The Role of Nuclear Power Plant Operators' Communications in Providing Resilience and Stability in System Operation

Paulo Victor Rodrigues de Carvalho[1], Isaac Luquetti dos Santos [1] , Jose Orlando Gomes[2,3] Marcos Roberto da Silva Borges [2] and Gilbert J Huber [3]

[1] National Nuclear Energy Commission/ Nuclear Engineering Institute
paulov@ien.gov.br, luquetti@ien.gov.br
[2] Graduate Program in Informatics-NCE&IM
[3] Industrial Engineering Department
Federal University of Rio de Janeiro
joseorlando@nce.ufrj.br , mborges@nce.ufrj.br

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. This paper, based on empirical data collected during nuclear power plant control room operation, analyses the communications within control room crews, including shift changeover. We 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 essential to maintain system resilience. Such continuous interactions enable the operators to detect, prevent and/or reverse system errors or flaws by anticipation or regulation. This study aims to provide recommendations, for the design of more workable systems for human cooperation in nuclear power plant operation.

1 INTRODUCTION

The overall performance of complex sociotechnical systems has to be controlled in order to produce with safety, quality, and low cost (Woods, 2006). According to Wreathall (2006) *"Resilience is the ability of an organization (system) to maintain, or recover quickly to, a stable state, allowing it to continue operations during and after a major mishap or in the presence of continuous stress"* (p.275). In such an arrangement, both controllers (human and automatic) have fundamental roles, such as to establish system goals, to know the system status and its behavior in the near future, to know how the other agents are performing their actions. This is done through continuous observation/feedback/feedforward communication nested loops at different levels – tracking, regulating, monitoring, targeting according to the ECOM model (Hollnagel and Woods, 2005). In the regulating/monitoring roles, the agents must construct their specific functioning system model in order to compare with the status indicators/controllers, to be able to act on the system to produce desired outcomes. Thus, the communication loops play a fundamental role in the control system, which can be viewed as a complex and structured set of hardware control systems embedded in a porous communication system which arises from human communication (figure 1).

Porous communication system is a theoretical model proposed by Grant (2001), whose principal concern is the construction of a 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.

