Human Factors and Ergonomics in Manufacturing, Vol. 17 (1) 43–78 (2007)

Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/hfm.20062

Nuclear Power Plant Communications in Normative and Actual Practice: A Field Study of Control Room Operators' Communications

Paulo V.R. Carvalho
Comissão Nacional de Energia Nuclear, Instituto de Engenharia Nuclear Cidade Univerisitária, Rio de Janeiro, Brazil

Mario C.R. Vidal
Grupo de Ergonomia e Novas Tecnologias, GENTE, COPPE/UFRJ Cidade Univerisitária, Rio de Janeiro, Brazil

Eduardo F. de Carvalho
Departamento de Engenharia Industrial, Escola Politécnica, UFRJ Cidade Univerisitária, Rio de Janeiro, Brazil

ABSTRACT

The safety and availability of sociotechnical critical systems still relies on human operators, both through human reliability and human ability to handle adequately unexpected events. In this article, the authors focus on ergonomic field studies of nuclear power plant control room operator activities, and more specifically on the analysis of communications within control room crews. They show how operators use vague and porous verbal exchanges to produce continuous, redundant, and diverse interactions to successfully construct and maintain individual and mutual awareness, which is paramount to achieve system stability and safety. Such continuous interactions enable the operators to prevent, detect, and reverse system errors or flaws by anticipation or regulation. This study helps in providing cues for the design of more workable systems for human cooperation in nuclear power plant operation. © 2007 Wiley Periodicals, Inc.

1. INTRODUCTION

The nuclear industry has always demonstrated their concern to avoid and mitigate the consequences of accidents by treating safety according to classical system safety engineering paradigms. Such safety design begins in the conceptual design phase and continues throughout the project life cycle: design, production, testing, licensing, operational use, and decommissioning. The primary emphasis is on the early identification and classification of hazards so that action can be taken to eliminate or minimize these hazards before final design decisions are made. Since the first Nuclear Power Plants (NPPs), the

Correspondence to: Paulo V.R. Carvalho, Comissão Nacional de Energia Nuclear, Instituto de Engenharia Nuclear Cidade Univerisitária, Ilha do Fundão, Rio de Janeiro, RJ, Brazil, CEP 21945-970. E-mail: paulov@ien.gov.br

hardware has been based on defense-in-depth concepts, barriers, redundancies, diversity, high-quality components, and so forth. The nuclear industry has also developed a sophisticated risk management system based on analytical safety control, considering postulated accident scenarios predicted from processes models to develop probabilistic risk analysis (PRA) to estimate the probability of harmful accidents.

Until the Three Mile Island (TMI) accident in 1979, human factors received little attention in nuclear safety (Mosey, 1990). After that, nuclear accidents have been revisited, from Windscale to Chernobyl, and root cause analyses have shown human errors as a major component in all of them. As a result, human error and human behavior have been treated in the same way as technical (hardware) linear systems. In this framework, the natural variability of the complex human agents must be controlled within the formal work constructs of the organization: procedures that should be strictly followed as a script (a good practice), a rigid hierarchy and labor division, function allocation, etc., which have been taken for granted as the basis for safety in the human work design processes in NPPs (De Terssac & Leplat, 1990; De Terssac, 1992; Hirshhorn, 1993; La Porte & Thomas, 1995; Vicente, 1999; Vicente, Mumaw, & Roth, 1997). Violations or deviation from procedures or good practices—those that designers and regulators have defined as necessary for a safe operation—have received special attention as a source of the human errors (Reason, 1990).

However, empirical ergonomic field study findings (Amalberti, 1992,1996; De Terssac, 1992; Faverge, 1970,1980; Poyet, 1990) lead to indications that in actual work conditions, where there are performance standards and where skilled personnel show a consistent use of strategies, what some people call *human error* or *routine violation* can be viewed as an innovative method used by these experts to cope with complex situations. Under these circumstances, routine violations can be seen as opportunities for efficient action and even learning on the job processes; instead, they are too often to be seen as generators of accidents (Besnard & Greathead, 2003).

The mismatch between how the work is actually performed and how the organization imagines it should be done contrasts the classical versus the complex system theory paradigms. We argue that human work design in complex sociotechnical systems should be treated under new paradigms based on the complex systems theory.

2. WHAT SYSTEM?

Modern organizations are complex sociotechnical systems consisting of many nested levels: government, regulators, company, management, staff, activities/work/technical systems/processes. According to Rasmussen and Svedung (2000), safety can be viewed as control problem and safety must be managed by a control structure embedded in an adaptive sociotechnical system. "Accidents such as Bhopal, Flixborough, Zeebrugge and Chernobyl have not been caused by a coincidence of independent failures and human errors. They were effects of a systematic organization behavior toward accident" (Rasmussen & Svedung, 2000, 14). From this perspective, an accident can be viewed as an emergent result of complex system operation. Adverse emergent properties in complex systems have higher possibilities to occur when the control systems do not adequately handle systems failures/disturbances in a broad sense, such as external disturbances, component failures, human failures, or dysfunctional interactions among system components, throughout the system's life cycle.

2.1. The Control System

In control theory, systems can be modeled as interrelated components that maintain the system's stability by feedback loops of information and control. The plant's overall performance has to be controlled to produce with safety, quality, and low cost. In such an arrangement both controllers (human and automatic) play fundamental roles such as to establish system goals (set points), to know the system status and its behavior in the near future (situation awareness; Endsley, 1997), to know what the other agents know (mutual situation awareness). This is done through continuous observation/feedback/communication loops where the agents construct their system model of behavior to compare with system status to be able to act on the system to produce the desired outcomes.

Figure 1 shows the basic control loop in the sharp end (control rooms) of modern process industries. In this supervisory control mode, the human operator has a supervisory role related to the automatic controller. The operator has access to system state information, using the control room indicators, video display units (VDUs), strip charts, alarms (dotted lines), and the automation controller status, and may have direct ways to manipulate the controlled process, bypassing the automatic controller.

The human or automated controller obtains information about the process state from measured variables (feedback) and uses this information to initiate action by manipulating controlled variables to keep the process operating within predefined limits (constraints) or set points (the goal), despite disturbances to the process. According to Checkland (1981), the maintenance of any open-system hierarchy will require a set of processes in which there is communication of information for regulation or control. An industrial plant can be described as set of many nested hardware loops that have to be controlled by the control room crew. Figure 2 represents such a system.

As we can see in Figure 2, a complicated and well-organized set of hardware control systems is embedded in a porous communication system (Grant, 2001, 2004) that represents the human action.

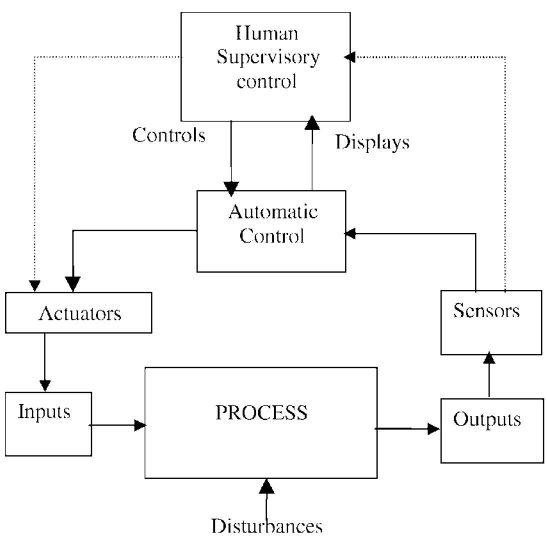

Figure 1 The basic control loop.

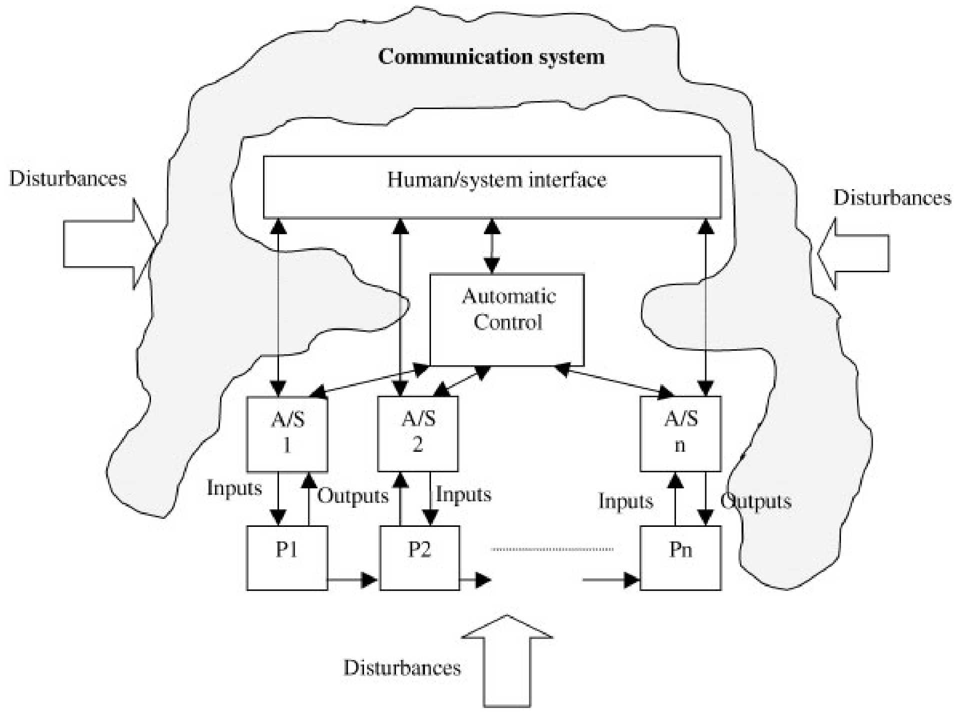

Figure 2 System representation. The A/S boxes represent the various actuators/sensors sets, while P1 . . . Pn represent the multiple processes to be controlled in the complex system.

A porous communication system is a theoretical model proposed by Grant (2001) in which the principal concern lies in the construction of a theory of social communication theory, which acknowledges contingency on three levels: language, communication, and society. It operates with a logically loose definition of language vagueness and, in direct relation to this, with what radical constructivists call the cognitive autonomy of social actors, in an attempt to integrate the concepts of vagueness and cognitive closure at the communication level. Vagueness is to language what porosity is to communication. Vagueness relates to language meaning—semantics—at a logical level of definition, whereas porosity relates to language use at the pragmatic level of social communication. Porosity does not signify logical vagueness but the use of fuzzy standards (e.g., the binary code—good/bad—of alarm windows can be increasingly fuzzy depending on the state of the plant; simple procedure instructions may lead to many different interpretative possibilities during real work; the state of equipment may be inferred by visual inspections, etc.). If language is vague, then communication, based on language, is porous, or "infinitely iterable" (Derrida, 1988, 61).

