Technical Note

Human errors of commission revisited: an evaluation of the ATHEANA approach

Ed Dougherty

Science Applications International Corporation, 1309 Continental Drive, Suite F, Abingdon, MD 21009, USA

(Received 26 August 1996; accepted 12 April 1997

1 INTRODUCTION

In the interim since calling for a second generation HRA (Human Error Analysis)[1], there have been few attempts to take up the challenge. In fact, some practitioners have suggested that quantitative HRA (QHRA) is like an 'eternal question,'[2] presumably meaning that it may be unsolvable, or being more bold, claiming that people cannot be so quantified[3]. These critics suggest that qualitative HRA is what is needed and focus should be redirected from the 'obsession' to quantify. Although the author shares some of the concerns of these critics, in particular a proponent of HR assurance over HR analysis, it is too early to rush in and risk throwing the baby out with the bath water[4].

These same critics are well aware that issues linger in areas that blend risk-significance with human reliability. One of these is the so-called issue of errors of commission (EOCs). The US Nuclear Regulatory Commission (NRC) has identified this issue as a residual undeveloped element in risk assessment methodology[5]. Previous NRC research by Idaho Engineering National Laboratory (INEL) to the contrary[6–9], it is widely perceived that there is no technology to assess EOCs. However, one project under development proposes a new approach. This effort is conducted by Brookhaven National Laboratory (BNL) and goes by the acronym ATHEANA (a technique for human error analysis)[10].

Since research NUREGs often lead to regulations to which the US nuclear utilities must dedicate scarce resources in compliance efforts, it seems relevant to critique this new proposed solution to EOCs. This technical note examines ATHEANA from three perspectives: its taxonomy, its event analysis, and an example of its quantification of an EOC. In order to accomplish this, special attention will be paid to a small loss of coolant accident (SLOCA) that occurred on July 3, 1992 at Ft. Calhoun[11–15]. In the midst of what overall was exemplary handling of the event, the crew on shift committed a 'classical' EOC. This error was of negligible overall consequence in the scenario, so much so in fact that one review complimented the teamwork of the crew[13]. However, it is important to clearly identify this error as an EOC *type* along with its influencing context so as to be able to ask 'where is the precipice?' That is, where might an EOC that, in this case *after the fact* proved insignificant, have led to a riskier plant condition? The Ft. Calhoun emergency operating procedures (EOPs) related to small LOCAs will also be used to examine the example quantification in the NUREG.

Notice up front that there is much of merit in the methodology of ATHEANA, particularly in its attempt to describe how EOCs might occur, this being of importance to risk management. This note points out some soft areas that are in need of extension or correction. It would also be interesting to re-examine the INEL efforts in the area of EOCs to see whether they can be integrated with ATHEANA but this effort is beyond the scope of this note.

2 THE SMALL LOCA EVENT AT FT. CALHOUN

July 3, 1992 was the start of a US holiday weekend (the 4th of July). The Ft. Calhoun reactor is a Combustion Engineering (CE), older vintage pressurized water reactor (PWR)[16]. It was being operated with a 'split' crew because of the holiday: the SRO and ROs were from one team and the STA was from another. The reactor tripped at 11:36pm at the beginning of the night shift. Table 1 presents an event timeline in the style of a decision flow chart[17] but with the phenomena divided according to context and control[18].

Table 1. Timeline of Ft. Calhoun's LOCA evolution

Time (h:m)	Context	Control
4:33	inverter #2 alarm	precursor to trip
6:36–23:30	series of trouble alarms with above	
23:36	R_x trip on PZR high pressure quench tank (QT) press/level alarms both backup charging pumps start initial LOCA signs	operators enter EOP-00
23:37	PZR pressure drops and begins to recover	
23:43	PZR pressure reaches 1925; then starts to decrease PPLS/SIAS/CIAS/VIAS actuate	operators block PORVs based on lowering pressure
23:44	panel RCS pressure indicator lags	operators lose subcooling margin
23:46		EOP-00 completed transfer to EOP-20 SIA 2B&2C (2/3 SI pumps) shutdown according to Floating Step for terminating SI (**EOC**)
23:52		Shift Supervisor declares ALERT based on Emergency Alert Levels 1.10
23:55	QT disk ruptures; containment cues	LOCA into containment noted
23:56	emergency feedwater storage tank (EFWST) low level alarm	operators begin ex-control room action (**EXCR**) to refill tank
0:04		Shift Supervisor directs plant cooldown
next hour		SI and charging started and stopped to optimize injection
1:10	EFWST low level alarm clears	refill successful
1:21		TSC assumes Site Director responsibilities
1:22		operators put non-safety 4160 kv busses on 345 backfeed; **EXCR**
2:18	QSPDS indicates possible voiding in RV head; may have been the result of the EOC	THIS WOULD REQUIRE THE RESTARTING OF HPSI IF OFF
8 hrs		operators overcome various minor difficulties in shutting down
6:30		TSC with NRC concurrence downgrades event to UNUSUAL EVENT
10:53		SI-1A started in preparation for shutdown cooling (SDC)
13:12		SDC established per EOP-20; **EXCR**
13:52		TSC allows exiting EOPs

The initiator was an electrical fault caused by a voltage oscillation upon returning a non-safety-related inverter to service after failing early that morning. The heat sink for the reactor was temporarily lost because of this fault, which tripped the reactor. The accompanying pressure buildup in the reactor coolant system (RCS) lifted power-operated relief valves (PORVs) as well as at least one pressurizer code safety valve (PSV). The PORVs re-shut with the return of the heat sink that lowered RCS pressure enough to allow them to re-close. However, the PSV incrementally 'recalibrated' itself and remained open until pressure was reduced to 1,000 psi when it only partially closed. This open PSV was the source of a small LOCA, which was nonisolatable.

The operators on crew did not know that the PSV had remained open. However, the EOPs[19–23] do not require that either the specific assessment of the situation, i.e., the cause of the LOCA, or the isolation of the LOCA be accomplished. These are obvious 'niceties.' The EOPs do call for the operators to maintain 20°F subcooling margin (SCM), which is an optimal cooling path (see Fig. 1) but not a risk-significant one necessarily. To do so they must monitor RCS pressure. The Ft. Calhoun control board contains one pressure indicator on the front panel but has two redundant ones on a back panel not visible to the crew. This separation of crucial instrumentation is clearly a human engineering deficiency (HED). The front-panel indicator failed high but tracked the correct pressure, misleadingly indicating sufficient SCM (note that a high pressure reading for any temperature on the figure would falsely indicate more cooling than exists). Apparently, in the crush of indications and activities, the RO could not go to back of the panel to confirm the reading. Since he actually had no reason to do so based on his panel indicators, this was a failure in situation assessment but could not reasonably be called an error[24], at least not his.