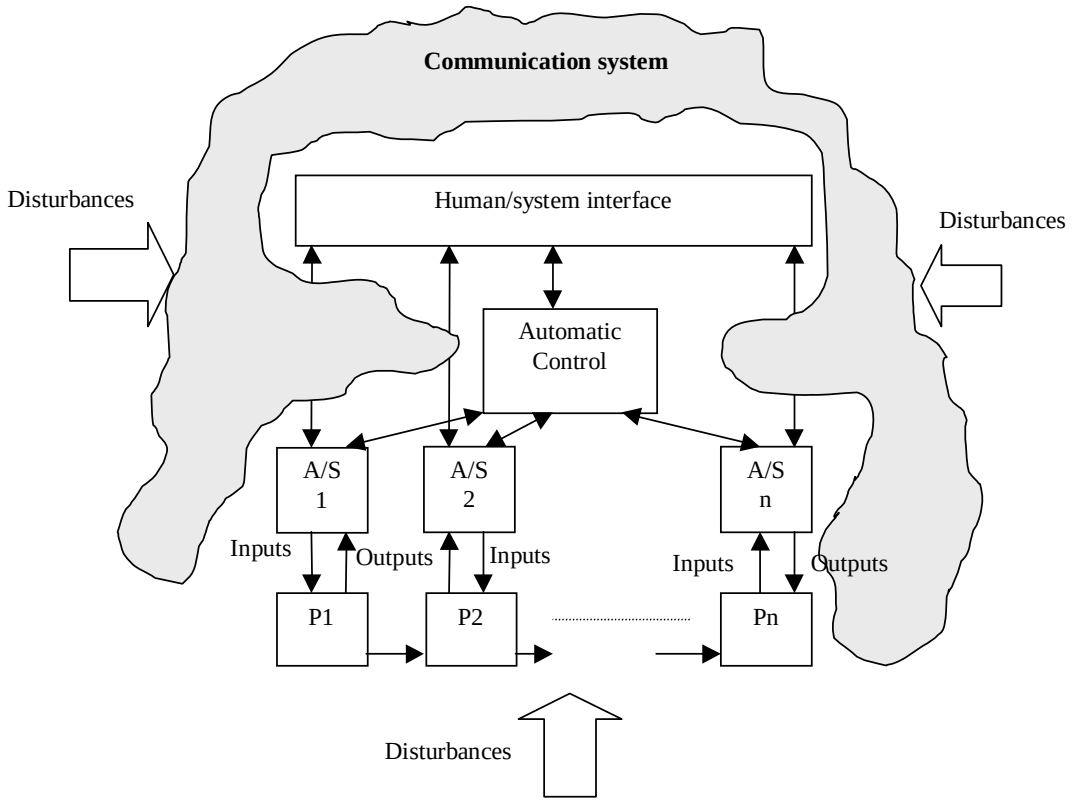

Fig.1. The basic control loop at the sharp end of modern process industries.

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 signs by someone. Examples of fuzzy signs in process operations can be found in the misuse of the sharp binary code – good/bad – of alarm windows that can be increasingly fuzzy depending on the state of the plant; in simple procedure instructions, when they lead to many different interpretative possibilities during actual work; when the state of equipment is inferred by visual inspections, instead of the use of formal documents. If language is vague, then communication, based on language, is porous, or "infinitely iterable"(Derrida 1988).

Accordingly, operators learn to use fuzzy signs (and porous communications) to deal with system complexity, enabling system operation during micro incidents (Carvalho et al., 2005) and in situations of continuous stress. 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 would not need to think about anything outside the scope of linear control system theory. However, this is not possible because of the complex (non linear) nature of the joint cognitive systems (Hollnagel & Woods, 2005), in which social communication systems are embedded. 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, 2001).

This argument may bring communication to the center of the debate about the resilience and stability of complex sociotechnical systems: how do such systems become resilient and stable as our daily experience indicates? We claim that stability may be maintained by resilience achieved through continuous interactions among agents and trade-offs across multiple goals, 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. Cook and Nemeth (2006) reached similar conclusions, pointing out that a *"resilient performance is the degree to which the operators are able to handle the disruption to the usual goal."*

In this paper, we use field studies to analyze the communications of control room operators in a nuclear power plant. We show some examples on how porous communications can contribute to a contingent system stability (maintain the operations according to specified goals), and how these communications overcome the limitations of the normative communication system (rules, norms, procedures, work permits, logical signals) prescribed for the plant operation, creating a resilience that is not easily achieved by organizational formal constructs.

The purpose of this research is to understand how the NPP control room joint cognitive system is resilient and brittle given the workload demands and operational (economic) pressures. The analysis uncovered goal conflicts that arise at the boundaries of the organization reaching control room operators, who adapt their work practices to cope with these conflicts.

2 MATERIALS AND METHODS

2.1 Research settings

This research was based on field studies in one nuclear power plant during a planned plant shutdown for maintenance/test activities. The operation of the plant started in the middle of 2000, however, most of instrumentation and control equipment had been acquired 15 years before (due to delays in plant construction). The control room and instrumentation/control systems use process control technology developed in the 70's in Germany.

The work organization follows the basic arrangements used in nuclear power plants around the world. To be undertaken during the outages, the work planning service prepares an extended task plan, together with the operation and maintenance departments. From the operation department side, maintenance periods imply preparing (isolating) the systems for maintenance, and delivering written documents (work-permits). However, having a work permit is not a sufficient condition to carry out the work. During normal plant operation, the final authorization to carry out any maintenance/test work comes from the Shift Supervisor. He has to sign all work permits during his shift, even when the plant is in the cold shutdown mode. During the plant shutdown the maintenance/instrumentation tests started together with the plant shutdown procedure, is a critical moment in which the co-ordination between operation, maintenance and planing can be tested.