Accordingly, people learned to use fuzzy signs (and porous communications) to deal with system complexity, enabling system operation. In other words, if we could organize people's work in the same way as we do hardware systems (i.e., using only formal organizational constructs such as rules, procedures, norms, etc.), we do not need to think about anything outside the scope of linear control system theory. However, we claim that this is not possible precisely because of the complex nature of the systems and especially because of the nature of social communication systems. The natural language used in verbal interactions of control room operators can be vague, and they use fuzzy signals leading to a porous communication system with the following characteristics:

1. Communication systems are unstable.
2. This instability cannot be suppressed.
3. Semantics and codes at a local level can allow a contingent stability (Grant, 2003).

This argument brings communication to the center of the debate about the stability of complex sociotechnical systems. Because experience indicates that we have stability, maybe it is not because of any transcendental community (see Habermas, 1999); rather, stability is reached through continuous interactions, where the communications oscillate between the new and the redundant, the right and the wrong, from agent to agent, and from one context to another.

In this article, we use field studies to analyze the communications of control room operators in a nuclear power plant. We show how porous communications can contribute to a contingent system stability, and how these communications overcome the limitations of the normative communication system (rules, norms, procedures, work permits, logical signals) prescribed for the plant operation.

3. FIELD STUDIES IN NUCLEAR POWER PLANT OPERATION

Field studies seem to be the natural approach for this research. As pointed out by Mumaw, Roth, Vicente, and Burns (2000), field observations afford the opportunity to gain a realistic view of the full complexity of the work environment, which is not possible with other approaches, like laboratory-controlled observations. Three field studies were carried out in one NPP control room and during simulator training. Although the methodological framework based on the observation of the operator's activities during their actual work was the same for all studies, each one has particular aims and specific procedures that will be described in the next sections. Findings from the first study were used to guide the procedures for the second and third studies. The first study—an exploratory study—was conducted to reach a better understanding of the NPP operators' work environment and activities during the work shift. In the second study, the activity of the operators during plant shutdown and start-up was observed with the help of audio and video recordings. In the third study, in the NPP full scope simulator, we observed how operators dealt with the safety critical function and emergency operation procedures.

3.1. The First Study: Understanding the Work Environment

In this exploratory study, our aim was to understand the work environment and the operator task, and to identify the operational modes and some constraints on the operators' activities.

3.1.1. Procedure. Two researchers, with background knowledge in nuclear operation, conducted observations in the control room, interviews with operators, and other plant workers. The pilot study took about 2 weeks (10 days), with five operator crews. During the study, the researchers spent 4 hr/day (40 hr total) inside the control room observing the operators' work and conducting interviews during work intervals. The researchers also conducted interviews with field operators, maintenance personnel, training staff (at the full-scope simulator), engineering personnel, and plant management. To collect empirical data in this exploratory study the only material used was paper and pencil.

3.1.2. Participants. The five control-room operator crews who participated in the study each were composed of four licensed operators—shift supervisor, foreman, reactor operator (RO), and secondary system operator (SCO)—and one unlicensed operator—the auxiliary panel operator (PO). The shift supervisors and foremen were senior reactor operators with ages ranging from 30 to 55, with more than 10 years experience in NPP operation (they were operators in another NPP before they came to this plant). Some reactor and secondary circuit operators (ages from 30 to 40) were also experienced operators (5 to 10 years), but other ROs were recently employed workers (1.5 years) with ages from 20 to 25, and no previous experience in plant operation. The had received training on the job.

3.1.3. First study results. Because the research approach attaches a great significance to the environment as the root of variation in people behavior, we present a brief description of the organization, the NPP control room, and the types of procedures used by the operators.

This utility operates the only two NPPs in the country, delivering about 1800 MWe (electrical megawatts), which represents about 4% of the country's total electric energy production. The present organizational arrangement was created in 1997 from the merging of two former state companies with different organizational cultures: a nuclear engineering company (a design company in charge of the new nuclear projects), and the nuclear directorate of the electric power utility. The merger process itself was complex, suffered opposition from the unions and technical associations, and brought tensions to the workers. When these studies were performed (summer 2001) the merging process was already finished and the organization was developing a safety culture access and enhancement program, with the support and advice of the International Atomic Energy Agency (IAEA; International Nuclear Safety Advisory Group [INSAG-15], 2000).

The operation of the plant where the field studies were carried out started in the middle of 2000; however, most of the instrumentation and control equipment had been acquired 15 years earlier (due to delays in plant completion). That is why the control room and instrumentation/control system uses process control technology developed in the 1970s in Germany (from where this plant was purchased). Figure 3 shows a schematic layout of this control room. It consists of stand-up control panels, an operator desk with two workplaces, one for the RO and one for the SCO, printers, a communication desk, and bookshelves for operating procedures.

There are also work desks for the foreman and the shift supervisor, who also has a small room that faces the control room. The control panels use the mosaic technology (see Figure 4). Accordingly, hard-wired meters, strip-chart recorders and control devices (start/stop pushbuttons) arranged in order to reproduce the functional diagrams of the various plant systems, replace the plastic tiles of the control panels. The alarms are presented in alarms windows distributed across the panels and the operator desks, according to the system to which they belong. There are five cathode ray tube displays (CRTs) placed in a panel in front of the operators' desks: CRTs 1 and 4 present plant variables (up to eight) in a bar graph and digital form, CRTs 2 and 5 present textual alarm messages

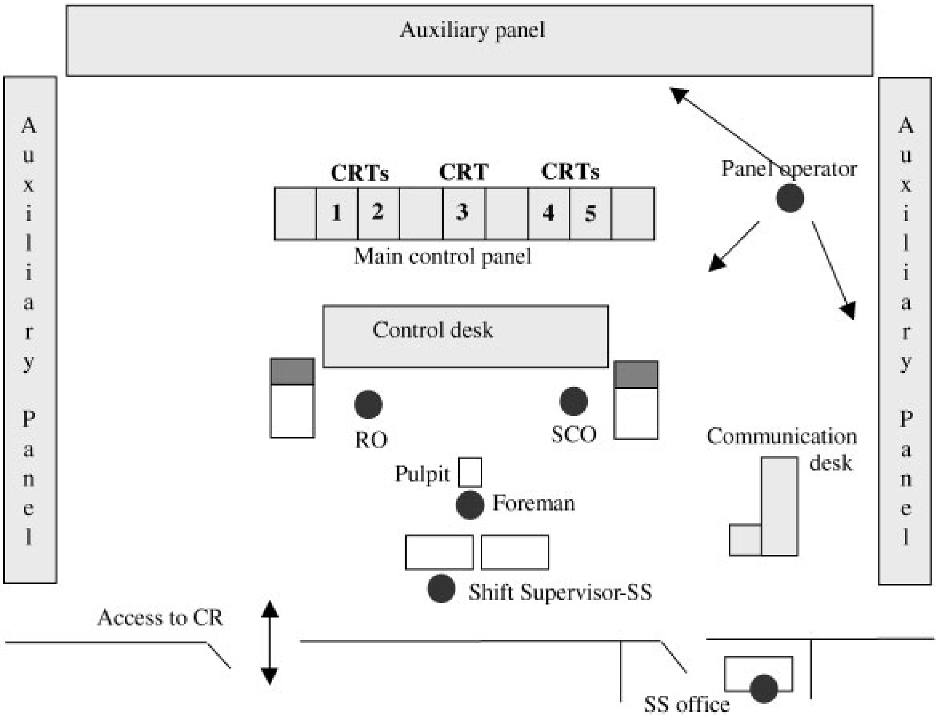

Figure 3 The NPP control room (CR) schematic layout.

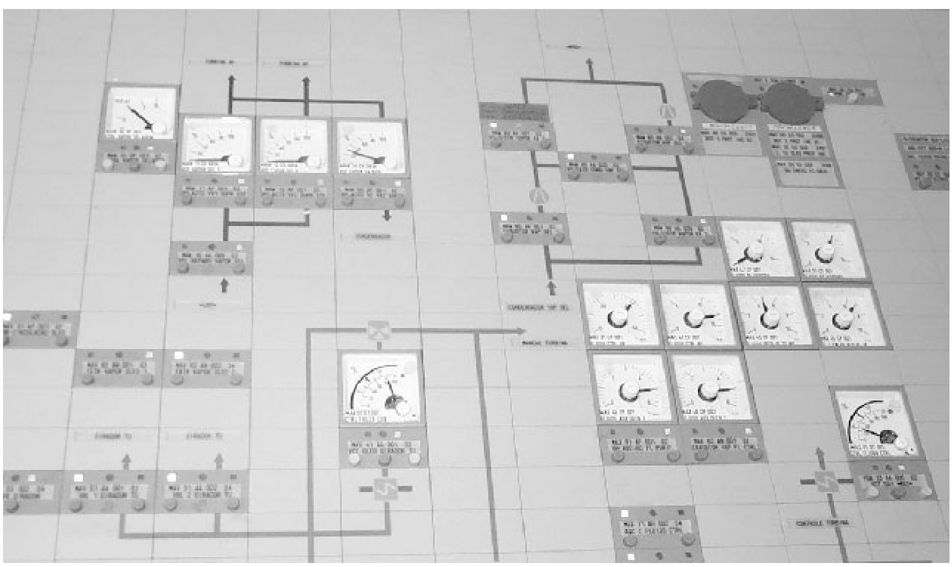

Figure 4 The mosaic technology control panel.

chronologically ordered in a list, and the last one, CRT 3 located at the middle of the panel, presents the automation system status (criteria display). The two operators also have a computer in their workplaces for administrative work and for the safety parameter display system, which was developed afterwards (it did not belong to the original vendor contract). From the pulpit, located in the middle of the room, the foreman reads procedures to the operators.

The plant procedures are written on paper. In Figures 5 and 6 we present the basic procedures format; they are used both for normal operation and for emergencies. In these procedures the operators actions are presented in two ways: flow diagrams to map the course of the actions (Figure 5), and check lists (Figure 6), in which the operators must fill the blanks with the detailed actions performed, when some variable reaches the expected condition, or when some command is activated. This format is justified to cope with the high degree of plant automation. The allegation here is that when filling out the check lists the operators would stay more alert to the situation or plant state. In the Figure 5 flow diagram, the rectangles S1 and S2 present actions that must be done when the condition (in the decision box) is true. S1 and S2 are main action labels, pointing to another part of the same procedure where the detailed steps of manual (or automatic) actions are described. Within this exploded structure, the operators have to browse the procedures continually, going from general to the detailed parts and vice-versa.

