A computerized tool to evaluate the cognitive compatibility of the emergency operational procedures task flow

Paulo Victor R. Carvalho*, Mauro Vitor de Oliveira, Isaac J. Luquetti dos Santos

National Nuclear Energy Commission/Nuclear Engineering Institute, Cidade Universitária – Ilha do Fundão, Rio de Janeiro, RJ 21945-970, Brazil

Keywords:
- Procedure design
- Nuclear power plant operation
- Cognitive engineering
- Task flow

Abstract

Nuclear power production is a safety-critical process where ultimate decisions lie with the operators. During postulated incidents and accidents, operators rely on emergency operational procedures (EOPs), which are the most used decision support tool. In this research, we present a method to develop a computerized tool, based on the ACT-R cognitive architecture, to evaluate the logical task flow in the EOPs, verifying if the timing assumptions for operator’s actions contained in the procedure scripts can be accomplished by the human operators. We apply the tool to model the nuclear power plant (NPP) operator crew tasks during a Loss of Coolant Accident (LOCA) simulation. To validate the procedural scripts, the tool calculates the time intervals that operators need to accomplish actions and compare these time intervals with the plant dynamic behavior during the evolution of the accident. The tool proved to be an adequate way to validate the logical task flow of the EOP analyzed, showing that operators have enough time to execute their actions and an adequate waiting (free) time between some of their actions. The developed tool provides a low-cost alternative solution for NPPs owners and regulatory bodies to validate the logical task flow and quality issues of the hundreds of NPPs procedures.

1. Introduction

Control and time are indispensable aspects of the control room operators’ work in industrial plants, influencing how their actions are coupled and organized. As pointed out by Perrow (1984), in a tightly coupled system, control may easily break down when time is too short. Thus, to have an adequate performance of the control system, we must be able to account for the dependency between the operators’ performance and time they have to execute control actions (Hollnagel, 2005). The operator control of an industrial process can be viewed as a set of actions taken to conduct a system or process in a safe path to achieve the desired goals. According to the cognitive engineering approach, the problem of control is how to obtain a given outcome either from a technical artifact, such as a machine or an automatic control system, from an articulation of persons and systems, a control room, or from a set of persons and technology, an organization (Hollnagel and Woods, 2005).

In the modeling of the control possibilities in a joint cognitive system, a distinction can be made between task flow and situated cognition models (e.g., Suchman, 1987). A task flow model, based on the assumption that the operators must follow an operational procedure, assumes that a pre-defined sequence of (elementary) actions or a procedural pattern exists, and represents the best way of doing things to achieve system goals (shutdown, startup, refrigerate etc.) with safety. During the evolution of the situation, the expected next action of the operator can be found in the operational procedure, referring to the natural ordering of actions that are determined by the physical process and the engineering safeguards of the plant systems.

In the situated models, given any set of goals and constraints (resources, working conditions, command and control paths, roles and responsibilities, experience, etc.), some actions are more likely than others. Therefore, the operator has more autonomy to decide to select the actions to achieve the system goals. This type of model considers that human control actions are constrained by the conditions under which control takes place and that there is no best way to do things. Thus, operators’ actions flow depends on the current situation, rather than on a fixed sequential relation of actions. During the evolution of the situation, the next action is determined by the current situation, the operator goal, and by a set of possible actions that an operator may use to restore the control of the system. Situated models – based on the characteristics of the environment rather than on the preprogrammed action sequences – have been considered the best way to model the actual control room operators’ work. In a comprehensive field study in several Canadian nuclear power plants, Vicente et al. (1997) found that good operators rely extensively on knowledge-driven monitoring instead of rote procedural compliance. They also

---

* Corresponding author. Tel.: +55 21 21733835.
E-mail addresses: paulov@ien.gov.br, paulov@pq.cnpq.br (P.V.R. Carvalho).
observed that this practice allows operators to compensate for poor design of procedures.

However, current training and licensing programs in nuclear power plants and in other safe-critical domains are still based on task flow models (La Porte and Thomas, 1995; De Terssac and Leplat, 1990; Hirshhorn, 1993), and the use of event-based procedures is considered as one of the most important ways for ensuring a reliable human performance (AICE, 2004; Ghosh and Apostolakis, 2005). Several justifications frame this fact. For instance, in the design simplification paradigm, to follow procedures scripts reduce the complexity level of human reasoning, allowing human tasks and decisions to be accomplished by using if-then rules, reducing mental and/or physical workload and the possibility of human errors (Rasmussen & Jensen, 1974; Roth et al., 1994; O’Hara et al., 2000). Procedures may standardize the human performance; enabling different operators with the same training background to maintain their performance level that otherwise could be much more affected by the human variability (Dien and Montmayeul, 1997). During emergencies, even experienced and well-trained operators cannot rely only on their knowledge and experiences to control the plant – following a procedure the operator minimizes the possibility of forgetting and/or skipping crucial actions, and again, reducing the possibilities of human errors (Wright and McCarthy, 2003). So, in emergency situations operators are requested to run the plant according to the written Emergency Operational Procedures – EOPs (Jung et al., 2004). From a sociotechnical point of view, for the nuclear industry workers to follow plans and procedures are paramount organizational and individual safety values, and the conflicts that emerge when the procedures do not match the actual operation cause problems and anxiety to operator crews (Gauthereau and Hollnagel, 2005).

