Analysis of the preliminary safety case report for the channel tunnel fixed link

Jean-Philippe Pineau, Françoise Abiven, F. Morin, M. Alonso

ANALYSIS OF THE PRELIMINARY SAFETY CASE REPORT FOR THE CHANNEL TUNNEL FIXED LINK

J.P. PINEAU, F. ABIVEN, INERIS,

Parc Technologique Alata, B.P. 2,

60550 VERNEUIL EN HALATTE, FRANCE

F. MORIN, M. ALONSO, EDF/CLI,

35-37 Rue Louis Guérin, B.P. 1212,

69611 VILLEURBANNE Cédex, FRANCE

In the beginning of 1991, after a number of discussions with the Intergovernmental Commission (IGC) for the Channel Tunnel and the Safety Authority (SA), it was decided that EUROTUNNEL (ET) would carry out a general study of the transport system to use the Channel Tunnel Fixed Link.

The basis for this said report was to be drawn from the results of the Avant-Projets already submitted to the IGC, from the existing Safety Reports and from a Quantified Risk Assessment as well as from Risk Criteria.

The final version of the Safety Case Report aims to present a comprehensive assessment of the design and operational safety of the Channel Tunnel Fixed Link, taking into account identified hazards and related risk quantification.

It lays the basis for a safe management of operations.

4th ESReDA Seminar on "Safety in Transport Systems",
Huddersfield, 14-15 avril 1993, pp. 199-211

The present comprehensive report draws from two of the three sections of the safety documentation :

- the safety arrangements which are the foundation for the Fixed Link operation

- the operating procedures describing the sequencing of activities.

The third part deals with :

- the operating rules which detail the required actions.

In view of the control of safety responsibility exercised by the governmental authorities (1), who assess the hazards and risks to which both users and staff present during operations are exposed, the Safety Authority have called on English (2) and French consultants to help them in their task of analyzing the Safety Case.

The subject of this report is limited to the assessment by the French consortium created on this occasion around EDF- CLI and INERIS. Noteworthy is that the EDF-CLI consultants have references in the fields of industrial safety and in particular nuclear safety, and the INERIS consultants in classified industrial plants. (7)

For the time being, the scope of this present analysis is limited to the preliminary safety case report ; all associated remarks are therefore to be taken as provisional. Two more elaborate reports, the Interim and the Final, are being drafted and shall integrate comments by the Safety Authority.

It is important to specify that the consortium's remit does not include the examination of security matters which are studied within other forums.

Also, since certain studies are not yet completed, in particular on operational safety management, signalling and on board or centralized control and command, the following comments are incomplete and likely to be amended.

A first section of this document shall briefly describe the Channel Tunnel Fixed Link.

A second section shall look at the respective roles of the deterministic and probabilistic approaches which have both been retained for the Safety Case Report.

Finally, a third section shall contain provisional comments of the consultants following the Preliminary Safety Case Report.

I. SYSTEM DESCRIPTION

The Concession Agreement given to Eurotunnel applies to the Channel Tunnel Fixed Link (total length approx. 50 km, with 37 under sea). This transport system provides a permanent fixed link between the road and rail networks of France and the United Kingdom. It comprises a rail system and a road system inside the terminals on either side of the Channel. These terminals are linked by two single track rail tunnels and one central service tunnel dug under the Channel.

I.1. Modes of operation

Two modes of operation apply to the Channel Tunnel.

. The rapid transfer of road vehicles (tourist vehicles, coaches, lorries ... and their passengers) by way of shuttle trains.

. The passage of through-trains (passengers, freight) thus linking via the tunnel, the national rail networks for all types of trains, including the high speed trains of the French "TGV" type.

Both diesel and electric locomotives can be used to pull rolling stock.

In normal operating conditions, both running tunnels are used in one single direction each. However, at several places along the Channel Tunnel, trains can pass from one track to the other using crossovers. This allows for operations inside the tunnel to continue when a section of track located between two successive crossovers is out of service.. This could arise for example :

. during tunnel maintenance (railway equipment, civil engineering general equipment)

. following a rail incident preventing traffic on a section of track (breakdown of a train, failure of a catenary, ...).

The main functional characteristics of the Link are the following :

. The Channel Tunnel shall operate for rail and road traffic round the clock and year round.