However, a qualified safety parameter display system (QSPDS) compares the three RCS pressure instrument readings but was cryptically and confusingly indicating the mismatch, a second HED. The senior reactor operator (SRO) noted this but apparently mistakenly discounted this indication as an inoperable QSPDS. Notice that the SPDS, industry-wide, has had a problem of availability and operability during the very events that require an SPDS. Eventually, the shift technical advisor (STA), with whom the operators did not normally work, paged down the QSPDS displays to find the actual readings causing the mismatch.

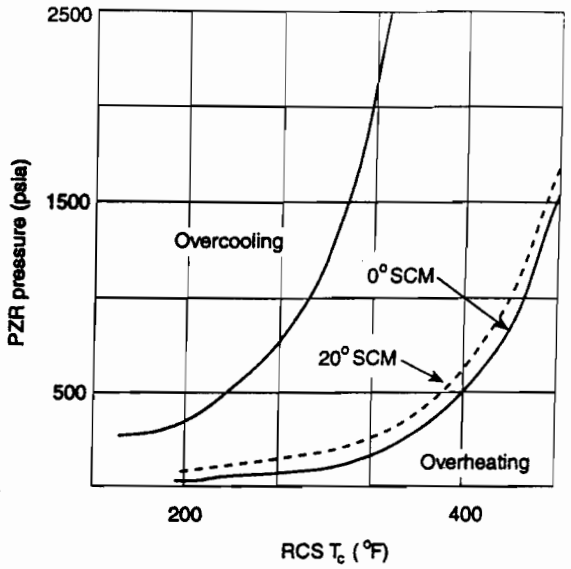

Fig. 1. RCS pressure versus RCS temperature and SCM.

He reported to the SRO that the front-panel reading was inconsistent with the back panel readings. The panel operator swore by his reading since no other panel indicator showed a problem and the SRO mistakenly decided to believe the panel operator, with whom he was familiar. Notice that the acceptance of the STA in nuclear power plant crews has also been an industry-wide problem.

Fig. 2 show the crew 'dynamics' of the situation. The SRO's decision was a mistake; since the operators did not increase safety injection (SI) to compensate for the low SCM, this could be labelled an error of omission (EOO). However, the operators apparently reduced SI according to the EOP (see Table 1 at 23:46) and the faulted indicator. Hence, the error could be termed an EOC.

3 ATHEANA'S TAXONOMIC PROBLEMS

This note significantly expands on an earlier critique of ATHEANA[25]. As the description of the Ft. Calhoun SLOCA indicates, the use of the general phenotype[26] of commission, i.e., EOC, is not always straightforward in the case of an event involving crew dynamics in a highly proceduralized context. ATHEANA is about commissions that are also either mistakes or even deliberate actions which are termed circumventions. In other words, there is a strong element of situational assessment and/or decision making underlying the error, which leads some to the term 'cognitive error.' The problem with this overt description, i.e., the commission, is that cognitive errors of omission (EOOs) are not particularly distinct from them, particularly in a team situation. Notice that either a mistake or a circumvention may be either a commission or an omission. The notorious failure to attempt feed and bleed[27] was a deliberate, and after the fact, successful circumventive omission. The error basis is the same for commissions or omissions and the distinction is causally irrelevant.

ATHEANA raises other taxonomic issues as well. First, some of the language used in ATHEANA is unfortunate, mostly because of the attempt to be taxonomically precise and descriptive while having to use a living language. ATHEANA adopts Reason's taxonomy of human error[28]: slip, lapse, mistake, and violation[29], which are all termed unsafe acts. ATHEANA adopts 'unsafe acts' and, despite the problems with the concept[30,31], substitutes 'circumvention' for 'violation'. However, the latter change in terminology is misleading, since violation at least has a dictionary meaning that is a legal analog to what is intended whereas circumvention connotes sneakiness, which is not meant. (Other possible substitutes for violation-challenge, contravention, defiance, intervention-also carry derogatory baggage presumably unintended in this application.)

The ATHEANA definition for commission error[32] is:

> an overt, unsafe act that, when taken, leads to a change in plant configuration with the consequence of a degraded safety-state.

Unfortunately the phrase 'overt, unsafe act' has a clear ordinary meaning of an action knowingly unsafe, which

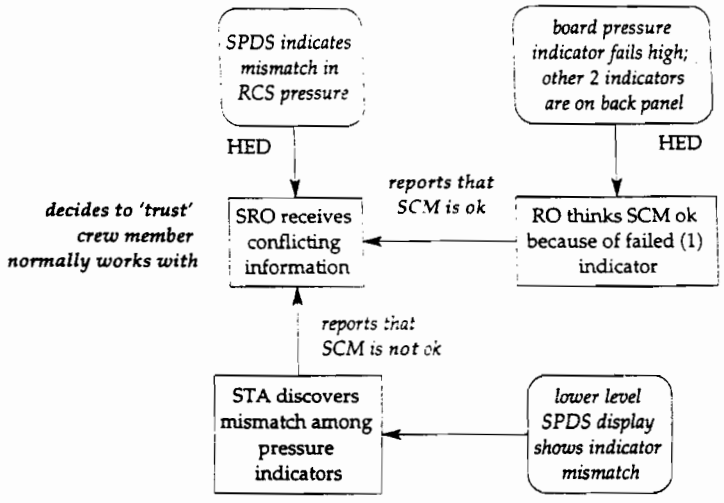

Fig. 2. The crew commission error on 2 July 1992

Table 2. An alternative error taxonomy

Error source	Phenotype	Error label	Failure status
1. failure in cognition	commission	a. mistake	e. harm
		b. circumvention	f. no harm
2. failure in cognition	omission	a. mistake	e harm
		b. circumvention	f. no harm
3. failure in cognitive control	commission	a. slip	e. harm
		b. lapse	f. no harm
4. failure in cognitive control	omission	a. slip	e. harm
		b. lapse	f. no harm

makes the technical usage by ATHEANA rather alarmist. Also, one must wonder whether the consequential 'unsafety' is merely temporary or 'permanent,' i.e., the latter being that it caused actual harm or loss. Finally, the ATHEANA definition is more restrictive than Reason's, adopting the consequence criterion-plant safety is degraded—rather than a potential loss of safety, i.e., the act is performed 'in relation to the presence of a particular hazard.'[28] At least Reason's definition recognizes that, particularly, violations are unsafe only in potential, that they might prove, after the fact, to have been the 'correct' and safest option. The possibility space evolves as follows:

1.	error	with harm
2.	error	with no harm
3.	circumvention	with harm
4.	circumvention	with no harm.

