMS method that recognises such fundamental need in modern technology.

Several methods have been developed over the years in this frame, and some of them will be briefly revised in the next chapter that deals with specific methods and models for HMS.

2.6.2 Ecological Systems in HERMES Perspective

The large family of ecological approaches to human–machine systems represents a well-founded and conceptually sound formalism to approach to human factor issues in modern technological environments.

The consideration for the ecology of the HMS is a fundamental principle that should be respected when tackling different areas of application. It is therefore clear that any application of human factors must respect or adhere to the ecology principles, expressed in terms of theoretical “global perspective,” as well as to all the different *forms* that ecology takes, according to the specific application and working environment.

The HERMES methodology, described in the previous sections of this chapter, is located at a different level, as it represents a practical and structured stepwise process of implementation and correlation of different methods for tackling human factors problems in technology-based areas of application.

HERMES, or more precisely the models that are applied in the process of application of the procedure outlined by HERMES, must respect the ecology principles, as expressed in their philosophical premises, and offers the logical roadmap for the connection and interplay of existing instantiations of ecological principles, in the form of integrated models and methods that consider and combine the interplay of working environments, organisations, technological systems, and humans in control.

The implementation of a design or safety analysis, as much as the study of an accident or the development of a training programme, for a human-machine system requires the combination of many different and specialised methods and approaches, with precise characteristics. The ecology of the human-machine system is one of them, and, although fundamental for its content of correlations between all socio-technical aspects of working contexts, it is not the only principle that human factors analysts must consider in the process of implementation and integration of methods.

A methodological framework like HERMES aims solely at clearing the way for the analyst in the process of stepwise and logical application of methods, models, and approaches for solving the problem at hand.

2.7 Summary of Chapter 2

In this chapter, a number of basic definitions and standpoints for performing Human Error and Accident Management (HEAM) have been considered. These have been developed starting from the consideration that any Human-Machine System (HMS) and Human-Machine Interaction (HMI) play a fundamental role in the process of design and assessment of any technological system, and that they involve the working context and socio-technical dynamic conditions, in addition to the direct interplay of the human operator with the plant under control and management.

The concepts discussed in this chapter rotate around *five standpoints* that represent the axioms and foundation on which any HMS and HEAM measure should be based (Figure 2.9).

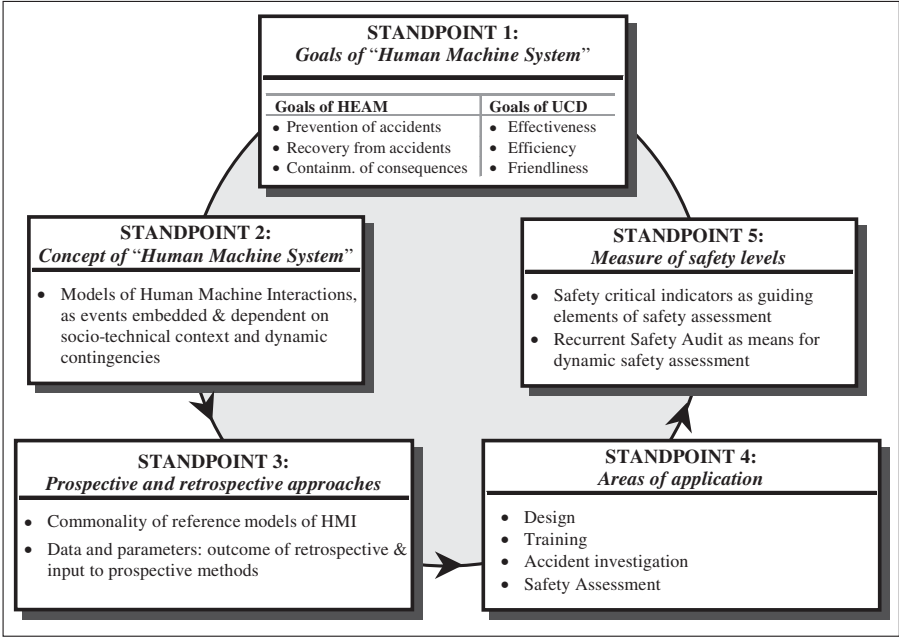


Figure 2.9 Standpoints for the development and assessment of defences, barriers, and safeguards for HEAM.