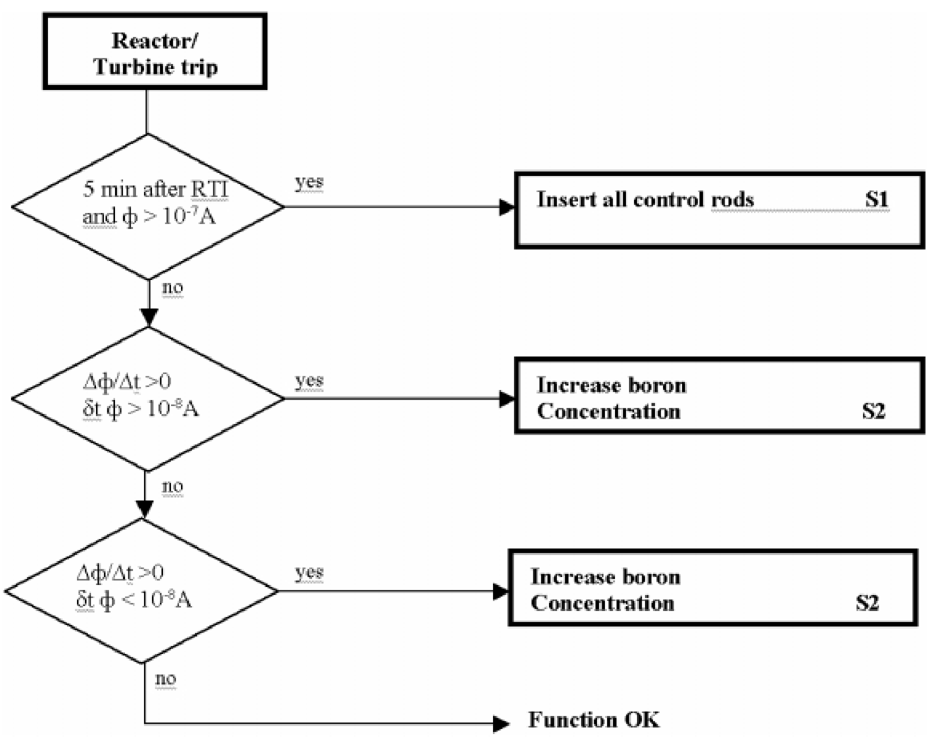

Figure 5 Example of a flow-diagram procedure format.

Insert control rods	1.2

RESA (on master control console or reactor protection system panel)	initiate	**RESA MANUAL**	❑
or			
Single release on core cross section display	select	**JTB 80 EX 111**	❑
or			
Group release on core cross section display	select	**JTB 80 EX 111**	❑
Affected control rod(s)			
on core cross section display	select	**JTE–H 88 FG *****	❑
STEW single	select	**JTB 80 EX 133**	❑
On master control console STEW	initiate	**JTP 36 EX 036**	❑

Remark:
Further information about unmaneuverable or jammed control rods or of uncontrolled moving control rods see OM 2–4.9 and OM 2–4.10.

Figure 6 Example of procedure checklist.

We observed some hardware constraints resulting from the obsolescence of instrumentation (hardware) systems and man/machine interfaces that can be summarized as follows:

1. Human-machine interface/instrumentation: Difficult display visualization, inadequate position of graphic registers, opacity of the automation, conventional alarm system design.
2. Communication system: The control room operators' initial contacts with field operators use a broadcast system that spread the control room call to the plant. The field operator called has to stop his work and go to the nearest plant communication point to contact back the control room. However, there are parts of the plant where field operators do not hear the first call, and sometimes they cannot stop their work immediately. Pagers or cellular phones are not allowed in the plant.

When some operational intervention is needed (change state, tests, emergencies) the foreman in charge reads the corresponding procedure to the RO and SCO. He also browses the procedures and full checklists, characterizing a nominal operational mode (see fig. 7). In this mode, the RO and SCO verbally confirm the instruction received, look at the controls—mainly the CRT displays—actuate the controls if needed, and verbally inform the foreman of the action taken. When the plant response is according to the procedural steps, the operators follow this mode. If something goes wrong, a more flexible and cooperative mode emerges, which includes more people such as field operators, I/C personnel, etc., as we will see in next field study.

3.2. Study 2: Plant Shutdown, Start-Up, and Simulator Training

In this study our aim was to examine the communications through which operators deal with micro incidents (MI; Bressolle, Decortis, Pavard, & Salembier, 1996) during their actual work activities, and based on that determine whether they use a cognitive strategy based on formal constructs (normative), or a naturalistic strategy. Micro incidents are any event that provokes a rupture with the normal operation (the nominal operation mode, see Figure 7), sending the operators to work in a new type of practical rationality. Micro incidents are complex entities with four basic properties: singularity, unpredictability, importance (the discriminator value from one event can be classified an MI), and immanence to the situation.

3.2.1. Procedure. In this study we used more than the paper and pencil for field notes. Audio and video recorders also were used. According to the naturalistic research approach, the operators received only one instruction: behave as normally as possible despite the presence of the analysts in the control room (this became easier because operators already knew the study procedure and some of the analysts from the pilot study). The procedure consisted of three phases: (a) data collection, (b) data preparation, and (c) analysis.

3.2.1.1. Data collection. We used three video cameras inside the control room and micro recorders in the pocket of the four control room licensed operators. From experience from the first study, and due to the shared characteristic of the operators' activities, we used four analysts at this time (two with nuclear operation background). We chose the planned shutdown and start-up of the power plant as the observation period, because during this period many activities must be done in a short time and the possibilities of MI emergence is greater. Beside that, during this period, the operators must deal with many procedures (e.g., operational and test procedures, task planning) at the same time. During work interval periods, interviews were carried out to probe certain decisions more closely. We asked questions like the cues used to make a situation assessment, the goals at particular parts of the procedure/micro incident, whether any other courses of action were considered when making a particular intervention decision, or whether the situation faced reminded them of any previous experience.

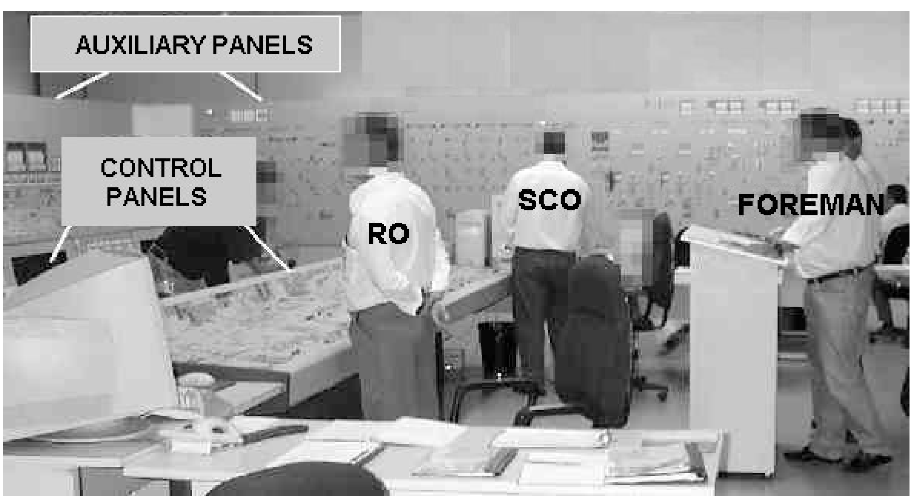

Figure 7 Nominal operational mode.

To observe the operators dealing with postulated accidents, we also observed two sections of simulator training in the plant simulator facility.

3.2.1.2. Data preparation. Both the verbal protocols and the debrief interviews recorded during the observation period were transcribed in chronological order, identifying the operator(s) and the other people who talked with them. The other set of data was a list of the entire micro incidents perceived by the analysts. To construct the MI list, the first step was the concatenation of the analysts' event field notes. Because each analyst followed one operator, we got from the field four lists of events. Some events were perceived by only one analyst, whereas others were perceived by all. After this concatenation procedure, we had tables with the chronological description of all events. The selection of some of these events as MIs was based on the MI relevance for the research objectives. After MI selection, we searched for all verbal protocol transcriptions related to each MI, from the start of observations (with some MIs, discussions related to the situation were noticed before the event, during the shift changeover for example).

3.2.1.3. Data analysis. A classification of the oral communications in cognitive strategies was carried out through coding exercises. The main purpose of the coding exercises was to fit the MIs' verbal protocols into basic categories to identify the reason for the interventions and the role of the communications. Table 1 shows the coding scheme used. The evidence from the debriefing interviews was used as a check on the classifications made based on the coding scheme. The analysis was conducted following the principles of protocol analysis (Ericsson & Simon, 1993) and content analysis (Krippendorff, 1980).

TABLE 1. Codification Scheme

Category	Definition
Intervention/decision	The decision taken in order to change the prescribed course of action (CoA).
Operator	Who made the decision.
Input	Information leading to an altered assessment needing a solution. Identification of when the problem-solving related topic was introduced, and what new factors caused the change.
Instigated by	Who identified the need to tackle the problem.
Involved	Team members involved from problem identification to decision making.
Goal	The objective of the decision. Stated verbally, or inferred by the researcher.
Reason	Based on the goal. For example, the goal may be to shut down the process, the reason was to minimize escalation potential. Could be verbally stated but often had to be inferred.
Options and consequences	Options available as alternative means of solving the problem. The consequences referred to what would happen if these options were selected. Options and consequences could be stated but mostly had to be inferred.
Time	The time taken from when the problem was identified until the decision was made.

3.2.2. Participants. Three operator crews, among the five who participated in the pilot study, participated in the second study, during the shutdown and start-up of the reactor. We observed one crew during the reactor shutdown for 12 hours, another crew for 9 hours in the execution of prestart-up tests, and the last one during the reactor start-up from criticality to full power, for another 9 hours. Two other (different) crews were observed during simulator training sessions.

3.2.3. Second study results. Table 2 presents some of the MIs identified during the plant shutdown, start-up, and simulator training that will described in turn.

We will now describe in a systematic way the MIs, presenting (a) the context of operation at the moment of the MI, (b) the communication protocols gathered, (c) the problem characterization as delineated by the codification scheme, (d) results of debriefing interviews (when available), and (e) a list of the relevant documentation.

3.2.3.1. MI–1: The boiler start-up.

1. Context of operation: The nuclear reactor shutdown process. This process involves reduction of reactor power from full power to the subcritical cold state—all control bars dropped inside the reactor core, primary circuit temperature 50°C, and atmospheric pressure in the primary circuit. It takes about 7 hours from the moment of the reactor trip (control bars inside the core) to the reactor subcritical cold state—the end of the shutdown process.

   The boiler is needed during the shutdown of a nuclear reactor to provide steam for some utilities after the reactor trip, when the main heat source is lost. The boilers (the plant has two redundant boilers) are equipment used only sporadically and when they are needed (as in planned shutdowns) they should receive special attention (maintenance, tests) in the previous shift to be ready for operation. This was the situation in this planned shutdown, according to the dialog below during the shift changeover, just before the shutdown.

TABLE 2. The Micro-Incidents (MIs)

Reactor shutdown—Crew 1	Pre-start-up tests—Crew 2	Increasing reactor power—Crew 3	Simulator training Crews 4 and 5
MI–1Boiler 1 start-up	MI-4 Incompatibility between Procedure requirements	MI-6 Limitation system parameter oscillation	MI-8 Use of EOP procedures
MI–2 Instrumentation tests	MI-5 Key operation on the control desk	MI-7 Leakage in MKF tank	
MI–3 Reactor heat removal circuit blockade after pump shutdown			

2. Communication protocols.

Foreman going out: "Boiler 1, changing the probe."
SCO: "Is it finished?"
Foreman going out: "It's done. It's being tested."
SCO: "It is being tested. The operator will be done . . ."

