White Paper
11/28/99

"RELIANCE" AND "DISTRACTION" EFFECTS IN PTC AUTOMATION

T.B. Sheridan (MIT), F.C. Gamst (Univ. of Mass. Boston), and R.A. Harvey (BLE)

EXECUTIVE SUMMARY

This document was requested by T. Raslear of the Federal Rail Administration (FRA) on 3/3/99 of the PTC Human Factors Team in conjunction with ongoing discussions of PTC standards. The charge was to investigate the "reliance effect" and the "distraction effect," where definition and focus were left to the authors.

With regard to future automation of railway systems, and in particular with regard to the implementation of Positive Train Control (PTC), questions have been raised about the possible propensity for a locomotive engineer (LE) or conductor (C) to become over-reliant on automation and/or to become distracted by the additional monitoring burdens required by the automation, and for these effects to compromise the performance of their duties and for safe and efficient train operation.

This white paper is organized by section as follows:

(1) First, details on the charge given to the authors by the FRA.

(2) Next, working definitions of terms "reliance effect" and "distraction effect" and the issues surrounding them.

(3) Review of the general human factors literature regarding humans and automation, and specifically the reliance and distraction phenomena -- for example in piloting aircraft, driving highway vehicles, operating nuclear power plants and performing routine machine operation tasks. For each of the reliance and distraction effects the relevance to PTC automation is discussed.

(4) Details of the relation of reliance and distraction to operations under PTC, along with implied recommendations. This section, the longest, reviews the "open system" nature of the rail transportation system, proposes a "human-centered" design philosophy for PTC, comments on the relevance of the UK's Great Western accident of 1997, discusses which kinds of distraction are particularly threatening, analyses the potential levels of automation for PTC design, and recommends which level seems best for safety.

(5) Classroom and simulator training for PTC.

(6) Conclusions.

The conclusions are:

(1) Over-reliance on (or not knowing how much to rely on) automation, and added distraction of having to (or poor ability to) monitor automation, are well known problems in the human factors literature, but there are few easy remedies.

(2) Maintenance of the locomotive engineer's perceptual, decision-making and control skills is considered mandatory.

(3) A PTC system should provide an auditory warning of appropriate hazards and graphical information about stopping profiles from the given speed. Otherwise it should allow for manual operation, unless certain limits are exceeded, at which point automatic braking enforcement should go into effect.

(4) Failures of a PTC system should be announced by a clearly discernible auditory alarm, and the type and time of failure recorded on the locomotive event recorder.

(5) Special classroom and simulator training for PTC operation, including failure scenarios, should be given to train crews.

1. CHARGE FROM THE FRA

The original charge to the RSAC "Human Factors Team" dated 3/30/99 was as follows.

(1) "Investigate the 'Reliance Effect' on the non-fail safe systems. Will the operator become reliant upon the overlay system and become less attentive? If so, is it possible to estimate the effect on the safety of railroad operations? Are there countermeasures or redesign alternatives that warrant exploration?"

2. 'Investigate the 'Distraction Effect' associated with frequent or complex requirements to interact with the system. Is this a legitimate concern? To what extent? If it is a significant problem, is it possible to describe tolerable limits for these interactions and redesign alternatives that warrant exploration?"

The 9/8/99 Report of the Railroad Safety Advisory Committee to the Federal Railroad Administrator (page xiii, item 5.c) reads: "Develop human factors analysis methodology to project the response of crews and dispatchers to changes brought about by overlay' type PTC technology, including possible 'reliance' or 'complacency' and 'distraction' effects (initiated 2nd quarter 1999). Apply methodology to candidate projects."

2. THE CONCEPTS OF RELIANCE AND DISTRACTION

2.1 Purpose of PTC and PTS

PTC has been defined to have the following core features in the Railroad Safety Advisory Committee's report to the Federal Railroad Administrator "Implementation of Positive Train Control Systems" (RSAC, 1999: vii, 16-17).

(1) Prevent train-to-train collisions (positive train separation).

(2) Enforce speed restrictions, including civil engineering restrictions (curves, bridges, etc.) and temporary slow orders.

(3) Provide protection for roadway workers and their equipment operating under specific authorities."

It should be noted that Positive Train Separation (PTS) is included in the core-feature definition of PTC. Consequently, PTS need not be mentioned in discussion of PTC without a particular reason to do so.