Clearly, HRA may need to consider all of the four possibilities, but it would seem to have been better off not using the phrase 'unsafe act' at all, merely recognizing errors (slips, lapses, mistakes) and circumventions.

As a candidate taxonomy, Table 2 blends overt behaviour with its performance impetus. Table 2 is, of course, an abbreviation of what might be displayed alternatively as 'logic' tree with a dozen more end states. In this scheme, there are failures in cognition or in the control used to execute the cognition[33]. Then there are the overt phenotypes, commission and omission. Each of the resulting errors may be labelled as mistake or circumvention for cognitive errors or slip or lapse for cognitive control errors. The error then is a failure depending upon whether the failure state leads to harm or not. In this light, ATHEANA as well as the NRC should be concerned with both taxons 1 and 2 but ATHEANA generally is not. Although the HRA concern is restricted to the failure status 'harm,' the development program must search for cognitive errors without harm as *precursors*. This exposes a fundamental weakness in HRA and risk analysis generally: the extrapolation from precursor to real or postulated occurrence is an intellectual minefield. In the language of the table, the Ft. Calhoun error was a 1af error, i.e., a failure in cognition, a mistake leading to a commission but no harm. The Davis-Besse error was a 2bf error, a failure in cognition, a circumvention leading to an omission but no harm (except, of course, that the NRC shut the plant down for fourteen months).

The nuances in semantics described above do not seem to detract from the value or the primary intent of ATHEANA and are not in that setting particularly significant. The second feature, event analysis, however, is a significant issue and one aspect is turned to next.

THE FORCE OF 'FORCING CONTEXT'

One of the major points of ATHEANA's analysis of events is that situational circumstances can be so contrary to successful human performance that the error is 'forced.' ATHEANA[10], in its small LOCA example, purports to examine such an error forcing context (EFC). The example in the ATHEANA NUREG is the inappropriate termination of safety injection (SI), the primary means of cooling the reactor core, during a small LOCA. When cooling is sufficient according to instrumented cues, then the operators are instructed by procedure to terminate SI according to *HPSI Stop and Throttle Criteria* in the Ft. Calhoun procedure for LOCA response. This occurs at step 8A, which is a floating step for all EOPs at Ft. Calhoun. It is not the only place in the procedure set that calls for this action. The step is important for optimal cooling and to meet the goal of avoiding overcooling, a rather insignificant problem relative to an overheated or melted core. More significantly, maintaining SCM meets the goal of avoiding reactor voiding during a cooldown, a phenomenon that reached alarming proportions at TMI.

Notice that the language of error 'forcing' goes beyond that of Swain's 'error likely situation'[34] and seems even more restrictive than Fujita's 'error prone situation.'[35] In fact, adopting Martin Stutzke's view of the event described in ATHEANA, 'error forcing' is a contradiction in terms, if taken literally. For if the action is forced then there is no chance for success and hence error is not appropriate; whereas, if the action is an error, then success was a possibility, and, hence, the situation is not really forcing.

The 'force' to the action of SI termination is presumed to be a failure of *both* reactor coolant system (RCS) pressure and pressurizer (PZR) level indications. In PWRs, pressure and temperature are combined to determine subcooling margin (SCM) which is supposed to be maintained at about 20°C (the dashed line in Fig. 2). Loss of SCM can eventually lead to reactor voiding which will be indicated by

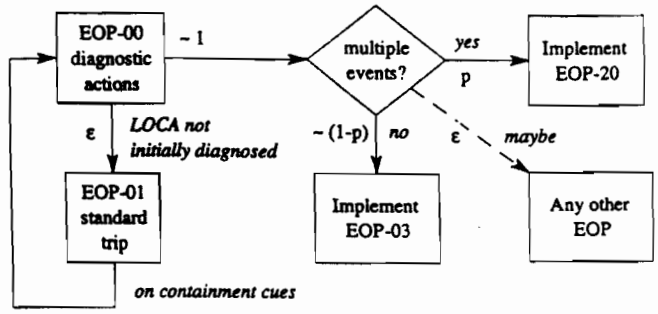

Fig. 3. Possible FCS EOP paths.

the reactor vessel level monitoring system (RVLMS). Reactor voiding can cause uneven overheating of the core and core melting can eventually occur. The time to melt, however, will be several hours. Also, EOP-03, step 5·6e, requires SI flow to be positive for RCS pressures less than about 1550 psi according to Attachment 3, *Safety Injection Flow v. Pressurizer Pressure*. Hence, the SI termination condition will not only not be forcing, it may not even be likely.

Floating step A (floating steps are section 8 of all EOPs), *HPSI Stop and Throttle Criteria*, indicates two possible actions. If all of the following stop and throttle criteria are satisfied:

1. RCS subcooling is greater than or equal to 20°F.
2. PZR level is greater than or equal to 45% and not lowering.
3. At least one steam generator (SG) is available for RCS heat removal.
4. RVLMS indicates level is at or above the top of the Hot Leg.

Then the operators are directed to turn HPSI off. In the situation assessed by ATHEANA, criterion 1 is met because pressure fails high and PZR level is (presumably) failed stuck above the 45% level. SG heat removal is assumed operable and RVLMS does not yet indicate low level. If HPSI stop and throttle criteria *cannot be maintained*, then the floating step directs the operators to (re)initiate HPSI flow by performing the following steps:

1. Start all of the HPSI Pumps, SI-2A/B/C.
2. Open all HPSI Loop Injection Valves.

Note that the step has a caution: as natural circulation develops, the expected rise in T_h will reduce subcooling which may jeopardize HPSI stop and throttle criteria. This actually might lead operators not to completely throttle HPSI or at least delay its termination.