Two hours later, we saw another operators' attempt to get conclusive information about the boiler final operational status:

PO: "Was Boiler 1 finished . . ."
SCO: "Yes."
Foreman: "So . . . theoretically it is available."
SCO: "But is it still hot?"
PO: Ok! I'm going to start warming it up."
SCO: "Because we will need the boiler soon, sometime in the early morning."
PO: "I'm going to start up Boiler 2."

The MI emerged 2 hours later. The time to connect the boiler in the circuit arrived and Boiler 2 did not start. As a result, Boiler 2 cannot be used anymore; if Boiler 1 did not start, the shutdown process must be stopped. At this moment, we got the transcription below:

Supervisor: "Look at the condition of this f. . .ing boiler! What is going on there?!
Thirty minutes later PO returns from boiler area.
PO: "There is a scaffold down there that was put there to hold up the tubes (interruption)"
Supervisor: "Why should this keep the boiler from starting?!"
PO: "No reason, nothing."
Supervisor: "OK, so let's start the boiler!"

Boiler 1 started, and MI was closed without any further problem.

3. Problem characterization. Tables 3 and 4 present the coding tables for the two main interventions related to the boiler MI.
4. Results of debriefing interviews. The PO who made the first decision did not participate in the interview, only the licensed operators. Asked why they tried to warm Boiler 2, the operators said that it was because of the scaffold near Boiler 1. Normally maintenance people remove scaffolds after they finish the service. They viewed this decision as an additional safety concern, to avoid the start-up of equipment in maintenance. The SS (shift supervisor) explained that is why he made the final decision only after sending the PO into the field. Asked why they did not take for granted the information about the Boiler 1 in the Work Permit document, they replied that, if there is a doubt (the scaffold), additional checks become necessary.
5. Relevant documentation: The shutdown procedure indicates when the boiler will be needed during the shutdown; the Work Permit document indicates that the maintenance of the Boiler 1 was finished. Maintenance procedures indicate that at the end of the maintenance services all maintenance tools must be removed.

TABLE 3. Boiler Micro-Incidents First Intervention

Category	Description
Intervention decision	Start up Boiler 2.
Operator	Panel operator
Input	Need to have at least one boiler available.
Instigated by	SCO
Involved	SCO, PO, foreman
Goal	To have a warmed boiler when needed, according to the shutdown procedure timing.
Reason	Due to the scaffold near Boiler 1, PO had doubts about Boiler condition.
Options and Consequences	To identify Boiler 1 actual conditions. If Boiler 1 was OK, warm and start Boiler 1.
Time	35 seconds

Note. SCO = secondary system operator; PO = panel operator.

3.2.3.2. MI–2: Instrumentation tests.

1. Context of operation. These MIs were related to the interference of the instrumentation tests in the reactor refrigeration process during the entire shutdown period. According to the shutdown task schedule, instrumentation tests should be initiated just after the reactor trip at 2330. However, the test procedure indicated that the

TABLE 4. Boiler Micro-Incidents Second Intervention

Category	Description
Intervention decision	Start up Boiler 1
Operator	SS
Input	Boiler 2 failure Boiler 1 condition verified. Boiler 1 available.
Instigated by	PO, who went to the boilers area.
Involved	PO, SCO, foreman, field operators (in the area)
Goal	To have a warmed boiler when needed, according to the shutdown procedure timing.
Reason	Supply steam for plant components during shutdown.
Options and Consequences	If Boiler 1 does not start, stop reactor shutdown process. Delay on the task schedule.
Time	30 minutes

Note. SCO = secondary system operator; PO = panel operator; SS = shift supervisor.

tests should be done only when the reactor reached the subcritical cold state. The subcritical cold state would only be reached after at least 6 hours from the reactor trip.

2. Communication protocols.

Instrumentation technician arriving in the control room: "Is it shut down? Can we proceed . . . ?" (with the tests)
Supervisor: "The reactor has been turned off. What do you need for the test?"
Instrumentation technician: "It has to be in a subcritical cold state."
Supervisor: "Well, it will not be cool until around 5. Right now it's in hot subcritical state."
Instrumentation technician: "Well, for this test . . ."
Supervisor: "Now what we have to check is how this test affects the primary circuit. . .
Take a look at the test. . .sees what conditions are really necessary to meet these requirements. . ."

Five minutes later, the instrumentation technician returned.

Supervisor: "Can we do it or not?"
Instrumentation technician: "The test we're going to do is just the part on train 1 . . . signals that are changed on the limitation system rack for train 1 . . . For limitation to work, we would need to have. . . 2 of 3 . . ." (interruption)
Foreman: "2 of 4, . . . but the reactor is already shut down! I don't care if the limitation system is on. . . The reactor is shut down."
Instrumentation technician: "The problem is that the test is . . . I doubt that most of it has been invalidated.
Supervisor: "Ok, Let's go. Get out of the control room. I have many things to do! I can't stay up with you all night!"
Just after the beginning of the tests, the control room was full of alarm sounds. The dialog below shows the situation:
Supervisor: "Wait a minute! What's going on here?" (referring to the alarms)
Foreman: "This business of starting the test . . . , the alarms go off all the time, man."
Supervisor: "We are in trip risk, right!" (laughing)
Supervisor: "I want to tell you something. To be in here with this sound going off is awful! Lets turn the alarm in the rack off!?"

The only way to turn off the alarm ring is an intervention inside the automation rack, which constitutes a routine violation. Beside the alarms, operators had problems with the automation system.

RO: "We don't know if the stoppages occurred because of the test or because of a real problem at the plant."

Two hours after the authorization (2 a.m.), the supervisor, pressured by the other operators, decided to stop the tests. Two hours later (4 a.m.), when the reactor heat removal was in operation, the supervisor tried the tests again but the same problems came up, and at 5:15 a.m., the supervisor stopped the tests for the second time.

3. Problem characterization. Tables 5, 6, 7, 8 and 9 present the coding tables for the authorizations and suspensions of the instrumentation tests.
4. Results of debrief interviews. During the shutdown process, just after the second test suspension, the supervisor answered some questions about the tests.

Analyst: "Let me ask a question. Now, do you do the tests only with 50°C?"
Supervisor: "Look, at 0700 a new SS will decide about the tests, do you understand?"
Analyst: "What is the difference between work to with 90°C (the current temperature) or 50°C?"
Supervisor: "The problem is: Now I am refrigerating. Then, to refrigerate, I need to add water in the primary circuit with the RHR (Reaction Heat Removal System) in service. Then, there are many systems entering in service to reach the 50°C condition of the plant. However, when I put these systems in service, they receive signals to stop, to close valves. Do you understand? This is what is happening! I don't know from where these signals are coming! In addition, this only begins when I authorize tests. I cannot even say for sure that the tests are the cause. The only thing I know is when the tests start this begins (pause). At that time (referring to the first test suspension) I suspended the tests and the signals stopped."
Analyst: "At that time the RHR was out, wasn't it?
Supervisor: "Yes, the RHR was still out of operation."
Analyst: "Then, is it the test effect?"
Supervisor: "Exactly. Then the alarms go on, a lot of alarms, ventilation, and blockade. Then man, it is crazy. We cannot concentrate ourselves in the refrigeration procedure, keeping the refrigeration rate (primary circuit temperature/hr). For example, now the people have to be concentrated in only one thing: to guarantee that I

TABLE 5. Authorization for the Limitation System Test

Category	Description
Intervention decision	To authorize the execution of the limitation system test just after the reactor trip.
Operator	Supervisor
Input	Shutdown task schedule—tests at 2330. Test procedure—subcritical cold state—at least 6 hours later.
Instigated by	Instrumentation technician
Involved	SCO, foreman, instrumentation technician
Goal	To carry out the limitation system test.
Reason	Safety systems must be tested periodically.
Options and Consequences	To wait until the subcritical cold state according to the test procedure. Do not accomplish the task schedule. Instrumentation technicians should wait 6 hours to start their work.
Time	10 minutes (2335 to 2345)

Note. SCO = secondary system operator.

TABLE 6. Authorization for The Pressure Transducer Tests

Category	Description
Intervention decision	To authorize the execution of the pressure transducers tests just after the reactor trip.
Operator	Supervisor
Input	Shutdown task schedule—tests at 2400. Test procedure—subcritical cold state—at least 6 hours later.
Instigated by	Instrumentation technicians.
Involved	SCO, foreman, another 2 instrumentation technicians.
Goal	To carry out tests on the pressurizer pressure transmitters.
Reason	Safety instrumentation channels must be tested periodically.
Options and Consequences	To wait until the subcritical cold state according to the test procedure. Do not accomplish the task schedule. Instrumentation technicians should wait 6 hours to start their work.
Time	15 minutes (2405–2420)

Note. SCO = secondary system operator.

will never refrigerate with a rate lower than 50°C/hr (according to the shutdown procedure). Then the people (operators) are getting crazy with this situation! When the plant temperature reaches the 50°C there will be nothing more to do here in the control room. It is just to keep the 50°C. You can have alarms and so forth, nothing

TABLE 7. First Suspension of the Tests

Category	Description
Intervention decision	To stop the execution of the instrumentation tests.
Operator	Supervisor
Input	RO lost the pressure indication on the CRT—the channel under test was the one he monitored. Alarms in the control room.
Instigated by	RO
Involved	Supervisor, RO, foreman, instrumentation technician
Goal	To avoid annoyances to the operators.
Reason	To restore the operational conditions during the rest of the reactor refrigeration process.
Options and Consequences	To continue with the tests. To jeopardize refrigeration process. To be under growing pressure by the operators.
Time	80 minutes (from 2430 when the alarms started up to 0150 when the SS stopped the tests)

Note. RO = reactor operator.

TABLE 8. Authorization for Tests After the Start of the Reactor Heat Removal (RHR) System

Category	Description
Intervention decision	To authorize the tests again.
Operator	Supervisor
Input	Supervisor experience. He thought that after the beginning of the operation of the RHR the tests could be resumed.
Instigated by	Instrumentation technicians, task schedule.
Involved	Supervisor
Goal	To do the tests.
Reason	To carry out the planned tasks.
Options and Consequences	To await the subcritical cold state. Do not accomplish the task schedule.
Time	The first instrumentation test was authorized again at 0330 and at 0434 the SS authorized all the tests.

Note. RHR = reactor heat removal system.

matters! Just look at the refrigeration system temperature, nothing more. Do you understand? Now, a clear explanation for what happened tonight I don't have, you don't have, and nobody has! The (foreman's name) is completely crazy, poor guy. He cannot convince me, as I cannot convince him either."

TABLE 9. The Second Test Suspension

Category	Description
Intervention decision	To stop all the tests.
Operator	Supervisor
Input	Alarms and blockades on the RHR system.
Instigated by	Foreman, RO, SCO.
Involved	Foreman, RO, SCO, instrumentation technicians.
Goal	To avoid spurious blockades on the RHR to finish the reactor refrigeration process on time.
Reason	The operators associate the blocks on the RHR water injection circuit to the limitation system test.
Options and Consequences	To continue with the tests. To jeopardize refrigeration process. To be under growing pressure by the operators.
Time	45 minutes. The first water injection blockade occurred at 0448. At 0533 the SS stopped the tests for the second time.