. The signalling system will allow for the passage of 20 trains per hour in each direction at the beginning of operations. Once the supplementary equipment has been installed, the allowance shall be for 30 trains per hour in each direction.

. 160 kilometers per hour shall be the maximum authorized speed along normal sections, except for freight trains.

. For shuttle trains, total journey time shall be approximately 35 minutes inside the tunnel, plus 15 minutes for departure and boarding formalities, namely a total of 50 minutes.

I.2. Terminals

Traffic is controlled from the terminals which comprise all the facilities required for rail traffic management as well as infrastructure for receiving passengers, for customs controls and for the transfer of road traffic on to the shuttle system.

On each terminal, a rail network is comprised of :
- a rail loop (on the British side, the loop is in a cut-and-cover),
- platforms ensuring access to the shuttle trains,
- junctions with the national rail networks,
- stabling and maintenance areas for rolling stock (depots, workshops, yard).

I.3. Other equipment

Concerning tunnel and track civil engineering :

. rail tunnels are connected through crossovers and piston relief ducts,

. rail tunnels are connected through communication cross-passages to the service tunnel .

. tunnel low points are equipped with sumps for the collection of seepage waters.

Among other fixed equipment :

. a ventilation system used for the renewal of air within the tunnel, for the swift extraction of smoke in the event of a fire, for pressurising the service tunnel to keep it smoke free to shelter passengers in the event of a fire, for the supply of fresh air to technical rooms. It is comprised of two separate networks - the Normal Ventilation System and the Supplementary Ventilation System only used during abnormal or degraded operating conditions ;

. an in-tunnel cooling system using a water cooling network to absorb the heat generated by the trains ; the technical rooms are equipped with forced ventilation sucked in from the service tunnel ;

. a fire-fighting system comprised of an in-tunnel detection system and fire mains and in the technical rooms, automatic extinguishing systems ;

. electricity supplied from the sub-stations for traction power supply and all auxiliary networks ;

. a catenary and earthing circuit ;

. rail signalling ;

. a main traffic control center on the U.K. side and a stand-by one on the French side ;

. control and communication systems including :

- an in-tunnel emergency telephone network
- a network for communication between terminals
- an in-tunnel radio communication system.

II. OBJECTIVES OF THE "PROBABILISTIC AND DETERMINISTIC" APPROACHES

"Deterministic" approaches serve mostly to demonstrate the strength of the concept by applying Codes of Practice and well established design regulations and standards. "Probabilistic" studies, on the other hand, are used to demonstrate the acceptability / tolerability of residual risks resulting from beyond design failures.

The approach selected, both probabilistic and deterministic, will lead to determine reasonably acceptable measures for reducing the risk.

II.1. Probabilistic approach.

A probabilistic analysis uses a quantitative risk assessment (QRA) in order to determine the acceptability of these said risks on the basis of the defined criteria. A QRA is based on the following : risks identification, predicted accident rate, modeling of accident consequences, calculations of the risk exposure of a person, assessment of the main factors contributing to the overall risk.

In the case of a system of such original design as the Channel Tunnel Fixed Link, any application of a quantitative risk assessment must be done with great care as it is difficult to refer to any statistics on equipment failure since this equipment is of an innovative design. However it appears fully justifiable to work from the consequences of accident scenarios which have happened in underground transport systems. To that effect, a detailed analysis of all of the accidents which have already happened, is enlightening.

No accident scenario must be waived aside however low its occurrence frequency may seem ; also, the decision to carry a given class of dangerous goods needs to be made in the light of all its consequences, in particular concerning whether the release of toxic products or a fire are possible (6). Besides the goods classed under dangerous goods, other combustible products may present a risk which is far from negligible when in a confined environment. The history of lorry fires in the Mont Blanc and Fréjus Tunnels demonstrate that reels of cotton thread or plastic objects have produced very touchy situations due to the thick smoke which was generated.

II.1.1. Risk criteria and acceptability.

One basic aspect is, of course, the risk acceptability criterion. A difference must be made between individual risk and societal risk (2). And it is important to point out that the French regulatory approach on transport is undergoing quite an evolution (4), contrarily to the British approach which, for instance, sets a tolerability threshold for individual risks at 1×10^{-3} per year for workers. However this figure is based on accident statistics data and only takes into account existing facilities.