These two completely different ways of thinking about the operators’ work in safe-critical configure a paradox that the safety managers, engineers, and licensing authorities are far from to solve. In this situation, the overall work system and safety culture of safe-critical systems are affected by errors in procedures, because at the end, operators must follow procedures that they do not trust.

2. Procedures in the nuclear industry

The nuclear industry recognizes the importance of the procedures and the NPPs’ designers, owners and regulators normally use guidelines and checklists, for instance, those developed by US Nuclear Regulatory Commission after the Three Miles Island (TMI) accident (USNRC, 1981; USNRC, 1982; USNRC, 1983), to design and check procedures. Despite all these efforts, flaws in the design of procedures do occur and, unfortunately, they may remain uncovered, as latent failures in many situations. After TMI accident, the USNRC (Nuclear Regulatory Commission) inspected the procedures of all US nuclear power plants (NPP), demanded that power plant utilities improve their procedures (Lapinsky, 1988). Issues regarding the lack of the actualization of the Chernobyl procedures in low power mode were viewed as the most important root cause in the Chernobyl accident (Reason, 1987). More recently, ergonomic field studies in Brazilian NPPs have shown some conflicts among plant operators caused by flaws in plant procedures during the startup and shutdown of the plant, and during simulator training (Carvalho et al., 2005, 2006). The dialog bellow, between the simulator instructor and the shift supervisor during the simulator training, exemplifies the problems faced by operators when the procedures that they must follow have errors or inaccuracies (Carvalho et al., 2007).

Instructor: “Now, what the procedure says about the steam in the primary side? The temperature of the tubes of this isolated SG (steam generator) is 296 degrees. Which is the saturation pressure? (Pointing to the PxF 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. Yes or no? I 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 …! Especially me, if I will not be well documented!”

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, which I want that you understand the situation! Or else, I didn’t need to be here!” (Carvalho et al., 2007)

3. Analytical models in nuclear power plant tasks and procedure evaluation

Operational and event-driven emergency procedures indicate a set of tasks the operator must perform or verify during the plant change of state or accident situations to configure the basic parameters and control their evolution. Procedures generally begin with “macro-tasks” such as START, REFRIGERATE, SHUTDOWN, etc. For each one of these macro-tasks there are several tasks to be accomplished and verified by the crew. Like any other formal prescription, the procedure does not describe the action exhaustively. Indeed, no linguistic construct can describe any action exhaustively (Garfinkel, 1967). This mean that the use of procedures still requires the operator to employ a strategy for sequential execution of the tasks in a timely manner, allowing him or her to ensure that each task are done in the correct order. In fact, procedures for safety-critical environments should be deliberately and carefully conceived and designed to reduce local and contingent control variability, providing a pre-defined selection of actions sequences for the execution of safety-critical tasks, which all need to be performed at the particular moment of the plant change of state or accident evolution. For these reasons, to assess the logical task flow of the procedural scripts, verifying if the human operators can accomplish with the timing assumptions the procedure designers made is a fundamental issue for the NPP owners and regulators. To licensing a NPP, we need to verify if the operators can follow the procedures’ instructions according to their cognitive capacity in a timely manner, constrained by the behavior of plant variables, and by the layout of the control room.

The guidelines mentioned above used to evaluate procedures and operators’ tasks, which can incorporate knowledge about human cognition, give only overview information about how procedures will actually be used by the operators. A further step required for the NPP owners and regulators is to validate the procedure use for a specific task and specific operators in the control room. The most obvious way to validate procedures is to conduct usability tests, using full scope simulators running the several accident scenarios and real plant operators (IAEA, 2006). However, there are hundreds of scenarios in the emergency procedures and their variations. Therefore, due to the lack of time to run all possible scenarios, the high cost of the full scope simulator working hours, and the availability of operators to run this entire set of scenarios, most of the scenarios are not tested, and procedure flaws remain undetected.
Another way to evaluate procedure is using analytical models of the operators’ behavior, which are often implemented as software tools. These models simulate some physical and cognitive processes and/or task knowledge of the operator in ways that allow an analyst to estimate various aspects of the procedure used. They can be used to supplement procedure verification/validation guidelines by providing alternative ways of analyzing the human information-processing and cognitive requirements of specific tasks contained in operational procedures. The analytic models also offer potential of improving procedures’ verification/validation issues, replacing some of the normal usability testing phases, thus reducing the cost of improving procedures’ verification/validation issues, replacing some of the normal usability testing phases, thus reducing the cost of improving procedures’ verification/validation guidelines by

To reduce the side effects of complicated procedures Park and Jung (2007) developed a task complexity measure called TACOM, which is based on cognitive complexity factors affecting the complexity of procedural steps in emergency operating procedures of a nuclear power plant (Park et al., 2005). TACOM aims to deliver a task complexity measure that can quantify the complexity of procedural tasks.

In this research, we develop a computerized tool to model the execution of the Emergency Operational Procedures (EOPs) by an NPP’s operator, using the ACT-R cognitive architecture (Anderson, 1993). Based on the procedure scripts, we model the operators’ task flow during the event. The model calculates the time the operators need to read and understand the procedure actions, and to carry out the control actions in the control room panels. The time intervals of each action obtained when the procedure tasks are modeled are added and compared with the dynamic behavior of the plant, indicating if there are incompatibilities between the procedure instructions timing and the actual time the operator need to accomplish his/her tasks in a safe manner. Using this tool, we do not need to make extensive simulation exercises with the complete operational crew for the entire set of scenarios involving the emergency procedures and their variations. We have only to run the operator model for each scenario and compare the results with the behavior of the plant variables that can be obtained by running the simulation software for the different scenarios, without the presence of the crew. To exemplify the computerized tool, we develop an application that uses the small-break Loss of Coolant Accident (LOCA) Emergency Operational Procedure of a real NPP.