2.2. Working definitions of "Reliance Effect" and "Designed Reliance" in PTC Automation

The "reliance effect" is taken to refer to the tendency of the LE, C or train dispatcher to over-rely (rely more than the system designers or managers intend) on automation such as PTC in performing work tasks, particularly to the degree that the automation is deemed not to be fail-safe by itself. Concepts closely related to "reliance" are "complacency" and "over-trust."

Insofar as the system is intentionally designed, or the level of automation is such, that the that the human operator is compelled or encouraged to defer to the automation, we call that "designed reliance." In Section 4.5 below we make specific recommendations in that regard. There may be a thin line between intentional, designed-in reliance and unintentional over-reliance, especially as understood by the human operator.

2.3. Definition of Distraction Effect in PTC Automation

The "distraction effect" is assumed to refer to the tendency of the LE to be distracted from other duties by frequent or complex cognitive interactions with the automation to plan and program its operation, monitor its performance, detect and diagnose and stay aware of any abnormalities, and rectify any abnormalities and ensure control. (Of course there are other distractions from radio conversation or wayside events.) Associated with "distraction" are the concepts of "mental workload," "attention deficit," and decrement in "situation awareness."

2.4. Levels of Automation

Insofar as reliance implies reliance on automation by design it is sometimes useful to consider levels of automation from none to full computerized automation. The following scale (Sheridan, 1987) has been used in a variety of contexts:

1. The computer offers no assistance: the human must do it all.

2. The computer suggests alternative ways to do the task.

3. The computer selects one way to do the task, and

4. …executes that suggestion if the human approves, or

5. …allows the human a restricted time to veto before automatic execution, or

6. …executes automatically, then necessarily informs the human, or

7. …executes automatically, then informs the human only if asked.

8. The computer selects, executes, and ignores the human.

The tendency to move further along this scale has been a continuing trend in recent years, and is most evident in the evolution of commercial aircraft. It began with autopilot systems, then came navigation aids, then diagnostic aids, collision and stall and ground proximity warnings, and finally the integration of all these into the Flight Management System, a multi-purpose computer system which oversees all functions and through which the pilot flies the aircraft. Pilots now call themselves "flight managers." Similar evolution is beginning to happen in highway vehicles, ships, factories, chemical plants, power stations, and hospitals as well as trains. It is commonly called "supervisory control" (see Sheridan, 1987, 1992).

3. REVIEW OF RELIANCE AND DISTRACTION EFFECTS IN THE GENERAL LITERATURE, AND THEIR RELEVANCE TO PTC

In considering the experimental literature as well as practical experience with automation in piloting aircraft, driving highway vehicles, operating nuclear power plants and performing routine manufacturing tasks, one cannot discuss reliance without discussing complacency and trust.

3.1. Reliance Effect in the General Literature

When machines or people demonstrate their reliability it is only natural to depend on, indeed trust, them. Most of the technology around us works well, and even though our life may depend upon it, we simply do not think about it. Do we rely on the roofs over our heads or the buildings we are in not to fall down? Do we trust our brakes to slow and stop our cars from high speeds? Obviously we do - unless there are environmental circumstances (e.g., earthquakes, very steep hills) which cause us to make closer observations, or unless we receive unexpected signals (ominous noises, leaking oil, etc.). To some degree reliance on trustworthy systems is proper behavior, since we do not have time or attentional capacity to attend to and worry about everything around us. Clearly, however, one can become reliant on automation, trusting and complacent (insofar as the third term implies the first two) to a degree greater than is justified by the small risks which may be involved (where risk means probability of serious consequences times magnitude of those consequences.) There have been numerous studies of human reliance on automation recently (see, e.g., Riley, 1994; Sheridan, 1992; Parasuraman and Moula, 1994; Moula and Koonce, 1997).

Safety engineers have long worried about whether, if actions are taken to make systems safer, operators will simply take advantage of that safety margin to take correspondingly more risks, to the point where level of safety remains constant. The technical term for this is "risk homeostasis." Evidence in automotive vehicles is clearly that as brakes, tires, handling qualities and highways have improved drivers drive faster. Are they driving so fast that the safety improvements are nullified? Apparently not, for mortality and morbidity rates per passenger mile have declined significantly over the last 50 years (see National Highway Traffic Safety Administration database). At the same time it can be said they are not as safe as they would be if they continued to drive at the same speeds as they did 50 years ago. So clearly in this context risk homeostasis, in the sense of behaving so as to maintain constant risk, is a false premise. But, surely, drivers are taking advantage of the technology to achieve greater performance while maintaining acceptable risk, where what is acceptable is now significantly safer than it was earlier. "Acceptable" is an important term in understanding human behavior relative to risk. It is also a relative term regarding danger to humans and property. What might be acceptable to persons removed from a danger might not be to persons directly affected by such danger.