Upon onset of containment cues (19 minutes into the FCS event), it is difficult to believe that whatever procedure the operators were using that a LOCA would not be diagnosed. The operators at Ft. Calhoun (and at all CE reactor plants) have the option of combating a LOCA using the LOCA procedure, EOP-03, or using the *Functional Recovery Procedure*, EOP-20. Fig. 3 indicates the likely paths through the EOP system for FCS. A description of the overall EOP system for a CE reactor plant has been described previously[36]. There is little reason to believe that the operators would misdiagnose the LOCA as a LOCA, at least nothing in the description of the ATHEANA example would 'force' it and it isn't so assumed. However, the delay in the convincing information might be a few minutes (e.g., 19 in the FCS event) and the operators might spend some time in EOP-01, which is directed toward routine trips. Because of the tendency of FCS operators to prefer EOP-20 under most non-routine conditions because it 'works' in all circumstances, the probability, p, in the figure is likely to be close to unity for FCS. However, at other CE reactor plants, the option of EOP-03 may be more likely than at FCS. (Notice that the Westinghouse and Babcock and Wilcox PWRs have somewhat different EOP systems and especially the BWR EOP system is quite different; no claims are made relative to these EOP styles.)

The FCS event would have been mitigated well with EOP-03 but the FCS operators opted using EOP-20. In the FCS SLOCA event, EOP-20 was entered ten minutes after the onset of the event. Had EOP-03 been opted, however, one of the primary steps is to ensure SI flow is acceptable per Attachment 3, *Safety Injection Flow vs. Pressurizer Pressure*. Depending on whether the RCS pressure and level indications lagged their actual values or failed stuck high, this step would direct the operators to institute HPSI and the EOC would be cured. In the case of a stuck indicator, the arrival of containment cues would be contrary to the RCS cue and the operators would have another opportunity at situation assessment. In the case of lagging indicators, the reinstating of SI would be later than optimal. In either case, the EOC would be cured.

Furthermore, EOP-03, section 8·0, Floating Steps, part O, RCS Heat Removal, tells the operators to:

Verify adequate RCS Heat Removal via the S/Gs by both indications:

1. At least one S/G has wide range level greater than or equal to 20%.
2. RCS T_c temperatures are stable or lowering [this criterion would fail eventually].

If any of the following criteria are satisfied:

1. both S/G wide range levels are less than 20%
2. an uncontrolled rise in RCS T_c is greater than 5°F [this criterion would hold eventually]then go to Success Path HR-4 of EOP-20.

That procedure section directs the operators to implement *once-through-cooling* (OTC), i.e., what the industry generically terms feed and bleed, which would then direct them to turn the HPI pumps back on (along with opening a PORV).

When multiple symptoms exist, the CE EOPs direct operators to the *Functional Recovery Procedure*, as its termed at Ft. Calhoun, EOP-20. It is EOP-20 that the Ft. Calhoun operators chose to implement in the July 1992 event. In this EOP, the operators are directed to maintain various safety functions and at least for a while (apparently

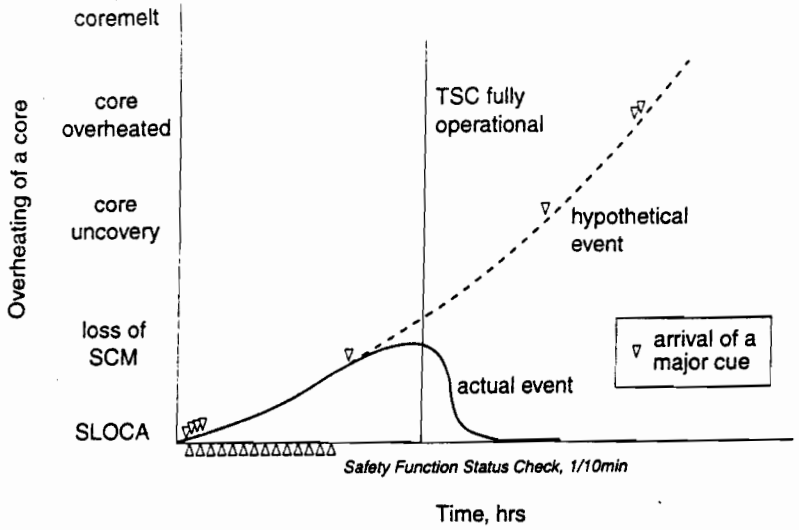

Fig. 4. Heatup chronology of SLOCA.

some nineteen minutes in the FCS event), these functions might appear satisfied because of misleading RCS indicators. However, in a few (in the FCS event, 19) minutes, the quench tank rupture disk would rupture from the inventory pouring from the LOCA. At that time, LOCA containment cues would begin to arrive: increasing containment pressure, sump level rising, radiation in the containment, etc. It is very difficult at this point to believe that the operators would continue to leave all HPSI turned off. If not, the EOC would be cured.

In EOP-20, the first four safety functions would likely be acceptable. Safety function 5, *RCS and Core Heat Removal*, is accomplished by means of one of five 'paths':

1. HR-1 forced circulation, no SI,
2. HR-2 natural circulation, no SI,
3. HR-3 steam generator heat sink with SI,
4. HR-4 once-through-cooling, and
5. HR-5 shutdown coolingin that order. The assumption of the termination of SI will eliminate the acceptability of path HR-3. The criteria of HR-1, 2, and 4 include:

1. core $\Delta T \leq 10°F$ and not increasing
2. $T_c \leq 545°F$ and not increasing
3. RVLMS indicates no reactor vessel voiding
4. difference between CETs and RCS $T_h \leq 10°F$
5. RVLMS indicates level above the top of the hot leg
6. CET temperature $<$ superheat
7. RCS pressure $<$ 1350 psi or decreasing.

At various times over the postulated scenario of an SLOCA with terminated SI, each of these criteria would fail with the exception of item 7 with pressure failed high. Fig. 4 depicts the arrival of various strong cues over the core heat up that would result from the supposedly unrecognized RCS inventory depletion with SI terminated. Criterion 7 would appear to fail if the failure of RCS pressure was of the mode: stuck high; otherwise, a tracking fault, as was the case at Ft. Calhoun, would mean that criterion would not fail. If HR-1, HR-2, and HR-3 could not be determined to be acceptable, then the operators are supposed to attempt OTC to satisfy HR-4. This would cure the EOC.