Note. SCO = secondary system operator; RO = reactor operator; RHR = reactor heat removal system.

At this moment, the SCO participated on the conversation.

SCO: "What?"
Supervisor: "We are talking about the tests."
SCO: "No, this problem (water injection blockades), is a problem that happened in the beginning of phase B (pause), no not in the phase B. In that part, start and stop the plant (commissioning tests), this had already happened. Do you understand?"
Supervisor: "I know, I know."
SCO: "It is a problem that we already know about! We have a serious flux measurement problem."
Supervisor: "I know this I know."
SCO: "This is because the system, in the way that it was designed, it is very critical. And, the transmitters we have out there are old transmitters, without many resources."
Supervisor: "I understand."
SCO: "So, this problem appears only when you have water injection. And, during normal operation, you don't have water injection!"

In debrief section, when asked why he authorized the tests, the shift supervisor explained his rationale:

Those tests, I would not have authorized, OK. I would not have authorized! However, people tried to do the tests, although they should be done when the plant is in subcritical cold state. In the test procedure, this is one of the requirements. Nevertheless, the plant tried to do the tests, in advance. Because we have a very short outage period! In such way, I took the challenge and I authorized the tests. But in the middle of the problems I felt that was impossible and I ordered to stop.

5. Relevant documentation: The shutdown procedure indicates the moment when subcritical cold state should be achieved and what systems were in operation during the reactor shutdown; the task schedule indicates when the tests should be carried out; tests procedures indicate the state of the plant to carry out the tests.

3.2.3.3. MI–3: Reactor heat removal circuit blockade after pump shutdown.

1. Context of operation. In the final phase of the reactor heat removal process, two of the four reactor refrigeration pumps have to be turned off (in this phase they become the main heat source). Just after the operator turned off the pumps, one of the three reactor heat removal circuits in operation was unexpectedly blocked by the automatic system, configuring the MI. The operators realized that the block was due to the overlap in the shutdown curve pressure limits. For some unknown reason to the operators, the pumps shutdown caused a slight increase in the pressure (33 to 36 bar), enough to trigger the automatic system (the set point is 34 bar). This occurred at the end of the shift, and operators from two operation crews discussed the problem and the strategy to restart the refrigeration circuit. They discussed two options: to open the breaker to bypass physically the interlock, or to lower the primary circuit pressure using the spray system.
2. Communication protocols.

Arriving RO: "We saw that thing before, and we reached the conclusion: The measure is in the hot leg in the circuit that was turned off, then you discharge the pressure of the other pump. That is clear, when you turn off the pump; the pressure of the circuit which is off becomes higher."

Arriving foreman: "I read in the Science Description [part of the plant's technical specifications] that the core ΔP is 3 bar. Now, we have 2 bars lower, it is possible, it is colder."

Arriving RO: ". . . last time what we did was lower the primary pressure here."

Arriving foreman: "I told him I would like to do so, but he (the arriving shift supervisor) is not sure."

Arriving RO: "It can be lowered manually! Look, I know a trick that you can use to get control with lower pressure."

Foreman leaving: "You gonna cheat the big brother, aren't you?" (laughing)

Leaving foreman: "We have done our job in a right way. You see, it is 69 °—to get to 50 by 11 a.m., I think is reasonable. . ."

Leaving RO: "But it's been some time . . . and its not getting any cooler."

Arriving foreman: "Ask him to open up over there; the guy is in a hurry!"

Leaving RO: "Tell them over there to open the breaker."

Arriving foreman: "Wait! We are not getting a reading . . . the pressure is still too high!

Leaving foreman: "I think it's high, too. We will have to drop the pressure a little. I will talk to (supervisor name)."

Leaving foreman: "The (RO name) says that this problem has happened before with him. He also said that they lowered the pressure manually . . . in the core. We switch to manual, spray, and later we go back. . . it's just to bypass the block. . . and to come back with the JN (heat removal circuit)."

Arriving supervisor: "OK. Let's go."

3. Problem characterization. Table 10 presents the coding table for this MI.
4. Results of debrief interviews. Commenting on the question, "You gonna cheat the big brother, aren't you?"—The operators express their concern about the automation system. Sometimes they simply don't know what is going on. A vendor consultant (an experienced operator from the plant supplier country), who also participated in the interview, said he had never seen such an event during the plant shutdown. He also explained that they use a different procedure format, with less-detailed instructions and requirements. Asked about what to do to avoid the repetition of this problem in other plant shutdowns, the operators talked about the accuracy of the pressure sensors and about the set point—34 bars—which seems to be too close to the real pressure, at this moment of the shutdown process. However, they will not formally propose corrective actions in the Shift logbook.
5. Relevant documentation: The shutdown procedure indicates the refrigeration rate 50°C/hr that should be followed. The plant technical specifications where the operators search for the reasons behind the pump trip (the plant is not allowed to be operated out of the limits given by the technical specifications). The Shift logbook is where the operators note what happens, but not why it happens.

3.2.3.4. MI–4 Incompatibility between procedure requirements.

1. Context of operation. During the plant prestart-up tests, a different operator crew follows the procedure to carry out the primary circuit leakage test, needed before

TABLE 10. Reactor Heat Removal Circuit Blockade After Pump Shutdown Micro-Incidents

Category	Description
Intervention decision	Lower primary circuit pressure using the pressurizer spray system.
Operator	Two operator crews during shift changeover
Input	Blockade in reactor removal circuit due to high pressure.
Instigated by	Supervisor, ROs, SCOs, foreman
Involved	Supervisor, ROs, SCOs, foreman
Goal	Resume the operation of the heat removal circuit, which was blocked, due high pressure.
Reason	To follow the shutdown procedure, keeping the primary circuit refrigeration rate at 50°C/hour.
Options	To open the circuit beaker in the automation rack. To do nothing and wait.
Consequences	1. To commit a violation, changing the automation connections. 2. Do not accomplish with the refrigeration tax requirement, wait more time to reach the subcritical cold state.
Time	10 minutes of discussion

Note. SCO = secondary system operator; RO = reactor operator.

the reactor start-up. In the test procedure, a pump must be electrically disconnected. However, if the operators electrically disconnect the pump, they have to execute the pump test again (it had been done the day before) and that takes about 8 hours.

2. Communication protocols.

Foreman: "What is the relationship between the Operation Manual, blocking this thing and the test (pause)? We are doing this test in the same region of the Operation Manual. (If). . . you are here, at this point, then he (the procedure writer) knows that the valve has already blocked it. Theoretically, the person who wrote the procedure . . . knows the plant condition. Then it would be redundant with what is written here. I am wondering if this double block is really necessary or if there is something else involved. . . blocking both the pump and the valve. What is his (the procedure writer's) primary concern?"

RO: "He is not asking for the valve, in here, no."

Foreman: "I know. The valve he is talking about is here . . . in the Operation Manual. He says that this valve has to be closed during the test. Because like he says, the valve has to be open after the test. During the test, it has to be closed. Then, why, if it is already closed there, did the guy insist that the valve be electrically disconnected!?"

3. Problem characterization. Table 11 presents the coding table for this MI.
4. Results of debrief interviews. This MI was not addressed in the debriefing interview.

TABLE 11. Incompatibility Between Procedure Requirements Micro-Incidents

Category	Description
Intervention decision	Do not follow the test procedure requirement—electrically disconnect the pump.
Operator	Operator crew
Input	Incompatible requirements in three documents: test procedure, task schedule and operation manual.
Instigated by	Operator crew
Involved	Operator crew Instrumentation technicians, supplier consultant.
Goal	To do the test without electrically disconnecting the pump.
Reason	If the operators electrically disconnect the pump, they have to carry out the pump test again.
Options and Consequences	To follow the test procedure and repeat the pump tests. Delay in the shutdown schedule.
Time	30 minutes discussion

5. Relevant documentation: The test procedure requirement—electrically disconnect the pump—would imply in the repetition of the pump test carried out the day before according to the task schedule. According to the Operation Manual the pump was already isolated (valve closed).

3.2.3.5. MI–5 Key operation on the control desk.

1. Context of operation. During a plant start-up test, a key in the control desk must be locked in one position. The operators believed that the key should have a lock mechanism, because according to the test procedure, it must be in locked in the position during the entire test. This MI covers a set of practically identical decisions, taken by many operators that manipulated the key trying to discover its operation mode.
2. Communication protocols.

Foreman: “So, lets go 540 there, 541, 542, 543 no energized. . . Oh!?” (surprise with an unexpected system answer)
RO: “What? Wait a minute . . . Why is it turned off?”
Foreman: “Did the key go back to the position?”
RO: “It did?!”

The cause of the problem was identified: The control key did not remain in the correct position.

Supervisor: “It (the key) has to be locked?” (To be locked in the last position.)
RO: “It comes back.”
Supervisor: “No, he did this, look! . . . he did this!” (Repeating the operator manipulation on the key.)

Foreman: "Look if it came back there?"
Supervisor: "Yes . . . it did not lock, it came back. When he released, it came back!"

After that, all operators manipulate the key trying to figure out its operation mode. According to the function in this test, it should be a retention key; however, it was not.

RO: ". . . he . . . keeps it lower, locked."
Supervisor: "I think he didn't succeed. Wait a minute let us see. He suggests that when he loosened, it returned. You told him to keep locked . . . then he loosened and the thing goes back. It seems that it doesn't lock!?"
Foreman: "It came back! What?"
Supervisor: "Wait a minute, let him take a look. (RO name), you try to lock the key in the low position."
Foreman: "Look! We have to press and lock it. See, you have to press and lock in the position!"
Supervisor: "Has it retention? When you loosen is there any lock? Let me see if it locks after pressing!"
Foreman: "No, no, keep it pressing in the lower position . . ."
Supervisor: "It doesn't lock! Doesn't lock! He has to be holding it then. . . (Pause). He has to be holding the key, it is the only way! . . . While they make the test. . . if they don't take a long time . . . It doesn't lock. It seems there is no retention mechanism."
Foreman: "Will we really have to hold it during the entire test?"
Supervisor: "Until he (instrumentation technician working in the test) disconnects . . . after that you can release"

3. Problem characterization. Table 12 presents the coding table for this MI.
4. Results of debriefing interviews. The operators were not sure if there is any other practical step (besides manipulating the key) to find out how the key operates. When

TABLE 12. Key Operation Micro-Incidents

Category	Description
Intervention decision	To be holding the key for about 30 minutes during the entire test.
Operator	RO, SCO, foreman, supervisor
Input	Test procedure: the key must be locked during the test.
Instigated by	RO, SCO, foreman, supervisor
Involved	RO, SCO, foreman, supervisor
Goal	To lock the key in the position indited by the test procedure.
Reason	To find out if the key has a lock mechanism.
Options and Consequences	To find out the key specification in the documentation. It takes more time to search on the documentation.
Time	10 minutes

Note. SCO = secondary system operator; RO = reactor operator.

asked about why they did not try to consult the key specification documents, the RO said: “This information we could find in the (pause); probably in the control desk specification . . . but look how many keys we have and the size of that book! Certainly it will take much more time if we search things like this in the paper specifications.”