As a reference, it was also accepted that a passenger travelling by train from London to Paris should be in the part of the journey through the Tunnel, as safe as in the equivalent journey (i.e. 50 km) from either Waterloo and Folkestone, or from Sangatte and Paris.

Concerning the societal risk, practically speaking, curves plotting accident frequencies against the number of fatalities will be used. These curves were obtained from rail accidents statistics.

In the risk criteria approach, it is mostly the risk of fatality which has been taken into account.

The method shall essentially compare the quantified risks of undesirable events with the selected risk criteria , taking into account the functional analysis and the development of fault and event trees.

The British approach has chosen the ALARP principle (As Low As Reasonably Practicable). Within the whole ALARP probability region which limits are in a 1/1000 ratio, any risk is tolerable only if its reduction is impracticable or if its cost is grossly disproportionate with the improvement gained.

This region shows an upper level above which risk is intolerable (for high probability of occurrence of an undesirable event) and a lower level below which risk is considered as negligible (for low probability of occurrence of this event) and therefore tolerable.

In the case of the Channel Tunnel Fixed Link, the Safety Authority has accepted this latter approach.

II.1.2. Undesirable events

The main initiating events studied under the QRA are fires, collisions and derailments. Evaluating their frequency is done through a fault tree.

The consequences of these events are modeled using an event tree, a tree which brings out the undesirable events in fine.

II.2 Deterministic approach

The main purpose of the deterministic approach, both on design and operational management aspects, is to prove, for different situations, that the severity of consequences is as limited as possible.

For this case study, a definition of safety parameters with associated criticality is to be dealt with for every situation.

In order to consider human and technical failures, measures are to be taken and graded in different levels :

. Prevention which consists in designing, constructing and operating the installation so as to give it protection to avoid failures and to limit their consequences throughout a range of selected normal and abnormal situations. Often important safety factors are included mainly at the design stage.

. Monitoring and protection of the installation during operations which is assured by operating arrangements, procedures and rapid shutdown / interlock systems, while the functionality of equipment is verified by means of periodic tests and non-destructive inspections. Operating rules are additional to safety devices.

. Protection against occurring incidents or accidents as a result of technical or human failures, despite these safety and operating arrangement. The installation is then equipped with very reliable safeguard systems whose sole function will be to limit the serious consequences of these incidents and accidents to acceptable levels, taking account of their estimated probability.

. Finally, preparation for the management of serious by highly unlikely accidents would assist in controlling serious or complex situations which have not been predicted.

The safety parameters which encompass all aspects of the system (technology, human and organizational), relate to each of the levels listed above. All arrangements confining them within a given region are as many barriers limiting the severity of an incident or an accident.

The safety parameters refer to various situations which were selected for the envelope character of the operating situations under study, hence, it is far more sensible to establish envelope operating situations in order to identify the most relevant safety parameters. Nevertheless further steps of the analysis will deal with the exhaustiveness of the approach.

To carry out such an analysis of a situation, a functional breakdown is necessary in order to bring out the failure conditions by following a procedure which is quite similar to a failure modes and effects analysis (FMEA).

ooOoo

The final advantage of these two approaches is that the obtained results can be compared through a cross analysis. Thus, both are based on possible failures whose knowledge is the keystone for operating safety organization. For operation, the deterministic approach results in catalogue of safety parameters for which the probabilistic approach allows to adapt the convenient operation monitoring according to the severity and gravity of undesirable events.

III. PROVISIONAL COMMENTS OF THE CONSULTANTS ON THE PRELIMINARY SAFETY CASE REPORT.

III.1. Organization

The consultants started by defining their working method and the work procedures which would allow for the best relationships between the consultants and the Safety Authority (fig. 1).

A major objective was to try and obtain a common position from the French and British consultants. This proved possible : reports were drafted in common and submitted to the Safety Authority.

Concerning work procedures, the organization was based on a grid showing the EDF-CLI and INERIS consultants' specialties (see fig. 2). This grid is identical to the one considered by Electrowatt, the English consultant.

Since various situations to be analyzed called for specialized consultants, lead roles were defined as well as processing methods (see fig. 3).

III. 2. Analysis of the Preliminary Safety Case Report

The following main provisional remarks concern the Preliminary Safety Case Report.

The scope of these comments is limited to :

III.2.1. The quantitative risk assessment and the risk criteria (probabilistic section).

III.2.2. Safety management linked to the definition of safety parameters (deterministic section).