4. Research setting

This research was carried out in a pressurized water nuclear reactor (PWR) that delivers 1200 MW of electrical energy. Fig. 1 shows the schematic view of the plant control room that is operated by 4 operators (Reactor Operator – RO, Secondary Circuit Operator – SCO, Panel Operator – PO, Foreman), and 1 Shift Supervisor, who is the ultimate responsible for the operation. The
control room consists of stand-up control panels, an operator desk with 2 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.

Paper procedures guide the plant operation. The Foreman read (and browse) the procedure to the RO and SCO during operational interventions (e.g., change power, shutdown), and in emergencies. The RO and SCO confirm the instruction received and act (search for information, push some button etc.) if necessary. Then, they inform to the Foremen the action taken. The PO helps the RO and SCO in the auxiliary control panels readings/manipulations. All the plant procedures have the same basic format. It begins with a flowchart, indicating the main event and operator actions. These actions are expanded in new flowcharts in a recursive way. Finally, the detailed instructions for each manual action and checklists are presented. The operators must fill out the blanks in the checklists with the detailed manual actions they made. Within this recursive-explored structure, the operators have to browse the paper procedures continually, going from general diagnostic flowcharts to the detailed manual actions and vice-versa.

Fig. 2 presents the main components of a pressurized water reactor (PWR). The plant under study has four redundant refrigeration circuits (4 loops), but only 1 of the 4 loops is shown in the figure. Each refrigeration circuit can be divided into two other circuits according to their function: the primary circuit and the secondary circuit. The primary circuit is composed by the reactor core, the pressurizer (PZR), the steam generator (primary side), the control rod banks, and the chemical and volumetric control system (CVCS). The reactor core is the main component of the primary circuit and it is responsible for heating the circulating water (nuclear fission process). This water, or reactor coolant, is pumped by the reactor coolant pump (RCP) in the primary circuit reaching the steam generator. The control rod banks control the nuclear fission process inside the core. The pressurizer controls the primary circuit pressure that must be kept high enough to guarantee the primary water in the liquid phase. On the secondary side, there are the steam generator system (secondary side), the turbine, the condenser, and the feedwater system. The secondary circuit coolant leaves the steam generator as superheated steam. It passes through the turbine where the energy is delivered to drive the turbine-generator unit. The remaining heat is removed in the condenser where the secondary coolant is returned to the liquid phase. From the condenser, the secondary coolant is pumped as feedwater to the steam generators where it picks up energy again from the primary coolant. Hence, the power cycle repeats. Extra water suppliers are the residual heat removal (RHR) system for the primary side and the auxiliary feedwater

Table 1
Dynamic behavior correspondent to break with 30 cm² of size, located in the cold leg between the reactor vessel and the injection nipple of the emergency cooling.

<table>
<thead>
<tr>
<th>Time (sec)</th>
<th>Events (in Grey automatic actions phase)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Accident starts</td>
</tr>
<tr>
<td>10</td>
<td>Differential pressure between equipment room/atmosphere &gt; 30 mbar ⇒ RESA\textsuperscript{a}/TUSA\textsuperscript{b}</td>
</tr>
<tr>
<td>23</td>
<td>Coolant pressure &lt; 131 bar ⇒ 100 K/h cooldown</td>
</tr>
<tr>
<td>35</td>
<td>PZR level &gt; 2.95 m ⇒ TURN OFF all the PZR heaters</td>
</tr>
<tr>
<td>40</td>
<td>PZR level &lt; 2.28 m ⇒ TURN OFF all the RCPs (Recirculation Coolant Pumps) ⇒ it is not anymore possible the intake from the PZR due to fulfill of 2 of 3 emergency cooling criteria</td>
</tr>
<tr>
<td>64</td>
<td>Coolant pressure &lt; 110 bar</td>
</tr>
<tr>
<td>65</td>
<td>Safety Injection Pumps (SIPs) starts: 4 SIPs injection in upper plenum nipple</td>
</tr>
<tr>
<td>290</td>
<td>Cooling temperature &lt; main steam temperature ⇒ its not possible anymore to sink the heat removal by the secondary side of the SGs (Steam Generators)</td>
</tr>
<tr>
<td>2000</td>
<td>The SIPs overcome the rupture</td>
</tr>
</tbody>
</table>

\textsuperscript{a}RESA – Reactor Safety Actuation (reactor shutdown, fall of control bars in the core).
\textsuperscript{b}TUSA – Turbine Safety Actuation (turbine shutdown).
Secondary-side heat sink 100 k/h cool down in progress via MS bypass

Sump level Rises

Primary-side heat transport By RCPs until shutdown, then by natural Pressure and temperature in Radioactivity in condenser vent stack exhaust air and radioactivity

Radioactive releases Terminated by containment HVAC isolation/containment evacuation alarm issued

Radioactive releases By containment HVAC isolation and RCS isolation Radioactivity in containment Rises

Coolant temperature rise already occurred

Subcooling Reactor tripped by control rods and boric acid injection by JN/JDH

RCS pressure < 2.28 m, may later rise to > 2.28 m

Activity in containment Rises

Radioactive releases Do not rise

Primary circuit integrity

Secondary-side heat sink

Plant conditions after automatic actions for small-break LOCA.