The NPP control room operator crews who participated in the study were composed of four licensed operators – Shift Supervisor, Foreman, Reactor Operator (RO), and Secondary Circuit Operator (SCO) – and one not licensed operator – the Auxiliary Panel Operator (PO). The Shift Supervisors and Foremen are 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. They were trained over 1.5 years work time in the utility.

2.2 Methods

The subjects (NPP operators) were systematically observed in the NPP control room by 4 analysts, 2 of them with backgrounds in NPP operation. We observe how operators collectively regulate (adapt) their work in increasing workload situations (shutdown and startup), describing how they cope with micro incidents (MI) (Bressolle et al., 1996). Audio and video recorders, together with analysts' field notes are used to collect empirical data on conversations and interactions that occur naturally within the work environment. To identify MIs we used analyst's field notes, the transcribed verbal protocols and the videotapes. In a first step, we identified all events perceived by each analyst (because each analyst was in closer contact with one specific operator, the perceptions of the events of each analyst could be quite different). In the second step we merged the analyst's event tables in order to have tables with the chronological description of all events. The selection of some of these events as MIs was done based on the MI relevance for the research objectives. After MIs selection, we searched for all verbal protocols transcriptions related to each MI, from the start of our observations in the previous work shift.

3 RESULTS AND DISCUSSION

Table 1 presents some of the MIs identified during the plant shutdown and startup, with 3 different operator crews, which will discussed in turn.

Table 1. Micro incidents list.

Reactor shutdown – crew 1	**Pre startup tests – crew 2**	**Increasing reactor power – crew 3**
MI-1 Boiler 1 startup	MI-3 Incompatibility between Procedure requirements	MI-4 Limitation system parameter oscillation
MI-2 Instrumentation tests		

3.1 The boiler 1 startup MI

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 2 redundant boilers) are equipment used only sporadically and when they are needed (as in planned shutdowns) they receive special attention (maintenance, tests) in the previous shift in order to be ready for operation. This was the situation in this planned shutdown, according the dialog below during the shift changeover, just before the shutdown.

Out-going Foreman: "Boiler 1, changing the probe."
SCO: "Has he finished?
Out-going Foreman: "It's done. It's being tested."
SCO: "It is being tested. The operator will be done ..."

The final information is not conclusive: "The operator will be done..." The information operators really needed – if the boiler could be used – was not available at this time (about 3 hours before the moment to connect the boiler). The operators use a kind of fuzzy sign. Written documents, such as work permits, shift changeover registers are being filled at this very moment and cannot be used to help operators, especially in this case, where fieldwork was involved. Two hours later, we saw another operators' attempt to have 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 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."

According to the first statement the boiler 1 is available. With the word "theoretically" the Foreman indicates his concern about the actual state of boiler 1. The SCO goes further, when asking if it is hot, he committed the PO to an action: to heat the boiler 1.

Committed to action, the PO gave an unexpected answer: “I’m going to start up boiler 2.” Boiler 2 is the redundant boiler, which had not gone through testing on the previous shift. From this answer, it can be inferred that the PO also had some concerns about the state of boiler 1. The reason behind the PO’s choice to start up boiler 2 was the presence of a scaffold near boiler 1, an indication that maintenance services could not have been finished yet. The PO knew about the scaffold from conversations with field operators. The MI emerged 2 hours later. The time to connect the boiler in the circuit approached and boiler 2 failed to start. At this moment, we got the following conversation:

Supervisor: “Look at the condition of this f...ing boiler! What is going on here?!
30 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 the MI was closed without any further problem.