The authors draw the attention to the fact that the following comments are provisional since only a limited number of scenarios have been studied so far and it is therefore impossible at this time to judge the exhaustiveness of the analysis.

A reminder also to point to the fact that operational characteristics can be normal, reflect a degraded mode or an emergency situation. This implies that the safe operational envelope must be defined in order to predict any passing from one operational mode to another.

III.2.1. Quantitative risk assessment and risk criteria

A preliminary analysis was carried out taking into account a sample of plausible events :

Eight events were considered :

- Fire in a vehicle in a tourist shuttle
- Fire in a vehicle in a heavy goods vehicle (HGV) shuttle
- Fire in a passenger through-train coach
- Derailment of a freight train
- Derailment of a tourist shuttle
- Derailment of a passenger through-train
- Derailment of an HGV shuttle
- Collision between two trains (general).

Noteworthy are the three initiating events which have been selected : fire, derailment and collision.

At this stage of the study, it is worth reminding that the circumstances in which these various events occur shall most likely need to be studied in greater depth, taking into account in particular the types of dangerous goods, substances and materials carried, the consequences of incidents inside the service tunnel, the operating circumstances and the exact nature of the trains accepted through the tunnel. Others events could also be studied : for instance the release of toxic products and failures of utilities.

The analyses by event trees were quantified mostly on the basis of British Rail operating statistics. The analysis will need to be extended to include the statistic results of other rail companies.

In view of the various types of trains, a more detailed analysis is still to be made, which would include other events and all of the operating conditions.

The consultants have insisted on the need to also include statistics from the operation of underground railways and reliability data determined by equipment firms.

Finally, uncertainty as to the statistical data used needs to be specified.

III.2.2. Safety management linked to the definition of safety parameters.

Safety operating management organizes all activities of operation, maintenance and relationship with the environment outside the Fixed Link System.

This organization is based on the definition of a set of safety parameters. These parameters must in turn be maintained within regions or in states allowing for a safe operation.

It must provide for experimental operational feed- back from the System through the recording and analysis of incidents and accidents, and collect reliability data. In that way, the design and related safety studies (hazard analysis, FMEA, fault trees and event trees) can be verified or corrected on the basis of lessons drawn from accidents or foretelling incidents, and from the obtained reliability data. The organization of this feedback is to be defined, when the operating management is finalized.

It must also control the modifications, in order to ensure that their impact on the design will indeed be taken into account, in particular for the catalogue of safety parameters and for a correct commissioning of the latter.

Working in conjunction with the system's designers, maintaining the evolutive nature of the safety studies ought to be an objective of the operational safety management system.

The present development of the Safety Case has not yet allowed for designing the operational safety management system. So far, a list of safety parameters corresponding to a few given situations has been established. This list must be as comprehensive as possible and provide a classification following the definition of a criticality rating. Thus far, it applies to the following situations :

- normal operation of a tourist shuttle
- normal operation of an HGV shuttle
- operating a Channel Tunnel train on a single track in a section close to a portal
- operating a freight train on a single track in a central section of the tunnel
- evacuation outside and along the shuttle in the event of a fire on board a tourist shuttle
- evacuation to the service tunnel in the event of a derailment of a tourist shuttle
- evacuation to the service tunnel in the event of a fire on board an HGV shuttle
- uncoupling a Channel Tunnel train operating on a single track near a portal.

At this stage, the analysis of the "normal operation of a tourist shuttle" situation is the only one which has been given to the consultants. It provides a first series of safety parameters with their criticality rating.

In this situation n° 1, the present analysis emphasizes signalling failures as the most critical, which was predictable. This first remark highlights the amount of attention which must be given to the reliability and the maintenance of the signalling system.

IV. CONCLUSION

The analysis of the Channel Tunnel Safety Case Report remains pending . So far, the consultants make provisional conclusions on the Preliminary Safety Case and other documents such as safety arrangements (volume B : system description and volume F : transport of dangerous goods) and risk criteria. These conclusions were given to Eurotunnel through the meetings of Safety Authority for the Safety Case, meetings at which the consultants were invited. Many aspects are still quite incomplete (safety parameters, description of accident scenarios).

This task allows for the integration of both the French and British approaches to risk analysis.