4

The story with respect to risk homeostasis appears to be similar in other aspects of driving and in other transportation contexts. Currently there is worry that radar-based intelligent cruise control systems will lead drivers to follow the lead car more closely, and that GPS-based air traffic displays in the cockpit, heretofore not available to pilots (only the ground controllers saw radar returns) will lead pilots to second-guess ground controllers and take more chances.

"Trust" is a term which is relatively new in the human factors literature but which is drawing much attention. The term can have different subtle meanings, but usually it relates to the subjective expectation of future performance. Muir and Moray (1996) showed that as automation errors manifest themselves trust declines and monitoring behavior increases. Lee and Moray (1992) showed that subjective trust is a significant determiner of whether an operator will use an automatic controller or, given the choice, or will opt for manual control. They modeled subjective trust as a function of both overall automation performance, the seriousness of faults, and the recency of faults. They also discuss the mounting evidence that a system is less trusted if there are no clear indications about what it is doing or about to do. Aircraft pilots, for example, frequently complain that they cannot tell what the automation is thinking or will do next (Woods and Roth, 1988).

Should we worry that human supervisors of automation may become complacent? Clearly this begs the further question of what is the optimum level of sampling the displays and/or adjusting the control settings. If, given the relative costs of attending to the automation (less time available to attend other things) and not attending, plus some assumptions about the statistics of how soon after a sample the automation is likely to become abnormal, one can specify an optimal sampling rate (Sheridan, 1970). If the operator samples at the optimal rate that of course does NOT mean that critical signals will never be missed - they still occasionally will. Moray (1999) argues that if the optimal rate is not specified one can never assert that there is complacency (assuming it means sampling at less than the optimal rate). A recent qualitative model by Moray, Inagaki and Itoh (1999) suggests that in the absence of faults or disagreements with the decisions of the automation, subjective trust asymptotes to a level just below the objective reliability, which does not suggest complacency.

A concern with automated warning systems is that a very small percentage of warnings truly indicate the condition to be avoided. This occurs because the designer has set the sensitivity threshold such that false alarms occur much more often than misses (the misses carrying a much more serious consequence) --which is rational based on the objective tradeoff between risks associated with each.

Signal detection theory, the same analytic techniques that design engineers developed during World War II to decide how to make the optimal trade-off between false alarms and misses, has by now been widely applied to measuring how humans should or actually do make the trade-off (Swets and Pickett, 1982; Parasuraman et al., 1998). It requires knowledge of probability densities for true positives (hits) and false positives (false alarms) as functions of input signals or symptoms, or the equivalent relative operating characteristic (ROC) curve - the cross-plot of probability of hit vs. probability of false alarm. It has been shown that the human operator does not respond mechanically and indifferently to these events. Indeed, the fact that the warning system may "cry wolf" so often may lead the operator to lose confidence in the automated warning system and come to respond slowly or even ignore it (Getty et al., 1995).

Classical expected-value decision theory, from which signal detection theory is derived, can also be used to make optimal decisions as to whether one or another form of automatic fault detection system is better, or whether the human is better (Sheridan and Parasuraman, 1999).

3.2. Operating Crew Reliance, Trust and Complacency with PTC

With regard to "risk homeostasis" there is some question as to whether a LB or C would ever be motivated to "take advantage" of the safety margin in a PTC system. This is because of an ever-present electronic monitoring of their acts. The event recorder on locomotives should be an interacting subsystem of PTC. Event recording should be of failures in PTC and other automation as well as errors in human performance. The overall PTC system will serve as a kind of event recorder, just as does the present centralized train control (CTC) system. Thus any infraction of the operating rules by the LE will meet with the normal disciplinary procedures and penalties--all the more so with the teeth in the rules of FRA certification, and decertification.

At present many computer workstations in ordinary business offices monitor and record the nature of an employee's work tasks and the speed, accuracy, and rules-compliance of employee performance. The ability of PTC, similarly, to monitor electronically operator compliance with the rules is comprehensive. The on-locomotive computers are all the more effective in this monitoring because of their interfacing with other machine systems, usually, having electronic and, often, computer characteristics. Railroads have traditionally and are required by FRA regulations to conduct in-field efficiency tests for operating employees. PTC has the capability of continuously testing operating personnel.