3.2 The instrumentation tests MIs

These MIs were related to the execution of instrumentation tests during the shutdown. According to the shutdown task schedule, instrumentation tests should be initiated just after the reactor trip at 23:30 o'clock. However, the test procedure indicated that the tests should be done only when the reactor reached the subcritical cold state. The subcritical cold state would be reached only 6:00 hours, at least, after the reactor trip. This situation is a vivid example of two prescriptions in conflict (the task planning and the test procedure), fuzzy signs that must be treated by operators. To solve this conflict, the Supervisor tried to understand the reason behind the subcritical cold state test requirement:

Instrument 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?”
Instrument Technician: “It has to be in a sub-critical cold state.”
Supervisor: “Well, it will not be cool until around 5 o’clock. Right now it’s in hot sub-critical state.”
Instrument 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…see what conditions are really necessary to meet these requirements...”

5 minutes later the Instrument Technician returned to the control room.

Supervisor: “Can we do it or not?”

Instrument 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.”
Instrument Technician: “The problem is that the test is ... I fear that most of it has been invalidated.
Supervisor: “Ok, Lets go. Get out of the Control Room. I have a lot of things to do! I can’t stay up with you all night!”

The authorization came without conclusive information (again). Why it is necessary to do the test in the cold subcritical reactor state? To get valid results, or to not jeopardize the operation (with the residual heat removal process still underway)? The procedures, intended to simplify operation with sharp information, are another source of fuzzy signs. They also do not help the operators in solving the conflict: procedures told what to do, but they (the procedures) didn’t tell why things should be done in this way. By not explaining the reasons for the requirements, the application of procedures, when confronted with other rules (as the planning of the tasks) and people’s desires (to do the tests), force the control room operators to use more complex cognitive strategies to understand those reasons, since they need construct explanations for the meanings behind the requirements. In moments of activity intensification this leads to simplifications in the decision-making process (the actual test influence in the operation was not taken into consideration) to reduce the operators’ cognitive load. As a result, just after the beginning of the tests the control room was full of alarms sounds. The dialog bellow describes 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 violation. However, this violation will clearly help the operation, since the reactor is already tripped, and the nuisance alarms due to the tests are disturbing the operation. Compounding the issue, this was not the only problem facing the operators at the time. The automation system uses the same signals used by the alarm system and spurious blockades in important systems, such as the Reactor Heat Removal System, were in progress. The reactor operator said: “We don’t know if the stoppages occurred because of the tests or because of a real condition at the plant.”

Two hours after the authorization (2 AM), the Supervisor, pressured by the other operators, decided to stop the tests. Two hours later (4:00 AM), when the Reactor Heat Removal was in operation, the Supervisor tried to do the tests again but the same problems came up and at 5:15 AM the Supervisor stopped the tests for the second time.

When asked about why he authorized the tests the Shift Supervisor explained his rationale:

"I should not have authorized those tests, ok. I should not have authorized them! But people tried to do the tests ... Because we have a very short down period! So I accepted the challenge and authorized the tests. But in the middle of the (…test…) I felt it was impossible and I ordered it stopped."

3.3 Incompatibility between procedure requirements

The operators follow the primary circuit leakage test procedure, before reactor startup. Following the test procedure operators reached an instruction to electrically disconnect a pump. At this juncture, this pump is already turned off and the valve nearby closed and locked. If the operators disconnect electrically the pump, they also have to do the pump test again, and that test takes about 8 hours. This same test had been performed the day before and was not scheduled to be done again in the task planning. This situation once again raises questions about the meanings behind procedures requirements, with a different operator crew. During the operator crew discussion, the following dialog summarizes one of the fundamental questions about procedure constructs and their temporality:

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 (the procedure writer) knows that the valve has already blocked it. Theoretically, the guy 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… to block both the pump and the valve. What is 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!?"

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 startup in order, according to the status of the plant and the results of previous tests (it makes no sense to test the pumps twice). Operators faced incompatibility in timing in the 3 documents: the Operation Manual, the test procedure and the task planning. Each one was prepared by a different group of specialists, in different organizations, in 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 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 according to the mutual situation awareness they achieved.