The objectives are :

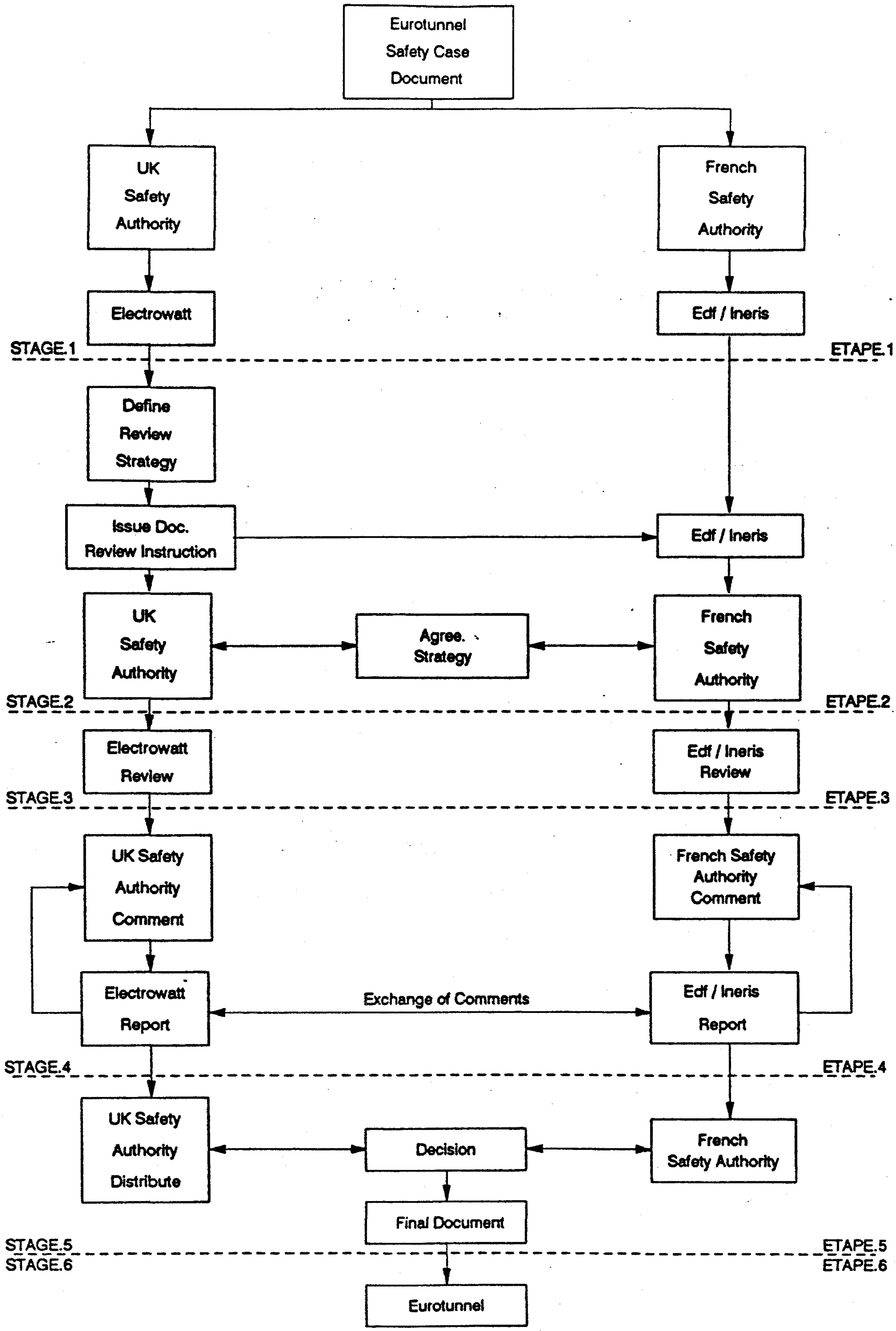
. a presentation of design coherence

. testing out this coherence by comparing the risk with a predetermined criterion and applying the ALARP principle

. using the most extensive catalogue of safety parameters, to identify a coherence between design and safety studies on the one hand, design and the operational safety management system on the other.

One of the expected advantages of this work between authorities, operators and consultants, is to determine as best as possible what the safe operating conditions for such a system are. Experimental feed-back into safety management including incidents and accidents is a major asset to improve the level of safety.

Finally, cross-comparing the results of the quantitative risk analysis with the list of safety parameters is essential and will have to be done in order to ensure the coherence and exhaustiveness of the Fixed Link Safety Case.