Table 2

<table>
<thead>
<tr>
<th>Plant component</th>
<th>Trends of plant parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reactor power</td>
<td>RESA/TUSA (reactor and turbine shutdown) borating up by JN/JDH system</td>
</tr>
<tr>
<td>ΔP containment/ atmosphere</td>
<td>Rises &gt; 30 mbar</td>
</tr>
<tr>
<td>PZR level</td>
<td>Drops to &lt; 2.28 m, may later rise to &gt; 2.28 m</td>
</tr>
<tr>
<td>RCS pressure</td>
<td>Drops &lt; 109 bar but remains &gt; 9 bar</td>
</tr>
<tr>
<td>Activity in containment</td>
<td>Rises</td>
</tr>
<tr>
<td>Radioactive releases</td>
<td>Terminated by containment HVAC isolation/containment evacuation alarm issued</td>
</tr>
<tr>
<td>Radioactivity in condenser vent</td>
<td>Do not rise</td>
</tr>
<tr>
<td>Pressure and temperature in PZR relief tank</td>
<td>Do no rise</td>
</tr>
<tr>
<td>Sump level</td>
<td>Rises</td>
</tr>
<tr>
<td>Primary-side heat transport</td>
<td>By RCPs until shutdown, then by natural circulation and by outflow through the break</td>
</tr>
<tr>
<td>Secondary-side heat sink</td>
<td>100 k/h cool down in progress via MS bypass or MS relief valves; feedwater supply to SGs by main feedwater pumps and possibly startup and shutdown pumps; emergency feedwater pumps startup if necessary</td>
</tr>
</tbody>
</table>

(AFW) system for the secondary side. These systems are used in low power operation conditions, shutdown conditions, and emergencies.

4.1. Cognitive overload situations and recommendations

To avoid NPP operators’ cognitive overload during accident situations, the standard ANSI/ANS 58.8 (1994) establishes the time response design criteria for safety-related operator actions to be used in the procedure design of a pressurized water nuclear reactor. The criteria are used to determine the minimum response time intervals for safety-related human actions to mitigate incident consequences, after the automatic reactor shutdown, when operators are following the emergency operational procedures. The aim is to assure that the time intervals between human actions prescribed by the procedure scripts are compatible with the time the operators actually have to search and obtain, at any moment, the information from the plant control panels, and to manipulate the controls in plant panels. The verification and validation of this issue is a necessary step of plant licensing process.

The time available for the operators’ actions is a function of the safety system design. In the plant under study, the safety system design follows the KTA 3501 (1985) standard. According to KTA 3501, the operator shall not execute any task during the first 30 min after the reactor automatic shutdown, considered the beginning of any emergency event. To accomplish with this requirement, the automatic actions shall guarantee, in the first 30 min after any incident, the control of the plant and the safe-critical conditions.

5. Development and implementation of the computerized tool

We use the ACT-R (Atomic Components of Thought – Rules, Anderson, 1993; Anderson et al., 2004) cognitive architecture to model the operators’ task flow during a small-break LOCA accident. ACT-R is a computerized model of a cognitive architecture based on a theory about how human cognition works. On the exterior, ACT-R looks like a programming language; however, its constructs reflect assumptions about human cognition. These assumptions are based on numerous facts derived from psychology experiments. ACT-R was originally developed by Anderson (1993) and has been applied to modeling domains such as cognitive workload modeling (Juvina et al., 2007), problem solving and decision making in cockpit (Boehm-Davis et al., 2002), human multitask analysis (Brumby and Saluvicci, 2006), and so forth. The currently supported versions of ACT-R are ACT-R 3.0, ACT-R 4.0, ACT-R 5.0, and ACT-R 6.0 that can be freely downloaded in the site http://act-r.psy.cmu.edu/. Because all systems are written in Common Lisp, they are easily extensible and can run without modification on any Common Lisp implementation for Macintosh, UNIX, and Windows platforms.

ACT-R cognitive architecture aims to define the basic and irreducible cognitive and perceptual operations that enable the human mind. A general assumption in ACT-R theory is that the human skills are made by the brain production system (Newell and Simon, 1972). A production system is a set of production rules – each of which represents a contingency for action – and a set of mechanisms for matching and applying production rules. In theory, each task that humans can perform should consist of a series of these discrete operations. The ACT-R’s main components are modules, buffers, and pattern matcher. There are two types of modules:

- Perceptual-motor modules, which take care of the interface with the real world (i.e., with a simulation of the real world).
- The most well-developed perceptual-motor modules in ACT-R are the visual and the motor modules;
- Memory modules.

We do not use the ACT-R with the entire set of sophisticated cognitive components of the architecture (activation, learning, decay, utilities, etc.) because we just want to model the actions’ interval time. We use the ACT-R framework as a scripting language to timely code the procedure tasks and corresponding operators actions.