5. Relevant documentation. The test procedure indicates the position of the key during the test. Key specification (not used, it was not easily available).

3.2.3.6. MI–6 Limitation system parameter oscillation.

1. Context of operation. Another crew was in charge of this phase of the reactor start-up process. During the reactor power increase (12.5%), an oscillation occurred in a limitation system parameter, and the RO stopped the start-up procedure.
2. Communication protocols.

RO: “It is oscillating, man! . . . The problem has started . . . look! . . . From 12.5 it went to 28! When it was in 12.5 it should have been changed to 17.5 and it didn’t move . . . it was stuck! And you could see that only if you were passing by. From that point, it went to 28, and . . . Now it is oscillating around that. Look!”
Supervisor: “Did it come back? It came back to 20.”
RO on the phone: “Do you think we can increase the power a little bit to avoid the oscillation? (pause). The flow is low, very low! No, it isn’t normal! The flow has to rise by more than 10%; otherwise we will not get out of the oscillation point. (pause) OK, but to increase the flow, we have to increase the power! (pause) OK, by how much, more or less? OK, bye.
RO: “(Supervisor name), he suggested increasing the power by 5%, to see if the feedwater flow increases by enough to get out of the low zone.”
Supervisor: “OK. Increase the power.”

3. Problem characterization. Table 13 presents the coding table for this MI.
4. Results of debriefing interviews. The SS explained his decision—increase 5% in the power to see if the oscillation stops—based on the limitation system characteristics and time schedule. The limitation system is conceived to operate only when the reactor reaches full power. The system purpose is to lower the reactor power to 70%, before the actuation of the shutdown system, avoiding unnecessary reactor shutdowns. Thus, he does not consider an oscillation in low power a major problem. Furthermore, the limitation system is one of the most complicated systems of the plant and a detailed investigation about low power problems would take a lot of time. The SS also explained that if the oscillation continued after the 5% power increase, he would stop the reactor start-up, and call for the engineering people help.
5. Relevant documentation. No documentation was used.

3.2.3.7. MI–7 Leakage in the MKF tank (MKF is a tag name for the tank without specific meaning).

1. Context of operation. During the reactor power increase process (reactor power around 33%), the field operator detected a leakage in an auxiliary tank. An automatic

TABLE 13. Limitation System Parameter Oscillation Micro-Incidents

Category	Description
Intervention decision	To increase reactor power by 5%.
Operator	Supervisor
Input	Oscillation in the limitation system parameter.
Instigated by	SCO
Involved	Supervisor, SCO, instrumentation technician
Goal	To stop the parameter oscillation.
Reason	To gets out of the low zone flux that seemed responsible for the oscillations.
Options and Consequences	To stop the reactor startup. Call for a detailed investigation about the limitation system behavior. Delay in the startup schedule.
Time	15 minutes

Note. SCO = secondary system operator.

shutdown (reactor trip) could occur due the low MKF level. The MKF tank level does not have an alarm window in the control room. The strip chart register located on the auxiliary panel presented the MKF's level indication.

2. Communication protocols.

SCO answering the phone: "Control room speaking . . . How critical is it? . . . Who is talking? . . . OK, bye."

SCO calls for supervisor: "Problem (supervisor's name)! The MKF's water is going down! Nobody knows from where! We have a trip risk!"

Supervisor: "Can we fill the tank, while we find where the leak is?"

The Supervisor immediately suggests an alternative to avoid the trip: to fill up the tank.

SCO: "MKF. . . No, not yet . . . we . . . but on the way it is going down, we have trip risk there."

Foreman: "The other time, it was a hose, do you remember?"

SCO: "Yes. It was the conductivity meter's hose, but there was a conductivity meter there. Look out there (pointing to the auxiliary panel) there is a level indicator. How bad is it (pause) . . . Yes? Is it going down too fast?!"

At this moment, operators, instrumentation and maintenance technicians went to the auxiliary panel to look at the MKF level behavior and the SCO answered a distracting phone call.

SCO on the phone: "Hi, talk! . . . Wait a minute, I cannot talk to you now. Call me later. Bye."

SCO called another field operator.

SCO on the phone: “Give me a break; go to MKF because the level is going down faster! I know that (name) is already there, but help him, otherwise, we will have a trip soon! OK, bye.”

While the SCO tried to find out where the water was leaking from, by sending more people to the tank neighborhood, the supervisor continued searching for ways to fill up the tank.

Supervisor: “There is an input here, look! But, I am not sure if it is to fill up the tank. There must be some place to fill water in this sh. . .t!”
SCO: “Where is this water going to?” (The SCO was still trying to understand the leak).
Supervisor: “No, the problem is . . . Until we discover to where the water is going—this is GHC input—we will have a trip!”

They did not have a trip. The field operators found and corrected the source of the leak—a drain valve that remained open after maintenance work.

3. Problem characterization. Tables 14 and 15 present the codification for the operators’ actions in this MI.
4. Results of debriefing interviews. The different approaches used by the supervisor and SCO were presented to the operators. In the first moment, they were surprised with the findings, considering that there was no different approach among the crew-members. After some reflection, they agree with the differences as the SS said: “As

TABLE 14. Leakage in the MKF tank: Fill Up the Tank

Category	Description
Intervention decision	To fill up the tank.
Operator	Supervisor
Input	MKF level going down, trip risk.
Instigated by	Field operator.
Involved	Supervisor, SCO, foreman, field operators
Goal	To restore the level of the tank.
Reason	To avoid reactor trip.
Options and Consequences	To identify the problem causes. If it took to much time, a reactor trip would occur.
Time	1 minute

Note. SCO = secondary system operator.

TABLE 15. Leakage in the MKF Tank Micro-Incidents: Identify the Leakage

Category	Description
Intervention decision	To identify the problem cause.
Operator	SCO
Input	MKF level going down, trip risk.
Instigated by	Field operator
Involved	Supervisor, SCO, foreman, field operators
Goal	To stop the leak of water.
Reason	To avoid reactor trip.
Options and Consequences	See Table 14 (to fill up the tank). If the water leak was not stopped, the water could damage other equipment located nearby.
Time	20 minutes (up to the moment the leak was stopped)

Note. SCO = secondary system operator.

a shift supervisor, I am responsible to keep it (the plant) working; I have to talk with the plant manager . . . They (the reactor operators) are more concerned with the operational processes."

5. Relevant documentation. No documentation was used.

3.2.3.8. MI–8 Using emergency operating procedures (EOPs).

1. Context of operation. This MI was observed during the simulator training. When dealing with postulated accidents in the simulator, the operator actions should be based on the instructions, rules, and checklists contained in the EOPs. EOP use begins just after the reactor trip. They are used (a) to identify the accident type, and (b) to mitigate the consequences. The communication protocol below starts when the simulator instructor went to the control room to talk with the operators.
2. Communication protocols.

Instructor (pointing to the P × T curve in the computer): "Take a look at here! What is the temperature? Look at this temperature here! 296.5°!"

Instructor: "Look at what it (the procedure) is saying there. It is saying that you should keep that difference to avoid saturation. The pressure is around 80. . . If you order to lower that pressure still more. . ."

The instructor's intervention was motivated by the fact that the operation team continued to reduce the pressure, that was at 81.6 bar, to 80 bar, as indicated in the procedure.

Supervisor: "The procedure orders to lower to 80, we are in 81.6. I am just adjusting according to the procedure!"

Instructor: “Here, it cannot go down anymore! Do you remember what we discussed yesterday? (During the briefing). I think that the procedure is wrong. Look! You have 81 bar in the primary. Which is the saturation temperature for 81.6 bar?! You are subcooled according to the indication. . .”

Supervisor: “Slightly subcooled.”

Instructor: “Now, what does the procedure say about the steam in the primary side? The temperature of the tubes of this isolated SG (steam generator) is 296°. Which is the saturation pressure? (Pointing to the P $\times$ T curve in the computer). Then, if you lower this thing still more. . .!? Because of this, I am saying that there is something wrong in this procedure (the steam generator tube rupture [SGTR] EOP). Yes or no?! In the way that our model is showing, at this temperature, we already have a saturation pressure!”

Supervisor: “The procedure orders to do a thing. . . but should we do other? In the way the things are, if the procedure orders to open, we have to open! Or else we are f. . .ed! Especially me, if I will not be documented!”

Instructor: “The operation has to change the procedures. Otherwise, you will be eternally with wrong procedures!”

SCO: “We are always inside there (the control room)! To do this when?”

Instructor: “But look, independently of what the procedure says, or the people behavior that it is very difficult to understand, this (pointing to the saturation curve) is what is really important for you to understand. Independently of what the procedure says, I want you to understand the situation! Or else, I didn’t need to be here!”

3. Problem characterization. Table 16 presents the codification for this MI.
4. Results of debriefing interviews. A debriefing interview was not carried out after the simulator training.

TABLE 16. The Use of Emergency Operating Procedures (EOPs) Procedure in the Simulator

Category	Description
Intervention decision	To reduce the primary circuit pressure to 80 bar
Operator	Foreman (reading EOP)
Input	EOP instruction.
Instigated by	EOP
Involved	Foreman, SS, SCO, RO, instructor
Goal	To follow an EOP instruction.
Reason	To mitigate the effects of the SGTR postulated accident.
Options and Consequences	Don’t follow the EOP instructions blindly. To analyze also the graphic PxT in the computer screen. Avoid the risk of the saturation (boiling) of the primary circuit.
Time	11 minutes (from the procedure instruction reading to the Instructor’s intervention)

Note. SCO = secondary system operator; PO = panel operator; RO = reactor operator.

5. Relevant documentation. Emergency operating procedure—EOP, related to the steam generator tube rupture accident. In this procedure there is the requirement to reduce the primary circuit pressure to 80 bar (see Figure 8).

4. POROUS COMMUNICATIONS IN THE MICROINCIDENTS

The protocols produced a wealth of data of relevance to cognitive strategies both with regard to the process and to the psychological mechanisms underlying cognitive performance. The results indicate that a limited number of options are available, and that significant cues and goals bound the cognitive strategies used by the operators. This focus on task boundaries corresponded to ideas coming from ecological psychology. According to the ecological approach, it is essential to start by studying the boundaries of the task that are relevant to the performer to understand rules governing behavior (Vicente, 1995). Cognitive economy and goal relevance both play an important part in this theory. People learned the strategy that was most economical for the particular task and thus concentrated on the minimal number of distinctive features that would successfully discriminate among the circumstances of interest (Amalberti, 1996). Training of attention was achieved by abstraction, filtering, and optimization of perceptual search. The process of skill acquisition consisted of adaptation to the constraints imposed by the environment. Experts have learned to work within, and exploit, the set of constraints that define their domain of expertise. We claim that in this situation porous communication plays a fundamental role to overcome the system constraints. The porous communication in each MI will be discussed next.