Flow of Documents : English - French Experts

Revision 3. 7th July 1992

FIGURE 1

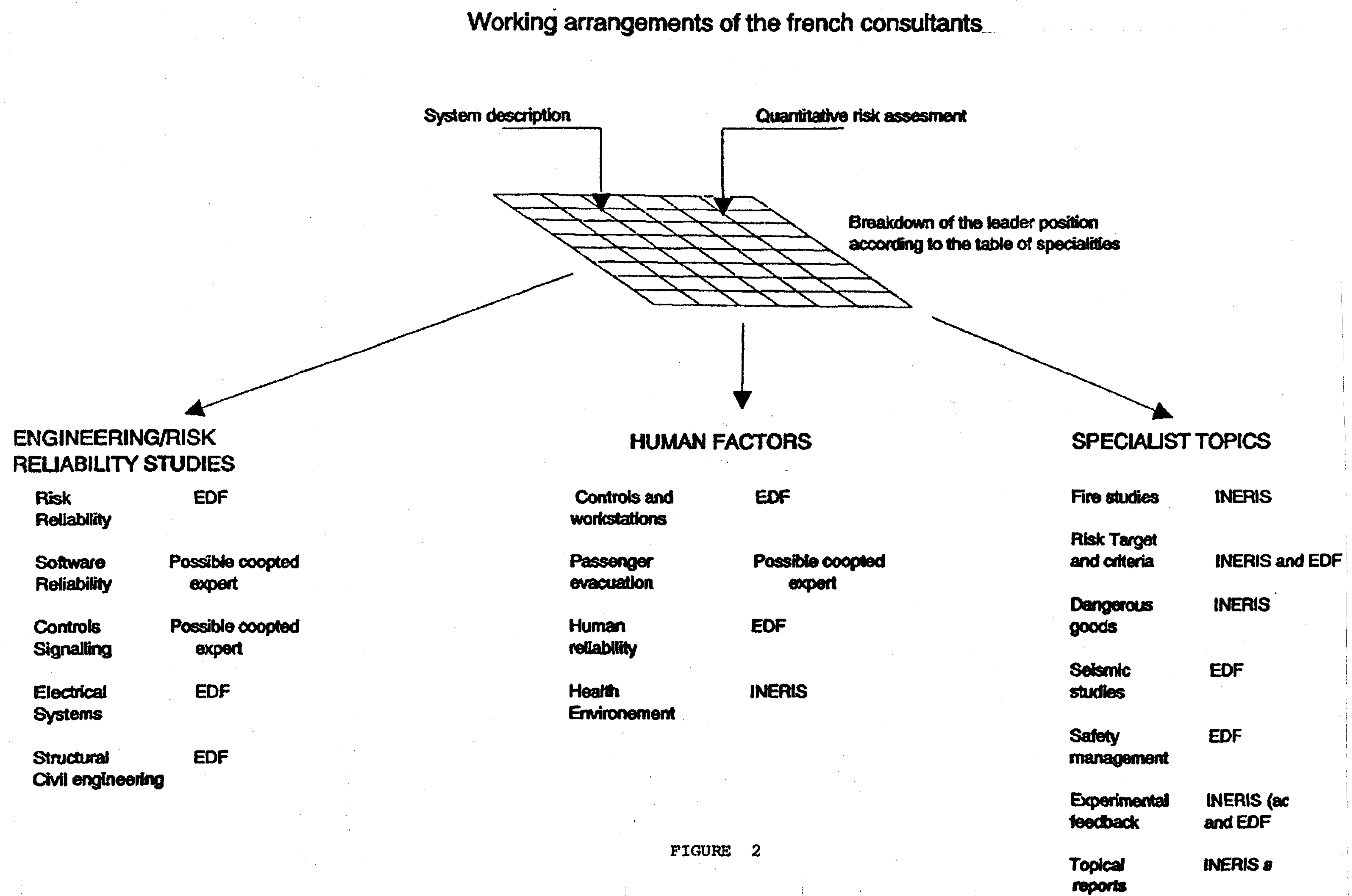

Working arrangements of the french consultants
System description
Quantitative risk assesment
Breakdown of the leader position according to the table of specialities
ENGINEERING/RISK RELIABILITY STUDIES
Risk Reliability
EDF
Software Reliability
Possible coopted expert
Controls Signalling
Possible coopted expert
Electrical Systems
EDF
Structural Civil engineering
EDF
HUMAN FACTORS
Controls and workstations
EDF
Passenger evacuation
Possible coopted expert
Human reliability
EDF
Health Environement
INERIS
SPECIALIST TOPICS
Fire studies
INERIS
Risk Target and criteria
INERIS and EDF
Dangerous goods
INERIS
Seismic studies
EDF
Safety management
EDF
Experimental feedback
INERIS (ac and EDF
Topical reports
INERIS a