It is generally true that in automated warning systems only a very small percentage of warnings truly indicate the condition to be avoided-- most are false alarms. Nevertheless, in railroading danger signals are ordinarily observed. We distinguish between false alarms not safety critical and those that constitute railroading's "danger (stop)" signals. And we realize the great operating frequency of such rail danger signals. A nonsafety in-cab warning such as "hot engine" or "dynamic brake overload" might go immediately unheeded but not so with a danger signal. First, the danger signal (such as red stop-and-proceed signal) is common in railroading. Repeating these signals on a display in the cab does not necessarily make them any different in their operating effect on personnel. Second, railroaders do not lose confidence in a danger signal: it might be for real; it might be an efficiency test; or it might be a false-alarm "wolf cry." But all tend to be heeded, regardless.

We would have to hypothesize PTC-generated wolf cries of danger signals that would overcome the particular culture of safety in railroading that observes possible wolf cries as danger signals. For example, when two torpedoes unexpectedly explode on the rail head and, from experiential knowledge, the LB immediately reduces to and observes restricted speed, it does not matter whether a MOW flagman forgot to pick them up at the end of the workday, or he left them for a good, unanticipated, reason. This is not an argument against a need for PTC. The LB or C could be incapacitated or distracted when first confronted with a danger signal.

A falsely and reportedly overacting warning device for a danger signal, such as an in-cab alarm, might not be heeded as much as one not giving false signals. But, then, the railroad rules ordinarily call for eliminating such failed components and a consequent operating under more restrictive rules than previously.

3.3. Distraction Effect in the General Literature

The long accepted Yerkes-Dodson "law" in experimental psychology refers to the notion that with very low attentional demand humans get bored and drowsy and are not vigilant, while with very high attentional demand people cannot take in all appropriate information. Performance is best in a broad middle-range of attentional demand.

During World War II there was interest in the low end of this curve because watches on ships and monitors of sonar in submarines and radar in aircraft ground control stations found themselves scanning electronic displays over long periods for signals which seldom occurred. The associated research was identified with the term "vigilance", and the net result was a variety of studies which showed that after about 30 minutes people's monitoring performance declines significantly (Mackworth and Taylor, 1963). Associated studies of operators performing visual inspection tasks on assembly lines produced a similar result. Allegedly it was asserted that in one test of a cola bottle washing inspection operation, a higher percentage of clean bottles resulted when cockroaches were randomly added to bottles at the start of the line.

Interest in the high-demand end of the curve peaked in the mid 1970s when many new attentional demands were being placed on fighter aircraft pilots, and military laboratories started research on "mental workload." At that same time, in conjunction with the certification of the MD-80, pressures from aircraft manufacturers and airlines to automate and allegedly justify reducing the crew from three to two set off a dispute with the pilots. The regulatory agency, the Federal Aviation Administration, turned to the human factors community to observe commercial pilots and try to define mental workload. After a flurry of research, four methods were evolved to define and measure mental workload: physiological indices, secondary task measures, subjective scaling, and task analysis (Moray, 1988). It should be noted that physical workload is nowadays relatively easily measured by percent of CO_2 increase between inhaled and exhaled respiratory gas, but this physical workload has no correlation with what is called mental workload.

The various physiological indices tested over the years include: heart rate variability, particularly in the power spectrum at 0.1 Hz.; galvanic skin response (as in a lie-detector test); pupil diameter; the 300 msec characteristics of the transient evoked response potential; and formant (spectral) changes in the voice (frequencies rise under stress). Unfortunately none of these measures has proven satisfactory for most requirements because the measures have to be calibrated to the individual being measured and because they usually require relatively long time samples - often longer than the period over which one seeks to measure changes in mental workload.

The second measure of mental workload is the secondary task. It assumes that a human monitor has a fixed workload capacity, and that by giving the test subject some easily measurable additional task (such as performing mental arithmetic or simple tasks of motor skill), along with specific instructions to perform the secondary task only as time is NOT required to perform the primary task, "spare capacity" can be measured. The assumption is made that the worse the performance on the secondary task the greater are the primary task mental workload. This technique has been used successfully in laboratory tests, but is usually impractical in real-world tasks such as landing an aircraft since operators refuse to cooperate because of possible compromise with safety.