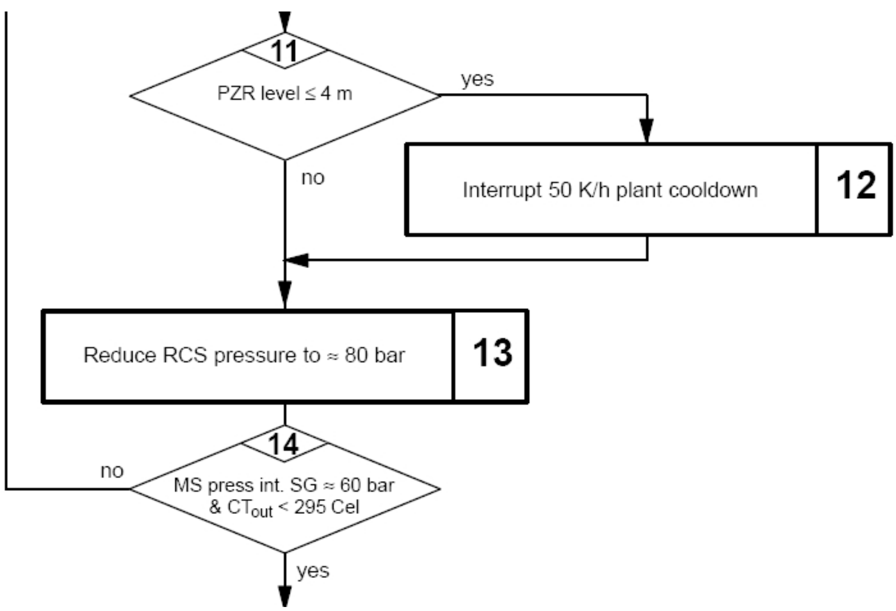

Figure 8 Part of the steam generator tube rupture procedure, which indicates to reduce the reactor cooling system (RCS) pressure to 80 bars.

4.1. The Boiler Problem

As discussed in Section 2.1 porous communications is characterized by the use of vague language and/or fuzzy signals. In the boiler MI, the verbal exchanges are replete of cryptic semantics. Examples are the PO responses about the Boiler 1 state: ". . . theoretically it is available", and the PO action when the SCO committed him to an action: "I'm going to start up Boiler 2" (the entire dialog was about Boiler 1). The reason behind this vague language was the scaffold near Boiler 1—a fuzzy signal (it could indicate that the maintenance service in Boiler 1 was not finished yet). Because of this, a written document (the work permit clearance that should have a clear meaning, indicating the end of maintenance services), also became a kind of fuzzy signal (people were not completely sure if it was correct).

A root cause analysis of this MI would indicate that the main cause was a maintenance flaw, a lack of compliance with the maintenance procedures or maintenance best practices, and the corrective action should be to stress the importance to follow procedures and best practices.

Our analysis shows that the operators deal with such procedure noncompliance using improvisation and porous communication. Although the PO improvised action ("I will start the Boiler 2") initially looks like a bad practice because operations must be meticulously prepared and not left to fortuitous actions, this PO action, caused by uncertainty (the scaffold), indicated his concerns with the equipment safety (he would not like to start any equipment in maintenance).

After that, the SS demonstrated the same concern, sending the PO to the boiler area before he starts the boiler. In this MI, we saw uncertainty—clearly an unwelcome contribution to safety. On the other hand, we also identified resilience in the operators actions, which is a highly praised safety characteristic for an organization that should be able to adapt to unexpected variability.

The question remains in this MI as to why the control room crew did not attempt to contact the maintenance crew to determine why the scaffold was left in Boiler 1; more specifically, why the SS seems satisfied with the PO answer about the scaffold question ("No reason, nothing."). The problem here was related to the supervisor's multiple roles, both technical and administrative, and the plant operational condition, the shutdown, a period of high workload. At the same time, the SS deal with the boiler problem, the instrumentation tests authorization, a request of the National Electrical Grid to suspend the power reduction and other administrative questions, which do not appear in the narrative presented. In other words, the SS simply had to many things to do. That is why he appeared satisfied with the meaningless PO answer and did not contact the maintenance crew for further explanations about a problem that (regarding the operational point of view) was already solved.

4.2. Instrumentation Tests

In the MIs related to the test authorization, the verbal exchanges appeared reasonably clear and understandable when compared with the previous MI. However, the language used is still vague and replete of fuzzy signals that must decoded. When the instrumentation technician asked for the SS authorization—"Is it already shutdown? Can we proceed?"—they already knew that the reactor was not in the cold subcritical state (experienced technicians of a NPP know that the cold subcritical state could not be reached just after the reactor trip). The real question of the instrumentation technicians should be: Do you authorize the test in the hot subcritical state, against the test procedure that calls for the cold subcritical state? However, this question was never explicitly verbalized. Indeed, if the instrumentation technicians verbalize the question as presented above, they will probably receive a negative answer (test not authorized). The vague language was the way the instrumentation technician reached his objective.

In the presence of written documents with incompatible requirements (task schedule and tests procedures), fuzzy signs were generated and decisions were not taken based on effective information sources (the documents, plant state), but on the mind set of the technicians and SS. The instrumentation technicians want to do the tests to go home as soon as possible, and the SS want to accomplish with the task schedule, as he said in the debrief section: ". . . the plant tried to do the tests, in advance. Because we have a very short outage period!" It is interesting to note that the other operators (the foreman, RO, and SCO) clearly manifested their disagreement with that decision during the entire shift, especially when spurious and nonsense signals appeared in the control panels (". . . the tests began . . . it is alarm all the time man . . .").

The problem that underlines this MI was documents that created a situation where it was very difficult to follow the plan as a script. The written schedule for the outage instrumentation tests was incompatible with the plant operational condition. However, according to the SS statements, the plant management wanted to do as much servicing as possible during this short outage, which explains why so many activities overlap each other in the task plan.

4.3. Reactor Heat Removal Circuit Block

In this MI, the fuzzy signals came from the automation system, blocking the reactor heat removal circuit. We had cryptic exchanges, ". . . I know a trick to get control. . ." indicating a particular and tacit knowledge of one operator, or "You gonna cheat the big brother, aren't you?", when the other operator understood that the "trick" aimed to bypass the automation system. The MI illustrated that the verbal exchanges also have a learning role, sharing among the crews the knowledge about how to deal with unexpected situations (". . . last time we did . . ."). This MI presents some other technical questions: Is the shutdown curve set point too tight? Is there any problem with the accuracy of pressure transmitters? Is there really a need for this interlock at this very moment? If not, in what situations should it be important (because it forces the operators to bypass the automation system)? The problem here is that such technical questions are dealing with automation system design and the philosophy of the reactor control system, and whose answers lie elsewhere in the sociotechnical system (NPP vendor, engineering department, regulator), but certainly outside the scope of the operators. This means that the operators appear to have a nonexplicit assignment to deal with such situations as best as they can.

4.4. Incompatibility Between Procedure Requirements

When the foreman said, ". . . the guy who wrote the procedure . . . knows the plant condition," he means that whoever prepared the test procedure should have specified the tests that need to be done for reactor start-up in a logical order, according to the status of the plant state and the results of previous tests (it makes no sense to test the pumps twice).

Once more, operators faced fuzzy communication due to the incompatibility of timing in the three documents: the Operation Manual, and the test procedure and the task planning instructions. Each one was prepared by a different group of specialists, in different organizations, at different points in time—in completely different contexts; nevertheless, they are supposed to be followed without the need of human intervention (interpretation), and they must be compatible with the rationale of the operation.

At the end of about 20 minutes of discussion, and after checking the engineering/instrumentation diagrams, the operators decided not to electrically disconnect the pump during the test, ignoring the test procedure requirement and acting according to the mutual consensus they achieved through communication.

4.5. Key Operation

The operators expected this key to have a lock position based on the test procedure instructions. The use of any formal help to discover the mechanical characteristics of the key, such as procedures, specifications, diagrams was not addressed in the verbal exchanges (see debrief interview for explanations). The problem was solved based on verbal exchanges together with key manipulations. Once more, communication played a fundamental role to solve a problem caused by a fuzzy signal.

4.6. Parameter Oscillation

In the presence of an unexpected oscillation in the limitation system parameter (a fuzzy signal), the RO halted the reactor power increase process. It is clear from the beginning of the verbal exchange that the RO and the SS had no explanations about the reason for that oscillation. The problem solution came from the instrumentation technician by phone consultation. He suggested increasing the reactor power by 5%, to see if the oscillation stopped.

The oscillating parameter is made up of many signals. One of them is the feedwater flow, which was very low. The instrumentation technician recognizes the pattern, in which small variations in a low flow can give spurious value signals, inferring this might be the cause of the oscillation. The low flow could only be increased by an increase in the reactor power—but the increase in the reactor power was stopped because of the oscillation problem—creating two conflicting conditions.

This MI is an example of collaborative strategies based on verbal exchanges enabling feedback loops to restore the plant operation. It shows that, even in the normative environment of the nuclear power operation, some problems are solved without knowing what actually caused the problem, which means that the problem will continue to exist in the system.

4.7. Leakage in the MKF

In this MI, the control room crew is alerted by the field operator's phone call about a problem that they had not detected yet. The field operator noticed the water leak on the floor near the tank, before the control room operators noticed the water level decrease in the control room recorder. The verbal exchanges showed parallel ways of reasoning: the SS trying to fill the tank and the SCO trying to find the location of the leak.

Once more, communication feedback loops were used to restore successfully the plant operation. The loops were not based on clear information, did not follow specific procedures, and were not even related to each other. While the SS think aloud "There must be some place to fill water in that sh. .t.!", the SCO ask for help in the field, "I know that (name) is already there, but help him." The SCO also tried to found out the causes and consequences of the leak, "Where is the water going to?". Other members of the crew were also involved in the communication loop, e.g., the foreman, who remembered a similar problem, "That time, it was the hose, do you remember?"

4.8. Reduce pressure according to EOP.

This MI shows again that the plant's own written documentation was fuzzy, a fact that the operators should be aware of. The instructor interrupted the training section when the operator set the primary circuit pressure to 80 bars. He told the operators that they must look at P $\times$ T graphic (on the computer screen) before they reduce the pressure to 80 bars, even if the procedure tells them to do so unconditionally. The operator replies, ". . . if we do not follow the procedures we are just f. . .ed."

Following the instructor's rationale, operators have to interpret the written procedure, correct, and complement it to make the procedure an effective guide for action. Therefore, dealing with an actual accident could be a very complicated situation. In a stressful situation, operators are trained to follow procedures and are held accountable if they do not. According to the classic safety engineer paradigm, operational instructions are the result of the capitalization of knowledge and experience: They must be always correct (not fuzzy). This brings a contradiction with the reality of the operation, where the actual work situation demands procedure-reading–then interpret habits, which is not fully accounted for in actual operator-competence parameters.