5.1. The small-break LOCA accident

In Loss of Cooling Accident (LOCA), the coolant is escaping from the reactor circuits, and the Reactor Cooling System (RCS) looses its refrigeration capability. The modeled accident corresponds to
a break with 30 cm² of size, located in the cold leg (see Fig. 2). In this situation, the most important objective of the safety actions (automatic and human) is to cool the reactor core. To cool the reactor core the coolant inventory, the heat transfer rate, and the system pressure must be maintained inside the safety envelop during the entire event. The entire set of relevant and time-critical safety actions in the first phase of the LOCA are carried out by reactor protection system automatic actions. The last (non-critical) phase of a loss of coolant accident is handled by manual (operators) actions. These actions aims: 1) to monitor and ensure core cooling, 2) to operate the residual heat removal pumps, 3) to monitor the boron concentration in the containment sump, 4) to cool the spent fuel pool, to monitor the H₂ concentration, and 5) the retention of radioactivity within the containment. To do so, the operators must follow the emergency operation procedure (EOP), driving the plant into a safe condition.

The dynamic behavior of the plant during this accident, including the automatic actions, is shown in Table 1. The time, on the left column of Table 1, is obtained according to the dynamic behavior of the main plant variables during the evolution of the modeled accident. The automatic actions carried out by the reactor protection systems were done from time 0 to 2000 s. The manual actions of the operators were modeled from the end of automatic actions (~ 2000 s) until the elapse time of 6200 s, when the plant returns to a safe condition.

### 5.2. The accident procedure

The trends of the main plant parameters after the initiation of the small-break LOCA accident that used for the accident identification are shown in the Table 2. Table 3 presents the critical safety parameter values at the end of automatic actions (and at the beginning of manual actions). The manual actions are exemplified in Fig. 3 (the flow graph in the beginning of the procedure). The dotted arrow in the flow graph shows the procedure pathway for the small-break LOCA accident with emergency core cooling criteria met. Fig. 4 shows the beginning of the manual actions (action1) for the small-break LOCA.

---

**Fig. 3.** Initial steps procedure for the small-break LOCA accident.
5.3. Model implementation

The first step to model the task flow during the LOCA accident is to define the operators’ declarative knowledge about the simulated accident. In ACT-R architecture, the declarative knowledge is represented in chunks. A chunk is a memory unit that consists of several components that are strongly associated with one another (Cowan, 2001), representing the knowledge that a person has to solve a problem. A chunk is defined by its type or category (e.g., birds), and its slot or category attributes (e.g., color or size). Thus, to model the operators’ knowledge about the accident we create chunks, based on the plant accident procedure. During the ACT-R program execution, if any variable (slot) must be used in the program, the variable (or the entire chunk) is loaded into the working memory.

The first chunk created was the chunk ACCIDENT to define the current accident (in our case a small-break LOCA). The Lisp code for the chunk accident is given by

\[
\text{(Chunk-type accident type action time end)}
\]

Where the slot type defines the accident type, the slot action defines the current manual action of the accident, the slot time defines the time interval since the beginning of the accident, and the slot end defines the end condition for the accident.

The other important chunk created was the chunk TIME, to define the average time (including perceptual and motor/cognitive time) that the operators need to accomplish their actions. These average times were obtained through several measures of a crew working in the full scope simulator of the plant control room (see Fig. 2). Three operators, a Reactor Operator – RO, a Secondary Circuit Operator – SCO, and a Shift Supervisor – SS, compose the crew. The RO and SCO look at indicators and manipulate controls in the panels of the plant. The function of the SS is to read the accident procedure to the plant operators (RO and SCO). Table 4 summarizes the average time response obtained for the operators’ control actions, where MCD is the Main Control Desk, MIB is the Main Instrumentation Board, CAP is the Central Auxiliary Panel, LAP is the Left Auxiliary Panel, and RAP is the Right Auxiliary Panel. The Lisp code for the chunk TIME is given by

\[
\text{(Chunk-type time t1a t1b t1c t1d t2 t4 t5 t7 t8 t9 t10 t11 tmem)}
\]

In the simulated accident, the operators do not access the VDUs screens and, consequently, the estimated time to access VDUs menus (t3) was not used in the chunk TIME.

To achieve our objective – to develop a low cost modeling tool to test the cognitive compatibility of the operators’ task flow using procedures, avoiding the need to connect the model to the simulator software – we create chunks to represent the dynamic behavior of the plant during the simulated accident (for the LOCA, the plant variables are updated in real time based on the data presented in Table 1). Thus, the time that the operators need to accomplish their actions can be compared to the evolution of the plant variables during the accident. For example, the chunk HEATTRANSPORT defines the critical safety function of heat transport, carried out in the primary circuit of the reactor. The primary pumps (RCPs) do the heat transport function until the shutdown of the reactor. After the shutdown, this function is done by natural circulation and by the outflow through the break. The Lisp code for the chunk HEATTRANSPORT is given by

\[
\text{(Chunk-type heattransport intemp outtemp rcpson)}
\]

Where the slot INTEMP defines the average water temperature at the input of the reactor vessel, the slot OUTTEMP defines the average water temperature at the output of the reactor vessel, and the slot RCPSON defines the number of RCPs running.

The emergency operation procedure (EOP) of the simulated accident (in which the operators’ task flow is based) was introduced in the model using production rules. In the ACT-R framework, production rules represent the knowledge about how we do things. Productions code the available knowledge (in the EOP) about the accident using production rules in the form of IF-THEN or CONDITION-ACTIONS pairs. When a condition is satisfied (chunks list) the action to be taken is given by the production selected.