A third method, subjective scaling, is not the design engineer's ideal, simply because it is subjective rather than objective. Yet it is the method most often used, and indeed is the method most frequently used to validate the other methods. NASA has developed a subjective scale called TLX and the U.S. Air Force a scale called SWAT (Williges and

Wierwille, 1979). Multi-dimensional subjective scales have been suggested, including for example fraction of time busy (spare capacity), emotional stress, and problem complexity - the idea being that these are orthogonal attributes of a situation (Sheridan and Simpson, 1979).

The fourth method, task analysis, simply considers the number of items to be attended to, the number of actions to be performed, etc. without regard to the operator's actual performance or subjective sense of workload. This method has been criticized as not really being about mental workload because it neglects level of training or experience. A well trained or experienced operator, after all, may have an easy time performing a task, i.e., with insignificant mental workload, where a novice might be heavily loaded. However, such task analysis is amenable to objectivity, for example use of the Shannon (1949) information measure H= average of log [l/p(x)], p(x) being the probability of each different stimulus element (x) which must be attended to (or different response element which must be executed). This provides an index of "difficulty" or entropy (degree of uncertainty to be resolved). The problem lies in the somewhat arbitrary classification of stimulus and response elements.

For simple tasks the greater the mental work load and/or information difficulty (entropy) H the greater the operator's response time (Hick, 1952; Fitts, 1954) in almost direct proportionality to H. For complex tasks there may be great variability in response time. It is well established that human response times follow a log normal probability density, meaning that no response takes zero time, and the 95th percentile may be one or two orders of magnitude greater than the median. Experiments of experienced nuclear plant operators responding to simulated emergencies showed an almost perfect fit to a log normal function (Sheridan, 1992). The long responses often result from confusion about what problem is presented to the person and what is the expected criterion for satisfactory response.

There have been numerous studies to determine whether operators are better monitors or failure detectors when they are controlling a task manually or when they are monitoring automation. Mostly these studies have shown that performance capability (in terms of failure detection and response recovery) declines when operators are monitors of automation and the automation fails. (Wiener and Curry, 1980; Desmond et al., 1998; Wickens, 1992). However, at the extreme where the operator is so heavily loaded performing manual operations that there is no attentional capacity remaining for failure detection, automation may provide relief and improved capability to detect failures.

One problem with automation is that there may be very little to do for long periods of monitoring, but suddenly and without warning, the automation may fail and/or unexpected circumstances may arise, and the operator is expected to get back into the control loop instantly to set matters straight. Such workload transients are deemed to be more troublesome in many cases than sustained period of high workload, for the operator is unlikely to be able to "wake up" and figure out what is happening, and quickly make the correct decision.

A currently popular term in aviation is "situation awareness". The ideal is have a maximum level of situation awareness. A means to test situation awareness in a simulator experiment is to stop the simulation abruptly and unexpectedly and ask the subject to recall certain stimuli or response events (Endsley, 1995; Endsley and Kiris, 1995). Improvements in graphic displays and decision aids have been suggested to enhance situation awareness. Automation which is opaque to the user may well impede situation awareness. However it has been pointed out that to the extent that an operator expends more mental effort on situation awareness, to that extent less spare mental capacity, if we can accept that notion, remains for decision and response execution (Sheridan, 1999).

3.4. Maintaining Performance in a Broad Middle-Range of Attentional Demand

Given the Yerkes-Dodson "law," that with very low attentional demand humans do get bored and drowsy and are not vigilant, and with very high attentional demand people cannot take in all appropriate information, safety is clearly best in a broad middle-range of attentional demand. But how do we assure this in PTC operations for the C and LE? The most effective way to assure operation in the mid-range is by skills maintenance through retention of most pre-PTC motor and cognitive work tasks, despite the "designed in reliance" effect of PTC. A primarily manual operation of trains by the LE and C, with a fully automated safety compliance backup is, therefore, necessary. This primary manual operation should be at the reliance level-2 of the automation scale (the PTC suggests alternative ways to do the task) or, perhaps, 3 (the PTC selects one way to do the task). That is, the system provides an audible warning in advance of a civil speed restriction (CSR), a signal (in-cab or otherwise) change to a more restrictive indication, or some other restriction of train movement. And the system also meets the requirement of PTC in that the restrictions will be enforced by a sub-system on board the locomotive at level 6 (the PTC executes automatically, then necessarily informs the human and the event recorder). In all, the automation scale level of 2 or 3 is what we strive for as normal PTC operation, but level 6 must always be operable in the background as the safeguard.