5. CONCLUSIONS

After safety, planning is probably the most cultivated value in the nuclear industry. This value has its roots in the idea that human error is directly related to human variability and autonomy (Reason, 1990). The NPP operators usually see themselves as careful planners; their identities as experts are coupled with values associated with controlling in advance of a situation (i.e., planning). A senior operator said, "Here, (. . .in the NPP control room. . .) we don't like surprises. Everything is carefully planned." Therefore, the operators do not like to improvise: Ad hoc strategies to deal with unexpected conditions is considered inadequate behavior.

However, our field studies found that operators deal with situations where it is very difficult to follow normal procedures strictly and keep the plant working. The entire MI list presented situations in which the porous communications feedback loops are the way the operators used to achieve a consensual coordination of actions, making their decisions and solving the plant problems.

The verbal exchanges show that communications during the operators' work sometimes are complex, vague, and porous. These verbal exchanges comprise, among other things, sharing knowledge, drawing attention to something, getting authorization to do things, keeping operators informed, solving plant problems, and selecting tasks to action.

Verbal exchanges are crucial for the effective use of written documents like procedures, logbooks, engineering diagrams, work permits, and so forth. Indeed, working in real-time and bounded by environmental constraints, the operators use these exchanges to work in a timely way with the procedures. In MI–5, when the foreman said, ". . . the guy who wrote the procedure . . . he knew the plant condition," he used a verbal exchange to correlate between the written information contained in the operation manual, test procedure, and task-planning schedule. In the instrumentation test authorizations, the written schedules for the instrumentation tests did not show the actual relationships between the plant's operations and the requirements in the test procedures (subcritical cold state), giving the staff (operators, instrumentation technicians, maintenance people) "mixed signals," and the understanding that these tasks were independent of each other. Similarly, the work permit clearance and the scaffold left outside the boiler were incompatible with the prescribed normal practice; thereby producing fuzzy signals that operators must deal with.

Our findings show that people deal with noncompliance during the plant's normal operation by using porous communications to achieve a consensual coordination of actions and behaviors.

From the study results, we can see that the verbal feedback loops enable the very existence of the normative "best" practices like norms, rules, procedures; otherwise, it will be extremely difficult to follow the procedures strictly and keep the plant in operation.

Our results cause an impact in the organization, especially on the operators (careful planners), who did not expect findings like we had. However, the most important lesson learned is that the organization needs to recognize the complex nature of the situation that was to be dealt with. The normative practices, plans and procedures or instructions are paramount, but just some of the resources available for carrying out actions. The fundamental point to be considered is not so much the problem of the plan, or of the procedure, or instruction, but rather the idea that action/cognition calls on other resources, i.e. the material, social, and cultural characteristics of the environment in which events occur and which constitute the situation of the agent(s). As these characteristics can change at any time, to be adapted to them, individuals adjust their actions to the new environmental circumstances using communication feedback loops.

The verbal exchanges involve several participants, including those who are not physically present in the control room, such as the procedure writers, and the maintenance, instrumentation, and engineering people. For instance, the actions taken by the maintenance and instrumentation staff are discussed, e.g., "They worked on it, I don't know what they did with it." There are cases where operators acknowledge that someone is working in some part of the system, but without knowing precisely what they are doing (see boiler micro incident). In such situations, the purpose of the dialogue is to learn who is doing what on which part of the installation. Several exchanges indicate that while talking, the operator focuses his counterpart's attention on particular events "but be careful there might be problems."

Several exchanges are concerned with the need for situating the events in time (retrospective vs. prospective collective memories), based on events that are still developing, events that are finished, actions performed in the recent past, or actions to be performed in the near future. For example, "The subcritical cold state will be reached at 0600 this morning"; "If we disconnect it now, we have to do all those tests again!; "We have to stop it this afternoon because the chemical people asked us to. Therefore it is finished." Apart from the need to know who is doing what (including the other department people), this exchange also indicates the need to know what will be done in the near future, building a prospective memory: "but anyway it has to be done tomorrow morning." A distinction has to be made between recording past events and events that should occur in the near future, and there should be a further differentiation between a retrospective and a prospective collective memory.

In that sense, it can be said that porous communication provides information (right or wrong) recursively, which represents the basis for the construction of individual and mutual situation awareness (individual knowledge of a shared situation: People should be aware of the reciprocal awareness). The collaborative operational mode that emerges during the MIs in the activity of diagnosis and localization of a malfunction enables the operators to share an understanding of the current situation and to know that they do share this understanding. In other words, they search to be mutually aware of the situation (including both the process and their respective knowledge) to construct their cognitive strategies.

The field studies have shown that porous communication of information may lead to deficiencies in forming shared representations, but at the same time, it helps in the solution of most of the problems faced by the operators. Another feature that appears is the complexity of integrating written documents and verbal exchanges. There are several types of written documents that respond to different goals (administrative procedures, incident procedures, trial procedures, etc.), and several documents need to be filled out by supervisors and operators, even during the events. In general, these documents contain highly summarized information that seems to generate confusion (for instance, none of the MIs related in this study appear in the shift changeover logbook). Therefore, an approach to keeping an updated collective memory of plant status and plant incidents should be designed to avoid increasing documentation obligations. The alternative would be to find solutions for better document integration, and greater readability in terms of situating events in their contexts.

Finally, it can be said that safety in a shared workspace depends on porous communication. System stability and effective operation relies on the continuous and recursive interactions among operators and other operation-related workers, bringing redundancy and diversification to the information that are exploited within the team as means for preventing, tolerating, and recovering errors.

In this way, the continuous development of more workable settings, enabling an easier construction and continuous updating of the operators' situation awareness (through overall system design, task allocation and definition, procedures, training, and human-machine interfaces), should be a never-ending task for an organization that really wants to improve safety. The problem here is that the porous communication is often based on underlying or implicit characteristics of human behavior and cognition; normally, system designers do not consider it as something that should be discussed or improved. Contrary to characteristics of the system that must studied and improved, porous communications are viewed as problems of the system (bad practices) that should be avoided by the use of the (good) formal constructs. We claim that this paradigm must be changed: Identification of the basic characteristics of porous communication feedback loops, and their relation with systems behavior, provides fundamental information to design safer sociotechnical systems.

REFERENCES

Amalberti, R. (1992). Safety in process control: An operator centered point of view. Reliability Engineering and System Safety, 38, 1–3.

Amalberti, R. (1996). La conduite de systèmes à risques. Le travail humaine [The operation of risk systems]. Paris: Presses Universitaires de France–puf.

Besnard, D., & Greathead, D. (2003). A cognitive approach to safe violations. Cognition Tech Work, 5, 272–282.
Bressolle, M., Decortis, F.B., Pavard, B., & Salembier, P. (1996). Traitement cognitif et organisationnel des micro-incidents dans le domaine du contrôle aérien: Analyse des boucles de régulation formelles et informelles [Cognitive and organizational treatment of micro incidents in the air traffic control domain: Analysis of the formal and informal regulation loops]. Toulouse: Octarès.
Checkland, P. (1981). Systems thinking, systems practice. New York: Wiley.
De Terssac, G. (1992). Autonomie dans le travail [Autonomy in the Work]. Paris: Presses Universitaires de France–puf.
De Terssac, G., & Leplat, J. (1990). La fiabilité et l'ergonomie: Spécificité et complémentarité [Reliability and ergonomics: Specificity and complementarity]. Revue de Psychologie Appliquée, 40, 377–386.
Derrida, J. (1988). Limited, Inc. Translated by Samuel Weber and Jeffrey Mehlman. Evanston, IL: Northwestern University Press.
Endsley, M. (1997) The role of situation awareness in naturalistic decision making. In C.E. Zsambok & G.A. Klein (Eds.), Naturalistic decision making. Mahwah, NJ: Erlbaum.
Ericsson, K., & Simon, H. (1993). Protocol analysis: Verbal reports as data. Cambridge: Cambridge University Press.
Faverge, J. (1970). L'homme, agent de fiabilité et d'infiabilité [The man, agent of reliability and nonreliability]. Ergonomics, 13, 301–327.
Faverge, J. (1980). Le travail en tant qu'activité de récuperátion [Work as a recovery activity]. Bulletin de Psychologie, 33, 203–206.
Grant, C. (2001). Vagueness, porous communication, fictions of society. In C. Grant & G. McLaughlin (Eds.), Language-meaning-social construction (pp. 43–48). Interdisciplinary Studies. Amsterdam/New York: Rodopi.
Grant, C. (2003, May). Sistemas instáveis: Comunicação. Paper presented at the GENTE/COPPE annual meeting, Rio de Janeiro, Brazil.
Grant, C. (2004). Rethinking communicative interaction. New interdisciplinary horizons. Amsterdam/Philadelphia: Benjamins.
Habermas, J. (1999). Wahrheit und rechtfertigung [Truth and justification. Philosophical essay]. Philosophische aufsatze. Frankfurt: Suhrkamp.
Hirshhorn, L. (1993) Hierarchy versus bureaucracy: The case of a nuclear reactor. In K. Roberts (Ed.), New challenges to understand organizations (pp. 137–151). New York: Macmillan.
International Nuclear Safety Advisory Group [INSAG-15]. (2002). Key practical issues in strengthening safety culture. Safety series n.75. Vienna: International Atomic Energy Agency [IAEA].
Krippendorff, K. (1980). Content analysis. An introduction to its methodology. London: Sage.
La Porte, T., & Thomas, C. (1995). Regulatory compliance and the ethos of quality enhancement: Surprises in nuclear power plant operations. Journal of Public Administration Research and Theory, 12, 109–137.
Mosey, D. (1990). Reactor accidents: Nuclear safety and the role of institutional failure. Nuclear Engineering International Special Publication. London: Wilmington Media Ltd.
Mumaw, R.J., Roth, E.M., Vicente, K.J., & Burns, C.M. (2000). There is more to monitoring a nuclear power plant than meets the eye. Human Factors, 42, 36–55.
Poyet, C. (1990). L'homme agent de fiabilitá dans les systemes informatisés [Man as the reliability agent in computerized systems]. In G. de Tersac & J. Leplat (Eds.), Le fateurs humains de la fiabilité [The human factors of reliability] (pp. 223–240). Toulouse: Octares.
Rasmussen, J., & Svedung, I. (2000) Proactive risk management in a dynamic society. Karlstadt. Sweden: Swedish Rescue Services Publishing.
Reason, J. (1990). Human error. Cambridge: Cambridge University Press.
Vicente, K. (1999). Cognitive work analysis. London: Erlbaum.
Vicente, K., Mumaw, R., & Roth, E. (1997). Cognitive functioning of control room operators—Final phase (Pub. #AECB 96-175). Ottawa, Canada: Atomic Energy Canadian Bureau.
Vicente, K.J. (1995). A few implications of an ecological approach to human factors. In J.M. Flach, P.A. Hancock, J.K. Caird, & K.J. Vicente (Eds.), Global perspectives on the ecology of human-machine systems (pp. 54–67). Hillsdale, NJ: Erlbaum.