A methodology that guides the user and safety analyst in the application of Human Factors methods and respects these five standpoints has been developed. This methodology is named HERMES (Human Error Risk Management for Engineering Systems).

The five standpoints and HERMES methodology will now be briefly summarised.

Standpoint 1: Goals of Human–Machine System

The improvement of safety in any technological system demands that appropriate measures are developed aiming at creating awareness, warning, protection, recovery, containment, and escape from hazards and accidents.

These are usually defined as DBS and represent all structures and components, i.e., physical, human, or social that are designed, programmed, and inserted in the human–machine system with the objective of making the management of a plant more efficient and safe, in normal and emergency conditions. DBS must be developed in consideration of the overall design of a system.

Moreover, in the case of the design of HMS, three fundamental principles of modern technological systems must be accounted for, namely: *Supervisory Control*, *User-Centred Design (UCD)*, and *Systems’ Usability*. These three principles must combine in such a way to enable the designer to include the user role already from

the initial design process, e.g., by considering a joint cognitive model of HMI that accounts for all types of human-machine interactions, and then to verify and improve effectiveness, efficiency, and usability by iterative feedback processes and field tests with adequately selected users.

Therefore, the *first standpoint* to be considered by the designer or safety analyst consists in:

The clear identification and appreciation of the goals for which certain HMS or HEAM measures are developed.

In principle, DBS and HEAM measures should tackle one of three objectives: (a) *prevention* of human errors and system failures; (b) *recovery* from errors and failures, once they occur; and (c) *containment* of the consequences that result from accidents and incidents when prevention or recovery did not succeed.

Standpoint 2: Concept of Human–Machine System

Control systems and DBS are directly related to some forms of performance, either appropriate or erroneous. It is therefore important to develop a clear understanding of human performances or behaviours, and their dependence on the specific dynamic context or contingencies and on the socio-technical environment in which they are imbedded.

Consequently, it is important to develop or consider a model, which allows the simultaneous, or joint, representation of the interactions of humans and machines. This includes also a general concept of what is meant by “human error.”

From a designer viewpoint, a strict definition of “human error” is not necessary, and may be bounding or limiting the focus of DBS. What is essential instead is that DBS enable to tackle inappropriate performance/behaviour, in relation to the context and dynamic contingencies, and the specific socio-technical environment in which they are imbedded. In this perspective, the consideration for “human errors” expands the more classical definitions and embraces all behaviours that may engender dangerous configurations of a plant.

Consequently, the *second standpoint* in the development of effective HMS and HEAM measures demands that:

Adequate models of human-machine systems and interactions must be applied for simulating dynamic interplays of humans and machines, as events embedded and dependent on the socio-technical contexts in which they are generated and evolve.

Standpoint 3: Prospective and Retrospective Approaches

The variety of models and methods that are necessary for the development of DBS and HEAM measures can be structured in an integrated framework that considers two types of analysis, i.e., retrospective and prospective studies. These are complementary to each other and equally contribute to the development and safety assessment of HMS and HEAM measures.

Retrospective analyses are oriented to the identification of “data and parameters,” and are built on structured studies that combine RCA, observation and evaluation of working contexts (ES), CTA, and theories and models of HMI. Prospective analyses aim at the “evaluation of consequences” of HMI scenarios, given selected spectrum of: “initiating events and boundary conditions,” appropriate “data and parameters,” predictive models of HMI, and “creative thinking.”

In practice, these analyses rest on a common empirical and theoretical platform: the evaluation of socio-technical context, and the model of HMI and related taxonomies.

The consideration and clear understanding of the differences and synergies between prospective and retrospective analyses is of fundamental importance in the development of any HMS and HEAM measure, in particular all defences, barriers, and safeguards that rest on human intervention and control.