3.4.1. Benefits of maintaining operating skills. In maintaining their judgment and skills through on-the-job experience, the LE and C team (coordinating with the train dispatcher) protect a number of personnel from danger: themselves, any other personnel on their train, personnel on other trains, other railroad employees along the track, persons on passenger trains, and the public along the right-of-way. In their vigilance, this coordinated team also protects from damage to material property: their engine and cars; any lading of these cars; other engines and cars; railroad structures such as track, wayside signaling, buildings, bridges, and tunnels; and nonrailroad property along the right-of-way. Besides material property are railroad assets of incorporeal (nonmaterial) property. The courts have ruled that even incorporeal things such as a company's good name and reputation for conducting business constitute property. The assets safeguarded by the LE, C, and train dispatcher thus include a railroad's business reputation as a carrier, unhindered flow of traffic, cost-effective turnaround time on equipment, and freedom from penalties in contractual performance. In the few times when the experience-based judgment and skills of the LE, C and train dispatchers were not maintained, the result has made the headlines. Not to maintain experience-based judgment and skills for operating crews engenders unacceptable safety risks to all of the just-enumerated kinds of persons and property.

Most railroad operating rules are written for an at-the-moment-of-event assessing of the appropriateness and range of interrelations of their applications. Such assessment must be constantly altered as the operating conditions change during a single run. Different assessments must be made as operating conditions vary across several trips. Several of the many interrelated rules must be, first, selected to form what could be called a rule set, then, mentally sequenced, and, finally, applied to an operating situation.

Every train-train collision and cut of rolling equipment moving out of control results from a hazardous combination of a number of operating events. Sometimes preventing the occurrence of just one of these events makes the combination of the others non-hazardous. Maintaining the experience-based skills and judgments in applications of the rules by the C and LE is one way to remove such a crucial event from a chain of accident events.

3.4.2. The nature of the skills to be maintained and the railroad environment. First of all, "you've got to know the territory," through hands-on experience. For safe, efficient operations, a LE, among other things, must learn and continually re-experience the train handling constraints of every upgrade, downgrade, curve, turnout, crossover, auxiliary track such as passing siding, fixed signal location, crossing at grade, and engineering and operating speed restriction. Given knowing the territory, the LE can have little advance information on a particular train's handling characteristics. These comprise a large number of dynamic variably simultaneous and sequential events to be monitored continuously by the LE for constantly changing inputs.

Above all, the LE is the operator of a long (often a mile or more), heavy (usually many thousands of tons), fragile (it is easy to carelessly "break a train in two" or more parts or derail a train) mobile, (at speeds from 5 to 100 + mph and having great braking distances, proportionate to speed and weight), highly dynamic (averaging a foot of drawbar slack for each entrained car and with individual car air brakes of varying power) electromechanical system --that is, a North American freight train.

Control responses of a freight train are delayed and must be given advance time. Often a rear car on a mile-long train will not begin a brake release until 1/2 minute after the brake pipe signal is initiated by the LE. A power throttle or dynamic brake cannot be rapidly advanced or shut off without adverse train (and track) dynamics. Too great of an initial reduction of automatic air brake pressure or too great of an increase of independent air brake pressure can cause a violent lading-damaging and potentially derailing run-in of draft-gear slack. In all, the LE must always plan ahead for any operating contingency. He does this by knowing the then current intricate dynamics of his train with regard to the territory over which he now advances and will advance.

The North American LE handles and dynamically monitors (by hands on the responsive controls and eyes and ears on the informing indicators) a machine system with complex subsystems, each having ever-varying critical statuses, while transiting an ever-changing environment, which itself is alterable from trip to trip. The LE can have little information on the handling characteristics of the these interrelating variables upon his train, because the exact consist of most freight trains differs considerably. A LE manipulates and monitors variables such as velocity, drawbar pull and compression on draft equipment, amperage in traction motors, train brake pipe pressure and thus car brake cylinder pressure, brake pipe leakage, independent engine brake cylinder pressure, statuses reported by the end-of-train device, statuses reported by any remotely controlled "rear" and "swing" helper units back in his train consist, profile of train by car weight and type and by weight of blocks of cars, and power of dynamic electrical brake. Although failure of the dynamic brake necessitates a short cycling of the automatic air brakes, perhaps with car wheel-cooling stops, too many operative dynamic brakes can cause a light car to compress in its draft gear with buff forces causing its wheel flanges riding up over the ball of a rail to a derailment.