Finally, EOP-20, Attachment 14, *Void Elimination*, would direct operators to use (i.e., turn on) HPI to eliminate void indicated by the RVLMS. This would cure the EOC.

These new cues, most more significant relative to the critical safety function hierarchy than previous ones, would likely arrive after a full complement of the technical support centre (TSC) staff has become available. The TSC consists of operators and management called from home in emergency situations. These cues are also strong enough to break an early mindset, i.e., that HPI is not needed. Hence, relative to the EOPs and the dynamics of cues during an SLOCA, the following points may be made:

1. Failure to realize that a LOCA is ongoing is not credible. EOP-00 Diagnostics and EOP-03, Attachment 1, *Containment Pressure*, etc. indicate LOCA.
2. Given a recognized LOCA, it is very unlikely that operators would think that HPI stop criteria are met.

EOP-00 6·0, Diagnostic Actions, based on containment pressure or sump level
EOP-03 5·2a, Break Identification (Attachment 1), based on containment pressure
EOP-20, 7·3, RCS Inventory Control, IC-1c, RVLMS indicates level above top of hot leg
EOP-20, 7·3, RCS Inventory Control, IC-2a, SI flow per attachment 3.

If HPI were terminated, then there are many later, strong cues that would direct operators to restart HPI.

The above discussion indicates an error potential during an SLOCA as summarized in Table 3. The recognition of a LOCA is not contested. However, for a while at least the operators terminate SI due to failure of instrumentation. ATHEANA calls this an EOC but it seems unfair to call an 'E' at all. However, ATHEANA rather cavalierly postulates that the error persists despite the arrival of a variety of

Table 3. Potential for cognitive error in SLOCA

Possible cognitive failure	Likelihood	Reason
Fail to recognize event as LOCA (cannot be considered EOC)	not credible	plethora of post-TMI cues and EOP support (ATEANA does not assume this)
Fail to maintain SCM, throttling SI (EOC)	occurred at FCS	instruments lagged and crew dynamics was not optimal
Inappropriately decide to terminate SI (EOC)	plausible initially	faulted primary cues; depends on actual kinds of faults
Persist in this situational assessment (EOO)	not credible	EOPs, TSC, strong later contrary cues

strong cues, a procedure set developed to avoid EOCs, and an independent source of situation assessment in the staff of the TSC. Error technologists know this can happen in some cases but the ATHEANA analysis does not give any credit for the post-TMI modifications to EOPs.

'The EOPs should thus be function-oriented (with provisions for specific event-based actions, if desired)... Function-oriented EOPs provide the operator with guidance on how to verify the adequacy of certain functions and how to restore and maintain those functions when they are degraded.'[37]

Further, their advantage is that 'the operator does not have to immediately diagnose an event ... to maintain the plant in a safe configuration.'

This extensive context of EOPs alone behooves ATHEANA and any HRA approach to take more seriously what Erik Hollnagel dubbed as the 'term of '93' as he issued his book on context and control related to HRA[3]. Context is a label surrogate for the complex of influences on a human performance. As can be found from analysis of actual and even simulated events, context can be quite varied[29,36,38–40]. Table 4 hints at the complex context of the FCS SLOCA event. Table 5 shows the barriers established post-TMI to avoid persistent EOCs. As the table notes (in bold), only some of the resources available were faulted, and then some only partially. From such reviews, it is quite obvious that the situational circumstances referred to as context drives such human cognitive performances as situational assessment and the decisions that are made from it. The result, often, is that the insights from event analysis are totally dependent upon the event analyst.

Neither ATHEANA nor a reasonable assessment indicates any credibility of the operators not realizing that, among possibly other things, a LOCA is ongoing. This is due to the many post-TMI modifications to plants because of the failure at TMI. There is (and was during the FCS event) a potential for an EOC related to maintenance of SCM. For a considerably long period (over 2 and a half hours at FCS), the loss of SCM would have little impact, although it could lead to suboptimal cooling and eventually voiding in the RCS.

The postulated inappropriate termination of SI is the EOC postulated in ATHEANA and it is plausible, at least initially in the event progression due to faulted primary instruments. However, the termination would occur only with a stuck high indication of pressure and level, since lagging indicators would lead to 'normal' LOCA mitigation that is somewhat late relative to optimal. However, it is the persistence of this assessed situation that is most troublesome in the ATHEANA analysis. One might concede that the example was provided only as a 'screening' example to demonstrate concerns with EOCs had not the producers of the example insisted that context and, in particular, forcing context was so crucial to the new HRA approach. Notice, finally, that the persistence of the situation assessment is no longer an EOC but an EOO.

Table 4. Factors leading to an EOC

Occurrence	Problem	Impacts cognition
split crew; STA not well-known	latent influence	decision making
STA is not well accepted	industry-wide latent influence	decision making
event on a holiday	latent influence	all
event at night	latent (circadian) influence	all
event at shift initiation	higher attention; lower readiness	all
stuck-open PCSV (industry emphasizes stuck-open PORVs but not PCSVs)	strong but wrong expectation	diagnosis
unusual pressure evolution	failed to recognize open PSV	diagnosis
failed indicator	misdiagnosis	diagnosis
redundant indicators on back panel	HED	diagnosis
cryptic SPDS	HED	situation assessment
acceptance of SPDS	industry-wide latent influence	situation assessment
strong but wrong assessment by RO	forced but not an error	diagnosis
STA is not well known	latent influence	decision making
SRO assumes RO correct	mistake (EOC)	decision making

Consequence: loss of SCM; suboptimal response to the event with insignificant risk because of the EOPs.

Table 5. Redundant barriers to persisting EOCs

Indications	Procedures	Personnel
pressure	specific EOP	**reactor operators** (ROs)
level	safety function status check	**senior reactor operator** (SRO)
pressurizer	floating steps (A & O)	**shift technical advisor** (STA)
RVLMS	EOP-20 (in particular HR-4)	shift supervisor
temperature		technical support center (TSC)

Bold indicates barrier was at least partially 'faulted'.

5 TOWARD A MORE REALISTIC QUANTIFICATION

The ATHEANA quantitative estimate of the sequence frequency would dominate most PRA/IPEs. Its generation, by example, also defies its own rule that the situation 'forces' human failure. Moreover, the example fails to take in all of the context as noted above.