To exemplify the several production rules created to simulate the operators’ task flow, we describe the production rule P ACTION27 – switch on the RHR pumps. The production rule P ACTION27 starts when the next action to be executed by the program is action 27. When this occurs, the chunk variable time (chunk accident), ta27 (chunk action), t1d, t2, t4, t5, t7, t8, t9, t10, and t11 (chunk times) are brought to the working memory to be manipulated. The chunk variable rhrpp (chunk others) is set to 4 (4 RHR pumps are switched on). The first evaluation command (!eval!) of ta27 (in the chunk action) calculates the time spent for turn on the 4 RHR pumps. The last command, !eval!, updates the variable time at the end of the production rule action 27.

\[
\text{Remark: All available RHR pumps must be started up: they run in minimum flow recirculation mode, in parallel with the (available) SIPs. If emergency power mode occurs after the RHR pumps have been cut in, the RHR pumps must immediately be restarted by manual command, as this is not performed automatically. Additionally shutdown running startup/shutdown pumps and HP charging pumps (see manual action block "Assure startup of RHR pumps") if safety injection pumps are still in operation.}
\]

![Fig. 4. Detailed instructions of the manual action 27 for the small-break LOCA accident.](image-url)
Fig. 4 shows the detailed instructions for the manual action 27 of the small-break LOCA accident. First, the SS goes to the pulpit and reads the Remark to the operators (78 words), spending 78 times \( t_{10} \) s \((** = t_{10} \times 78)**) in the (eval) command line. Next, the RO goes to the central auxiliary panel (CAP) for reading the values (spending \( t_{11} \) s). The SS reads to RO the variables to be checked, spending 8 times \( t_{11} \) s for all variables \((** = t_{11} \times 8)**). The RO spends time for visual orientation in the CAP for read the 4 values, 4 times \( t_{2} \) s \((** = t_{2} \times 4)**). The RO spends time to compare among the on/off RHR possibilities, 4 times \( t_{4} \) s \((** = t_{4} \times 4)**). The RO spends time to compare the readings with his previous knowledge, 4 times \( t_{5} \) s \((** = t_{5} \times 4)**). The RO spends time to compare some code in the reactor protection system, 4 times \( t_{9} \) s \((** = t_{9} \times 4)**). Finally, the RO goes back to his desk in the control room (spending \( t_{1d} \) s). In the simulation, the obtained time for the crew carry out the action 27 was about 92 s.

6. Results

The objective of the actions taken in response to a loss of coolant accident is to run down the plant to the “cold shutdown, depressurized” condition, while minimizing the release of radioactivity to the environment. Table 5 presents the results obtained by the model developed (the time that the operators need to accomplish their actions) and the dynamic behavior of the plant variables for the simulated accident. The modeling tool calculated the time steps for the operators’ manual actions that start at the end of the automatic protection systems actions (30 min after the beginning of the accident or the reactor shutdown – fall of the control rods in the reactor core).

When we compare the dynamic behavior of the plant with the calculated time that the operators need to accomplish their actions during the simulated accident, we find that the operators have enough time to execute their actions. Sometimes the plant variables reach the expected value slightly before or after the moment of the operator action calculated by the tool. This situation does not indicate a problem in this procedure because the manual actions started at acceptable values, considering that the operators’ actions to cool down the plant in this accident cannot be considered time-critical.

The results also show adequate waiting times between the actions that have to be carried out by the plant operators. The Table 5 shows a waiting time (operators’ free time) between the end of action 4 and beginning of action 6 \((t_{w4-6} = 608 \text{ s})\). The action 6 can only be started after a RCS outlet temperature of 160 °C and the steam pressure below 4 bar. Other wait times obtained are 300, 71, and 25 s between the action \( t_{w20-21}, t_{w21-24}, \) and \( t_{w24-22} \), respectively. These waiting times show a reasonable free time between the actions for the operators.

The action 29 is a checking condition to leave the action 28, i.e., action 29 is carried out together with the action 28, and, consequently, no additional time is shown in the table for the action 29. Finally, the last free time \((t_{w30-31} = 260 \text{ s})\) calculates the elapse time between the check if the secondary side heat sink is available and the low-level limit in the borated water tank is reached, and the RHR initiates to circulate from the containment sump. For this situation, we can see from Table 5 a free time \((t_{w30-31} = 260 \text{ s})\) (more than 4 min), enabling a reasonable time for the operators to accomplish their tasks.

The actions from 31 (initiate sump recirculation mode) to 64 (monitor long-term plant condition) were not modeled because they are long-term actions and, consequently, the operators have a long time to carry out these procedure steps that do not demand cognitive overload.

6.1. Identification of problems in procedures

During the implementation of the modeling tool for the small-break LOCA accident, it was identified a mismatch between the flow graph procedure and the detailed instructions of the manual actions. More specifically, before bypasses the emergency core cooling criteria (action 22) the water level in the pressurizer must reach 8 meters (action 24), during the accident evolution and, consequently, the action \((t_{a24})\) must be done previously than the action 22 \((t_{a22})\). In Table 5, is shown the corrected sequence for these accident actions. The operators, during their full scope simulator training, identified the same mismatch and acted based on their situation awareness, changing the order of the procedure actions. This situation illustrates the importance of validating the plant procedures using simulators and modeling techniques. It also demonstrates that the operators adapt and are capable to interpret procedure instructions, i.e., the operators fill out the blanks and the implicit aspects in the procedures. They use their cognitive flexibility to solve the conflict between the written procedure and the way that the system works. In this case, for safety reasons, the pressurizer must have at least 8 meters of water level before the operator bypasses the emergency core cooling system. Naturally, the identification and solution of any mismatch between written procedures during the accident evolution causes additional cognitive overload in the operators and must be corrected as soon as possible.
Table 5
Dynamic behavior of the plant and the calculated time that operators need to accomplish their actions using de modeling tool for a small break with 30 cm² of size located in the cold leg between the reactor vessel and the injection nipple of the emergency cooling.