3.4 Limitation system parameter oscillation

To solve the problem of oscillation in the limitation system parameter in low power (12.5%), the RO, first consulting by phone with instrumentation technicians and with the Supervisor, increased reactor power by 5%, to see if the oscillation stopped. This dialog begins when the RO, after halting the power increase procedure, explains the oscillation to the Supervisor.

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 changed to 17.5 and it didn't move... it was stuck! And you could see that only it 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, real 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."

These conversations illustrate the importance of the collaborative strategies to achieve a resilient performance. When the RO noticed the limitation system parameter oscillation, he immediately stopped the power increase, reported the problem to Supervisor, and asked for the help of the instrumentation technician. The oscillating parameter is made up of many signals. One of them is the feedwater flow, which was very low. The instrumentation technician recognized 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. The decision to increase the power by 5% (another violation of routine, since no formal construct considers the possibility of raising a 1300 MWE reactor by 5 % just to see if the oscillation stops) was successfully initiated by the operator crew.

4 CONCLUSIONS

The field studies findings indicated that to achieve a resilient performance the operators can not rely only on the formal (normative) organizational constructs. The MIs presented situations in which the porous communications recursive feedback loops are the

way that the operators negotiate trade-offs across conflicting goals, making their decisions, and solving the plant problems. The verbal exchanges comprise sharing knowledge, drawing attention to something, getting authorization to do things, keeping operators informed, solving problems of the plant, negotiating goals, and selecting actions to perform. Verbal exchanges are crucial for the adequate 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 allow work in a timely way with the procedures. Our findings showed that people deal with the non-compliance during the normal operation 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 on 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 is to be dealt with. The normative practices, plans and procedures or instructions are paramount, but are 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 (which, of course, should be improved), 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.

In that sense, it can be said that porous communication provides information (right or wrong) recursively that 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 documentary obligations. The alternative would be to find solutions for better document integration, and greater readability in terms of situating events in their contexts. It can be finally said that a resilient performance in a shared workspace depends on porous communication. System stability and resilient operation rely on the continuous and recursive interactions among operators and other operation related workers, bringing redundancy and diversification to the information that is exploited within the team as means for preventing, tolerating and recovering errors.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support of the National Council for Scientific and Technological Development (CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico).

REFERENCES

Bressolle M., Decortis F., B., Pavard B., and Salembier P. (1996). *Traitement cognitif et organisationnel des micro-incidents dans le domaine du contrôle aérien: analyse des boucles de régulation formelles et informelles*, Toulouse: Octarès.

Carvalho P. V. R., Vidal M. C., Santos I. L. (2005) Nuclear power plant shift supervisor's decision-making during micro incidents. *International Journal of Industrial Ergonomics*, v.35, n.7, p. 619 - 644.

Cook R. and Nemeth,- C. (2006) Taking things in one's stride: cognitive features of two resilient performances. In Hollnagel E., Woods D., Leveson N. eds., *Resilience Engineering*, Ashgate Publishing, USA.

Derrida, J. (1988). *Ltd. Inc. Trans. Samuel Weber and Jeffrey Mehlman*. Evanston: Northwestern UP, 1988.

Grant, C. (2001). Vagueness, porous communication, fictions of society. In C. Grant and McLaughlin, G. (eds.), *Language-meaning-social construction: interdisciplinary studies*, Amsterdam/New York: Rodopi.

Hollnagel, E. & Woods, D. (2005). *Joint Cognitive Systems: An Introduction to Cognitive Systems Engineering.* Taylor & Francis.

Hollnagel E. (2006). Resilience: the challenge of unstable. In Hollnagel E., Woods D., Leveson N. eds., *Resilience Engineering*, Ashgate Publishing, USA.

Woods, D.D. (2006). Resilience: Essential characteristics of resilience. In Hollnagel E., Woods D., Leveson N. eds., *Resilience Engineering*, Ashgate Publishing, USA.

Wreathall, J. (2006). Properties if resilient organizations: an initial view. In Hollnagel E., Woods D., Leveson N. eds., *Resilience Engineering*, Ashgate Publishing, USA.