Consequently, the *third standpoint* in the development of effective HMS and HEAM measures can be defined as:

HMI models and theories, as well as data and parameters, derived from evaluation of real events and working environment (retrospective studies) must be consistently and effectively applied for predicting consequences and evaluating effectiveness of safety measures (prospective studies).

Standpoint 4: Areas of Application

Only applying specific methods at different stages of development and management of a system, it is possible to ensure efficiency, effectiveness, and user friendliness of HMS and DBS and preservation of adequate safety levels throughout the lifetime of a plant.

In particular, four areas of application must be considered, namely: *design*, *training*, *safety assessment*, and *accident investigation*. The *design* of human–machine interactions implies implementing basic principles of human-centred automation in the design process, as discussed in Standpoint 1. *Training*, and more specifically nontechnical training, intends to increase the ability of operators to manage safety critical situations, and to capture and notice those factors and indicators of the context that favour the occurrence of errors or mismatches between human situational awareness and system performance. *Safety assessment* of plants and organisations represents a basic requirement and the most complete method by which prevention and control of possible accidents can be performed. *Accident/incident investigation* aims at identifying systemic and socio-technical root causes that generate accidents.

Each of these four areas of application encompasses specific types of assessments and analyses.

The fourth standpoint for designers and analysts of HMS and HEAM measures is correlated to this issue and can be defined as follows:

The development of effective HMS and HEAM measures demands that a variety of tools and approaches are applied for the continuous verification that adequate safety conditions exist and are maintained before and during the lifetime of a system, at the stages of design, training, safety assessment, and accident investigation.

Standpoint 5: Measure of Safety Levels

In order to complete the process of appreciation and generation of measures to improving and safeguarding the safety of a system, a final standpoint is necessary. This is related to the definition of appropriate safety levels of a plant and ways to regularly assess them.

Indeed, in all types of analyses (retrospective and prospective), and for all areas of application (design, training, safety assessment, and accident investigation), it is essential that adequate *indicators*, *markers*, and parameters are identified that allow the estimation or measurement of the safety level of a system.

As each plant and organisation bears specific peculiarities and characteristics related to their context and socio-technical environment, appropriate methods and approaches must be applied for the definition of numerical, as well as qualitative, indicators, which are unique to the plant and organisation under scrutiny.

Moreover, the assessment of acceptable safety levels and standards cannot be limited to the design or plant implementation stage. It is essential that recurrent assessments are performed, in order to account for aging, technical updates and modification, improvements due to accidents or incidents, or simply ameliorations derived from implementing a different technology.

The continuous check and verification that a plant respects safety standards, by carrying out audits and evaluation of safety indicators, is of paramount importance in ensuring that hazards for plants, humans and environments are limited and contained within acceptable boundaries.

The *fifth standpoint* that sustain the activity of analysts and designers of HMS and HEAM measures refers to safety audits and is defined as follows:

The continuous measurement and assessment of safety levels of HMSs is essential for ensuring minimum risk and effective performance of a plant. This process requires the identification of safety critical indicators, as guiding elements of safety assessment, and the performance of recurrent safety audits throughout the whole socio-technical system and organisation.

This last standpoint completes the generic framework of different topics that play a role in developing safety measures for a system. The analyst and designers should select within this framework the features and the most suitable methods and techniques that are of interest for the system under study.

In any case, all five standpoints discussed here need consideration, before developing, or implementing and assessing specific safety measures.

Human Error Risk Management for Engineering Systems

A methodology that offers a roadmap for safety analysts in respecting the five standpoints for applying methods and techniques for HF analyses has been discussed.

This methodology is called HERMES and demands that a series of field studies is performed in association with models and taxonomies of HMI in order to achieve the necessary knowledge of the system under study as well as to develop a consolidated database of information concerning the whole socio-technical working environment that can support predictive assessment of safety.

This methodology will be applied in all test cases and applications shown in the forthcoming Chapters 4–8.

Guide to Applying Human Factors Methods
Human Error and Accident Management in
Safety-Critical Systems

Cacciabue, C.

2004, IX, 347 p. 152 illus., Hardcover

ISBN: 978-1-85233-705-6