<table>
<thead>
<tr>
<th>Manual action/ wait time procedure</th>
<th>Event (event cues)</th>
<th>Flow path action</th>
<th>Dynamic behavior time (s)</th>
<th>Calculated time (s) Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>ta0</td>
<td>Manual initial condition</td>
<td>Execute</td>
<td>1800</td>
<td>–</td>
<td>1800</td>
</tr>
<tr>
<td>ta1</td>
<td>Check plant conditions</td>
<td>Execute</td>
<td>NA</td>
<td>1801</td>
<td>2292</td>
</tr>
<tr>
<td>ta2</td>
<td>Check if the plant is in emergency power mode</td>
<td>NO</td>
<td>NA</td>
<td>2293</td>
<td>2374</td>
</tr>
<tr>
<td>ta4</td>
<td>Check if the plant has an LOCA in PZR</td>
<td>NO</td>
<td>NA</td>
<td>2375</td>
<td>2391</td>
</tr>
<tr>
<td>tw4-6</td>
<td>Waiting time for RCS outlet temperature &lt; 160 °C and steam pressure &lt; 4 bar</td>
<td>Wait</td>
<td>NA</td>
<td>2392</td>
<td>3000</td>
</tr>
<tr>
<td>ta6</td>
<td>Check if the plant conditions is RCS outlet temperature &lt; 160 °C and steam pressure &lt; 4 bar</td>
<td>YES</td>
<td>3000</td>
<td>–</td>
<td>3093</td>
</tr>
<tr>
<td>ta7</td>
<td>Check if the RHR pump is in operation</td>
<td>NO</td>
<td>3000</td>
<td>–</td>
<td>3094</td>
</tr>
<tr>
<td>ta16</td>
<td>Check if the plant has an LOCA via PZR</td>
<td>NO</td>
<td>3000</td>
<td>–</td>
<td>3151</td>
</tr>
<tr>
<td>ta18</td>
<td>Check if the PZR level &lt; 2.28 m</td>
<td>YES</td>
<td>3000</td>
<td>–</td>
<td>3168</td>
</tr>
<tr>
<td>ta19</td>
<td>Due to: PZR level &lt; 2.28 m ⇒ Reset RP signals <em>JR 41/42</em>. Starts the manual aspersion with the additional boration system and/or with the volume control system in the steam region of the PZR</td>
<td>Execute</td>
<td>3000</td>
<td>–</td>
<td>3376</td>
</tr>
<tr>
<td>tw20-21</td>
<td>Waiting time for RCS outlet temperature &lt; 160 °C and steam pressure &lt; 4 bar</td>
<td>Wait</td>
<td>3300</td>
<td>–</td>
<td>3810</td>
</tr>
<tr>
<td>ta20</td>
<td>Due to: PZR level &lt; 2.28 m ⇒ TURN ON the PZR spray (Raise PZR level to 8 m by spray out of &quot;JDH&quot;)</td>
<td>Execute</td>
<td>3450</td>
<td>–</td>
<td>4011</td>
</tr>
<tr>
<td>tw21-24</td>
<td>Waiting time for PZR level &gt; 3.2 m (300 s after the spray beginning)</td>
<td>Wait</td>
<td>3450</td>
<td>–</td>
<td>3986</td>
</tr>
<tr>
<td>ta21</td>
<td>Check if the PZR level &gt; 3.2 m and/or RCS outlet temperature &lt; 160 °C and/or ΔP containment/ atmosphere &gt; 0.03 bar ⇒ Alarm class 5: switch over to RHR recirculation mode</td>
<td>YES</td>
<td>3450</td>
<td>–</td>
<td>3864</td>
</tr>
<tr>
<td>tw21-24</td>
<td>Waiting time for PZR level &gt; 3.2 m (423 s after the spray beginning)</td>
<td>Execute</td>
<td>3865</td>
<td>–</td>
<td>3936</td>
</tr>
<tr>
<td>ta24</td>
<td>Check if the PZR level = 8 m ⇒ TURN OFF the PZR spray (Stop spraying from &quot;JDH&quot;)</td>
<td>YES</td>
<td>3425</td>
<td>–</td>
<td>3985</td>
</tr>
<tr>
<td>tw24-22</td>
<td>Waiting time for the PZR level &gt; 8 m (450 s after the spray beginning)</td>
<td>Wait</td>
<td>3450</td>
<td>–</td>
<td>4011</td>
</tr>
<tr>
<td>ta25</td>
<td>Check if the PZR level &gt; 3.2 m and/or RCS outlet temperature &lt; 160 °C and steam pressure &lt; 4 bar</td>
<td>YES</td>
<td>3865</td>
<td>–</td>
<td>3936</td>
</tr>
<tr>
<td>ta27</td>
<td>TURN ON the RHRs, working in low head flux, accumulators valves blocked (manual or automatic) ⇒ Bypasses the SI</td>
<td>Automatic Execute</td>
<td>4400</td>
<td>–</td>
<td>4374</td>
</tr>
<tr>
<td>ta28a</td>
<td>TURN OFF the 1st SIP</td>
<td>Execute</td>
<td>4625</td>
<td>–</td>
<td>4375</td>
</tr>
<tr>
<td>ta28b</td>
<td>TURN OFF the 2nd SIP</td>
<td>Execute</td>
<td>4489</td>
<td>–</td>
<td>4488</td>
</tr>
<tr>
<td>ta28c</td>
<td>TURN OFF the 3rd SIPs</td>
<td>Execute</td>
<td>5190</td>
<td>–</td>
<td>4879</td>
</tr>
<tr>
<td>ta28d</td>
<td>Check if the PZR level &lt; 8 m ⇒ TURN ON the PZR spray</td>
<td>YES</td>
<td>5250</td>
<td>–</td>
<td>5380</td>
</tr>
<tr>
<td>ta28e</td>
<td>Check if the coolant pressure &lt; 9 bar ⇒ RHRs ON</td>
<td>YES</td>
<td>5560</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>ta28f</td>
<td>Check if the new equilibrium between flux injection and rupture losses is reach ⇒ TURN OFF the PZR spray</td>
<td>YES</td>
<td>5620</td>
<td>–</td>
<td>5787</td>
</tr>
<tr>
<td>ta29</td>
<td>Check if at least one SIP is running ⇒ TURN OFF the 4th SIP</td>
<td>YES</td>
<td>5635</td>
<td>–</td>
<td>5878</td>
</tr>
<tr>
<td>ta30</td>
<td>Check if the secondary-side heat sink is available in long-term (demineralized water inventory &gt; 250 Mg)</td>
<td>YES</td>
<td>5635</td>
<td>–</td>
<td>5878</td>
</tr>
<tr>
<td>tw30-31</td>
<td>Waiting time for the borated water tanks level reach level below 1.3 m</td>
<td>Wait</td>
<td>NA</td>
<td>5939</td>
<td>5199</td>
</tr>
<tr>
<td>ta31</td>
<td>Check if the borated water tanks level &lt; 1.3 m (minimum)</td>
<td>YES</td>
<td>6200</td>
<td>–</td>
<td>6200</td>
</tr>
</tbody>
</table>