First, it must be realized that a small LOCA-in most large capacity plants such as Surry and even smaller plants like Ft. Calhoun-is a slowly evolving event, vis-à-vis core heat up (Fig. 4 hints at this). This gives a lot of time for a lot of people to help make any EOC right. Hence, there is legitimate reason to credit the presence of the vast redundancy built into the nuclear plant/operator system since TMI.

The ATHEANA analysis of the SLOCA SI termination sequence is synopsized in Table 6. It is decomposed into four events. The first is the 'initiator,' i.e., the occurrence of the small LOCA. Risk assessment typically quantifies its occurrence rate to be no more than 2×10^{-2} yr. A stuck-open PORV is then assumed to be the cause of the LOCA; a probability of 0·5 is assigned this. But the analysis then assumes that the PZR level fails because of this kind of LOCA, which is clearly incorrect. The third event assumes a common-cause failure of 2 of 4 high pressure indicators fail stuck high. The conditional probability of this event is calculated to be 0·01 using 18 month exposure time (i.e., this vital instrumentation is not checked but once every year and a half; the more likely duration is a month, or a factor of 18 less). Finally, the fourth event is 'operators believe HPI termination criteria met and fail to recover.' This is quantified at 0·15 which is justified as an error forcing context due solely to the fact that the event might occur during 2–6am. The ATHEANA analysis assumes that circadian effects force not only the original error, which as noted above is not really an error, but its persistence in spite of all the redundancy of Table 5. It should be noted that Swain regards shift work as the 'norm' for nuclear power plants and does not recommend any adjustment from basic probabilities of error [34].

The total core damage frequency is the product of these, or $1{\cdot}5 \times 10^{-5}$ yr. The analysis includes the 2nd and 3rd event with the fourth as the human failure event, but this is not warranted.

So, let's add some of the context discussed above. Error rates will be taken from INTENT (for EOCs) and THERP for other considerations. INTENT identifies error type #12: 'symptoms noticed, but incorrect interpretation,' which seems to be the closest match to the error conceived by ATHEANA. INTENT suggests a range on the probability of such an EOC from an upper bound of 0·1 to a lower bound of 0·0042 [6]. The risk assessment tradition of assuming this to be the 90% 'confidence' range of a lognormally distributed parameter yields:

1.	median	0·02
2.	error factor	5
3.	mean	0·032.

An expert in circadian effects suggest a factor of 6 increase in failure probability for the early hours of the morning (not a 100% reduction in reliability as assessed in the NUREG)[41] which raises that basic human error probability to 0·19. Not a bad comparison, so far as it goes. However, the SRO makes the actual EOC, if one exists, and the RO's actions at the board are presumably 100% dependent on that decision. But the STA is available, as is the shift supervisor and the TSC (some 30–60 min later). The FCS SRO ignored the STA but he might not; it seems that high dependency is a fair assessment of his contributing positive information using the SPDS (and even this probability will dominate the failure probability of the SPDS) Swain assigns 0·5 to this[34]. The shift supervisor will be ignored (it is early morning) but the TSC, however, is virtually independent from the crew, and will be available. To be conservative, a moderate dependency factor is used, i.e., 0·14. Hence, a model of the persistent EOC, that

Table 6. Alternative quantification makes the difference

Sequence element	ATHEANA estimate	Contextual estimate
small break LOCA	2×10^{-2}/yr	2×10^{-2}/yr
failure of pressurizer level	0.5	0.5
2/4 high pressure indicators stuck high	0.01	0.01
operators fail to recover	0.15	2.5×10^{-4}
TOTALS	1.5×10^{-5}/yr	2.5×10^{-8}/yr

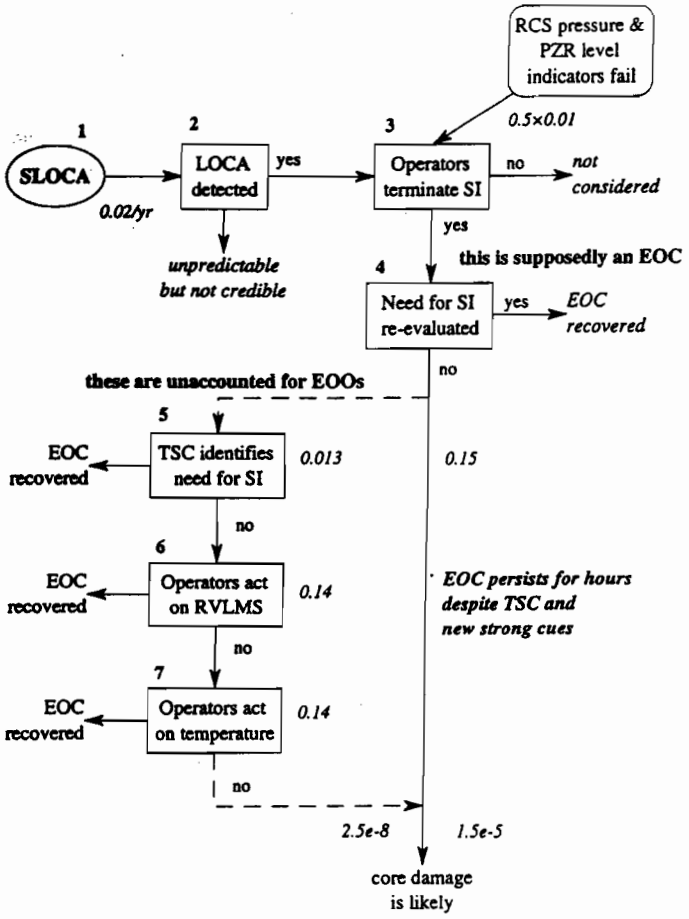

Fig. 5. Considering a more realistic context.

more realistically accounts for the actual personnel who will be available, makes for an HFE probability of:

$$0{\cdot}032 \times 6 \times 0{\cdot}5 \times 0{\cdot}14 = 0{\cdot}013.$$

This error rate improves on the ATHEANA estimate by a factor of 9, nearly an order of magnitude. It is necessary to realize that the INTENT value, the circadian factor and the two dependency factors are quite likely to be very conservative estimates.