FIGURE 2

ANALYSIS OF SITUATIONS

Breakdown of the leader role :

- normal situations ⟶ EDF
- degraded situations ⟶ INERIS or EDF
- emergency situations ⟶ INERIS

Processing method :

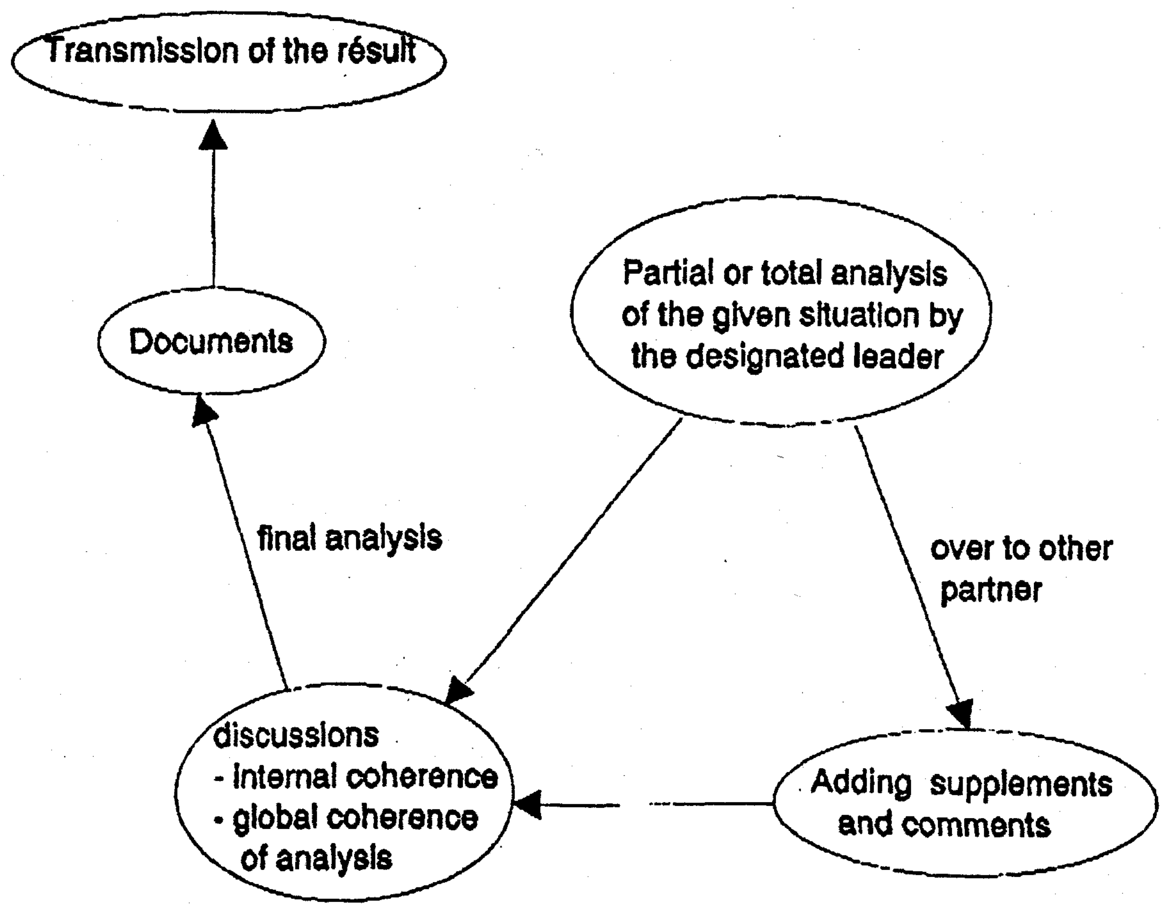


FIGURE 3