a taXX means manual action time XX, twYY-ZZ means waiting time between actions YY and ZZ, and – means not a manual action.
b Flow path actions YES, NO, Execute, Automatic and Wait: YES means select the YES flow pathway, NO means select the no flow pathway, Execute means execute the manual actions described, Automatic means automatic actions realized by the protection system, and Wait means waiting time for the next entry, in the procedure.
c NA means foreseen time not available.
7. Conclusions

After safety, planning and complying with procedures are probably the most cultivated values in the nuclear industry. The fact is that operators usually see themselves as careful planners and their identity as experts are coupled with values associated to have everything under control in advance (planning) and to know exactly what to do in a timely manner (follow the procedures). Thus, the operators do not like to see their work related to improvisation or ad hoc strategies and to address conflicting or wrong procedures. Such situations may lead to the construction of unconscious or underlying values or beliefs under which improvisation, ad hoc strategies, or being able to adapt to changing conditions is considered a bad or wrong behavior. However, sometimes, the operators faced situations were it was very difficult to follow the procedure as a script, and in many of these situations, the problems are in the procedures.

This research addresses the modeling of the time available to the operators to control safe-critical systems. Despite the time availability, clearly can be considered a factor that influences control, it is not considered in most of the operators’ tasks modeling research that focus on problem solving strategies, decision making, human error modeling, and so forth. However, operators’ activities take place in time and the available time is one of the most important determinants of whether an action is going to be successful or not (DeCortis et al., 1991; DeKeyser, 1995; Hollnagel, 2002). Few research address the actual work situation and problems faced by the operators of safe-critical systems that have to follow procedure scripts rapidly, and understand the plant evolution at the very same moment. In some situations, due to the complex nature of the work, already prepared plans and procedures, does not meet the dynamic requirements of the operators cognition, making the operators’ control tasks unnecessarily difficult. To achieve the active monitoring attitude to become a good operator, he/she needs spare time to think about the situation and plant processes. Therefore, time is always in short supply and more research on the subject is still needed. This applies to many different areas, such as industry, military operations, traffic, etc.

In this work, we exemplify our modeling tool, developing an application that simulates the task flow of a nuclear operator crew when following the procedure steps for a small-break LOCA accident. In the simulation, the correct identification of the accident type by the crew occurred during the period of automatic actions carried through the plant protection systems, i.e., the correct identification of the accident type is carried out during the first 30 min after the accident beginning.

An additional constraint was introduced with the reduction of the operation crew from 5 (actual plant crew) to only 3 operators in this model. This reduction certainly produces an increment in the workload of the operators, especially because the RO and SCO cannot have the Panel Operator help for read indicators and manipulate controls in the auxiliary panels.

This tool can also be used directly coupled with the plant simulator to simulate the plant behavior in real time. The coupling of the modeling tool to the plant simulator makes possible the introduction of commission and omission errors in the simulated scenario, and shall be investigated in near future. We conclude observing that cognitive architectures to model the operator tasks when dealing with procedures proved to be a useful low cost alternative to evaluate the cognitive compatibility of procedures in safe-critical systems.

Acknowledgements

This research was partially sponsored by the National Council of Scientific and Technological Development (CNPq – Conselho Nacional de Desenvolvimento Científico e Tecnológico).

References