Now, over the next few hours, the containment functions arrive, the RVLMS cues arrive, and the core and RCS temperature indications arrive. These are different enough (and this was the intent of all post-TMI training, the EOPs and the qualifying of instrumentation) that they cannot be considered completely dependent on the previous EOC. The cues themselves are rising up the hierarchy of significant safety function indicators. They will not be missed. So at worst, a couple more moderate dependency factors should be tacked onto this analysis for the TSC (the crew is not in command at this point) and the result is:

$$0{\cdot}013 \times 0{\cdot}14 \times 0{\cdot}14 = 0{\cdot}00025$$

or a factor of 600 improvement on the ATHEANA estimate. Many people would think this analysis very conservative. The resulting sequence frequency is $2{\cdot}5 \times 10^{-8}$ yr without considering quantitative adjustments of the system from the postulated ATHEANA EOC considering a more representative context. Fig. 5 synopsizes this re-evaluation by indicating some of the omitted significant context. This example indicates the justification that has been used in risk assessment to ignore this kind of human performance: the post-TMI modifications to all US nuclear power plants has indeed reduced the potential for EOCs to an acceptable level.

6 CONCLUSION

The point of this technical note critically discussing the latest rendition of the ATHEANA approach is not to put down what are obviously honest concerns related to errors of commission. It is not to demonstrate a 'superior' quantification, although publishing a calculation that is so obviously flawed does disservice to the authors, the NRC, and especially the nuclear industry, and a superior calculation is readily feasible. However, the note is offered as a challenge: HRA must account for context—all of its context. No matter the premature status of a project, at least this fact must be respected.

Another point is to indicate that, in a precursor such as the event at FCS, many things do go right. In that event, these include:

1. The procedure-to-safety function cue relationships are robust enough to accomplish their primary mission: to break any early mindset of the operating crew and lead to self-recovery.
2. The TSC is online and effective in time to provide its intended redundancy.
3. The reactor system is error-tolerant enough to survive temporary, but extended, suboptimal operation.
4. The operators, probably because of the older vintage of the plant, are highly skilled in performing ex-control actions during an emergency response (three during the FCS event).

An adequate second generation HRA, such as ATHEANA, must account for this prowess of the response system as well as search reasonably for credible opportunities in its failure to be realistic.

There are many ideas floating around the HRA literature that need to be pulled into a new HRA approach such as ATHEANA. They include the NRC-sponsored work with EOCs by INEL, as well as a variety of ideas such as those listed below in no preferential order:

1. the structure and potency of cue pattern types as they arrive during the evolution of a scenario[42],
2. the, often convoluted, logical structure to EOP sections[43],
3. the decision making that does go on in control rooms, which may be explicated by cognitive or goal-means analysis[17,18],
4. the opportunities of going awry in complex procedure

5. the scenario/EOP mismatches that force operators to use the procedures innovatively[31] or even to have to circumvent them, on the spot or as a habituated informal procedure[45], and
6. the dynamics of human performance[46,47].

Until HRA modelling can model what Hollnagel[48] has called cognitive reliability and produce an HRA model that is, to use Joseph Fragola's phrase, 'a within-the-black-box model,' HRA is best applied, and regulators and the industry are best served, by examining the full context of the EOPs, additional personnel and other redundancies created post-TMI with the seriousness their development deserves. Until so, the kind of EOC that is proffered by the latest ATHEANA analysis has negligible risk just as risk analysts have always assumed to be the case.

ACKNOWLEDGEMENTS

Of invaluable assistance in the Ft. Calhoun example was Jay Fluehr, a former SRO of the Omaha Public Power District's PRA team, as well as the operators who participated in the FCS event. However, as always, the interpretations and claims in this note are those of the author and are not intended to represent OPPD or anyone else.

REFERENCES

1. Dougherty, E. Human reliability analysis—where shouldst thou turn? *Reliability Engineering & System Safety*, 1990, **29**(3), 283–299.
2. Mosneron-Dupin, F., 'Is Probabilistic Human Reliability Assessment Possible?' Topic 6, *EdF International Seminar on PSA and HRA*, Paris, 21–23 November 1994.
3. Hollnagel, E., What is a man that he can be expressed by a number? In *Probabilistic Safety Assessment and Management*, ed. G. Apostolakis. Elsevier, NY, 1991.
4. Dougherty, E. Is human failure a stochastic process? *Reliability Engineering & System Safety*, 1996, **55,** 209–215.
5. US Nuclear Regulatory Commission, *Final Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities*, SECY-95-126. Washington, DC: USNRC, 16 May 1995.
6. Gertman, D. I., Harold, S. B., Lon, N. H., Karen, S. S. and Heidi, A. H. INTENT: a method for estimating human error probabilities for decisionbased errors. *Reliability Engineering & System Safety*, 1992, **35**(2), 127–136.
7. Gertman, D. I. Representing cognitive activities and errors in HRA trees. *Reliability Engineering & System Safety*, 1993, **39**(1), 25–34.
8. Gertman, D. I., Haney, L. N. and Nathan, O. S. Representing context, cognition, and crew performance in a shutdown risk assessment. *Reliability Engineering & System Safety*, 1996, **52**(3), 261–278.
9. Hahn, H. A., Gertman, D. I. and Harold, S. B. Applying sneak analysis to the identification of human errors of commission. *Reliability Engineering & System Safety*, 1991, **33,** 289–300.
10. Cooper, S. E., Ann, M. R. -S., John, W., Gareth, W. P., Dennis, C. B., William, J. L., Taylor, J. H. and Barriere, M. T. A technique for human error analysis (ATHEANA). NUREG/CR-6350. USNRC, Washington, DC, May 1996.
11. Omaha Public Power District, Licensee event report: reactor trip due to inverter malfunction and subsequent pressurizer safety valve leak. LER-285-92-023, 3 August 1992.
12. Rosenthal, I. E., Human performance study report — Fort Calhoun Station (7/3/92), USNRC Office for Analysis and Evaluation of Operational Data, letter to T. M. Novak, Director of OAED, 25 September 1992.
13. Meyer, O. R., Hill, S. G. and Steinke, W. F., Studies of human performance during operating events, 1990–1992, NUREG/CR-5953. US Nuclear Regulatory Commission, Washington DC, January 1993.
14. Kauffman, J. V., Lanik, G. F., Spence, R. A. and Trager, E. A., Operating experience feedback report—human performance in operating events. Commercial Power Reactors, NUREG-1275, vol. 8. US Nuclear Regulatory Commission, Washington DC, December 1992, pp. 13–14.
15. Kauffman, J. V., Engineering evaluation: operating events with inappropriate bypass or defeat of engineered safety features, AEOD/E95-01. US Nuclear Regulatory Commission (Office for Analysis and Evalution of Operational Data), Washington DC, July 1995.
16. Hackerott, H. A., Jay, J. F., Rick, C. K. and Ed, D., Early A/M actions in an older vintage plant. *Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, PSA "93, Clearwater, FL*, American Nuclear Society, 26–29 January 1993, pp. 868–872.
17. Roth, E. M., David, D. W. and Harry, E. P. Jr. Cognitive simulation as a tool for cognitive task analysis. *Ergonomics*, 1992, **35**(10), 1163–1198.
18. Hollnagel, E., *Human Reliability Analysis: Context and Control*, Academic Press, London, 1993.
19. Fort Calhoun Station, EOP-00 Standard post trip actions. Omaha Public Power District, Omaha, Nebraske, 13 February 1996.
20. Fort Calhoun Station, EOP-01, Reactor trip recovery. Omaha Public Power District, Omaha, Nebraska, 19 May 1995.
21. Fort Calhoun Station, EOP-03, Loss of coolant accident. Omaha Public Power District, Omaha, Nebraska, 13 February 1996.
22. Fort Calhoun Station, EOP-20, Functional recovery procedure. Omaha Public Power District, Omaha, Nebraska, 12 April 1996.
23. Fort Calhoun Station, EOP/AOP Attachments. Omaha Public Power District, Omaha, Nebraska, 12 April 1996.
24. Marsden, P. and Erik, H., Human computer interaction and models of human error for the accidental user. In *Proceedings of the 7th European Conference on Cognitive Ergonomics, Bonn*, Germany, 1994.
25. Stutzke, M. A., Ed, M. D. and Carol, S., Finding the dominant risk: a review of the ATHEANA method. In *Proceedings of the ANS/ENS 1996 International Conference and Embedded Topicals, November 10–15, 1996*. American Nuclear Society, La Grange Park, IL, 1996.
26. Hollnagel, E. The phenotype of erroneous actions. *International Journal of Man-Machine Studies*, 1993, **39,** 1–32.
27. US Nuclear Regulatory Commission, Loss of main and auxiliary feedwater event at the Davis-Besse plant on June 9, 1985. NUEG-1154. USNRC, Washington, DC, July 1985.
28. Reason, J. T., *Human Error*. Cambridge University Press, Cambridge, UK, 1990.
29. Reason, J. T. The Chernobyl errors. *Bulletin of the British Pschyological Society*, 1987, **40,** 201–206.
30. Dougherty, E. M. Violation-does HRA need the concept? *Reliability Engineering & System Safety*, 1995, **47**(2), 131–136.
31. Dougherty, E. M., Is human reliability enhanced by following procedures? *ANS 1994 Winter Meeting*, Washington, DC, 13–17 November 1994.

32. Mike, T., Barriere, W. J., Luckas, S. E., Cooper, J. W., Dennis, C. B., Ann, R. -S. and Thompson, C. M. Developmental status of an improved method for conducting an integrated HRA/PRA based on operating experience. In *Proceedings of the USNRC Twenty-Second Water Reactor Safety Information Meeting, October 24-26, 1994*, vol. 1, NUREG/CP-0140. US Nuclear Regulatory Commission, Washington DC, April 1995, pp. 317–340.
33. Reason, J. T., Absent-mindedness and cognitive control. In *Everyday Memory, Actions and Absent-Mindedness*, eds J. Harris and P. Morris. Academic Press, London, 1983, pp. 113–132.
34. Swain, A. D. and Guttmann, H. E., Handbook of human reliability analysis with emphasis on nuclear power applications. NUREG/CR-1278, US Nuclear Regulatory Commission, Washington DC, August 1983.
35. Fujita, Y. Human reliability analysis: a human point of view. *Reliability Engineering & System Safety*, 1992, **38**(1-2), 71–79.
36. Dougherty, E. M. Human reliability analysis and context. *Reliability Engineering & System Safety*, 1993, **41**(1), 25–47.
37. US Nuclear Regulatory Commission, Guidelines for the preparation of emergency operating procedures. NUREG-0899, USNRC, Washington DC, August 1982.
38. Barrierre, M. T., William, J. L., Donnie, W. W. and Ann, M. R. -S., An analysis of operational experience during LP&S and a plan for addressing human reliability assessment issues. NUREG/CR-6093, USNRC, Washington DC, June 1994.
39. Ballard, G. M., Reactor events involving misinterpretation/misunderstanding of plant status by plant staff. In *Proceedings of an International Conference on Man-Machine Interface in the Nuclear Industry, Tokyo, 15–19 February 1988*. International Atomic Energy Agency, Vienna, 1988.
40. Roth, E. M., Randall, J. M. and Paul, M. L., An empirical investigation of operator performance in cognitively demanding simulated emergencies. NUREG/CR-6208, USNRC, Washington DC, July 1994.
41. Moore-Ede, M. C., *The Twenty-Four-Hour Society*, Addison-Wesley Publishing Co., Reading, MA, 1993.
42. Moieni, P., Anthony, J. S. and Avtar, S. Advances in human reliability analysis methodology, part I: framewoks, models and data. *Reliability Engineering & System Safety*, 1994, **44**(1), 27–55.
43. Macwan, A. and Ali, M. A methodology for modelling operator errors of commission in probabilistic risk assessment. *Reliability Engineering & System Safety*, 1994, **45**(1-2), 139–157.
44. Julius, J., Jorgenson, E., Gareth, W. P. and Ali, M. M. A procedure for the analysis of errors of commission in a probabilistic safety assessment of a nuclear power plant at full power. *Reliability Engineering & System Safety*, 1995, **50**(2), 189–201.
45. Llory, M. Human reliability and human factors in complex organizations: epistemological and critical analysis—practical avenues to action. *Reliability Engineering & System Safety*, 1992, **38**(1-2), 109–117.
46. Cacciabue, P. C. Cognitive modelling: a fundamental issue for human reliability assessment methodology? *Reliability Engineering & System Safety*, 1992, **38**(1&2), 91–97.
47. Hsueh, K. -S. and Ali, M. The development and application of accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants. *Reliability Engineering & System Safety*, 1996, **52**(3), 297–314.
48. Hollnagel, E. Reliability analysis and operator modelling. *Reliability Engineering & System Safety*, 1996, **52**(3), 327–337.