For a narrow example, in cresting an upgrade, the LE must be aware of the slack status and the location of the equilibrium point in his train of cars. Thereby he knows, when descending from the summit, where to begin bunching the slack of his stretched train, and thus how gradually to reduce the power throttle and change over to how much dynamic electrical brake in concert with what rule-allowed reductions of the (air) brake pipe pressure, perhaps prior to easing up on the braking forces, for a determined while, when coming to a short decrease in descending gradient at a "drawbar flats." In reducing the braking systems' power on the head end, he must not allow the heavy engine (of perhaps four 200-ton units) to run out and perhaps break the train in two.

Some of the LE's skills and knowledge were first explored in the studies of the 1970s, fueled by the FRA's empowerment, in 1970, to superintend railroad safety. Accordingly, speaking of the LE's cognitive and motor skills in train handling and in general operations, researchers of railroading A. Hale and H. H. Jacobs say: "Fundamentally, the engineer is a sophisticated information processor and controller of a very complex, and often difficult to maintain, man-machine system" (1975:11). A study, analyzing the work of the LE, found: "Concerning safety of operations, these [data] reveal that approximately 65% of these tasks, if improperly performed, may lead to potentially hazardous situations" (McDonnell Douglas 1972:14).

4. CONCERNS AND RECOMMENDATIONS WITH RESPECT TO SAFETY OF PTC AUTOMATION

4.1 PTC Functions in an Open Railroad Operating Environment

A concern with a fully automated PTC at levels 5, 6, and 7 (as previously discussed) is degradation of operating skills and judgment developed during continuous experience. The motor skills and judgment of the LE, especially, and also the C, will degrade (that is, degenerate, deteriorate) from lack of practice in the unpredictable and therefore constantly skills-testing operating environment. Skills maintenance includes maintenance for coping with unpredictable events in the open operating environment.

We posit that railroad transportation is necessarily an open system, with all manner of events extraneous to the (relatively closed) systems of the locomotive and the railroad traffic control impinging on it.[1] Excluding some airport and urban guideway transit systems, the typical railroad system can never be closed.

The highly complex railroads are not operationally like the automated or highly automated rail transit systems. Railroads have danger from ever-increasing numbers of hazardous loads and the kinetic energy of enormous tonnages, while operating across and through humanly congested, economically costly, and ecologically fragile public spaces. These train-consist tonnages have increased over the years and will continue to do so, consistent with strength of coupler and draft gear components. Automated rail transit systems move in a sequestered right-of-way and have a much more limited number of operational variables and no hazardous lading. Accordingly, we cannot derive suitable operational models from transit systems under forms of automation for application to the nation's railroads under PTC. An automated subway and a people mover can be operated by someone without many railroad operating skills, or can even have no operator at all. Given the kinds of public spaces they operate across, the railroads, however, have a safety necessity of maintaining the experience-based judgment and skills for operating crews.

----

[1] * In the sciences, <u>a closed system</u> is considered as isolated from the environment. An <u>open system</u> is not isolated. It comprises a set of elements forming a connected whole which is not a bounded, sealed entity. In other words, the set is not demarcated to consist of a finite (hence, predictable or knowable) number of interacting elements. In the open railroad system, because of later, varying numbers of unpredictable, impinging conditions, a final state cannot be predetermined by initial conditions, say, a train's consist, tonnage, authorized speeds, track occupancy authority, and crewmember experience. A particular final state can be reached from different initial conditions, and the same initial conditions can result in different final states.

Part of the central problem of skills and knowledge maintenance, then, is such maintenance for coping with both extrasystemic and failure operating events. A fully automated PTC cannot handle all adverse extrasystemic and failure events in the unpredictable railroad operating environment. A few examples are: local police place a red fusee along a main track, an employee or contractor equipped with only red fusees and a white light advances toward a train that must be stopped, a civilian signals danger ahead by violently waving his arms while adjacent to a main track, a trespasser sabotages the train, a trespasser sabotages the right-of-way, an automotive vehicle fouls but does not touch a main track when not at a grade crossing, in the face of an approaching train a roadway worker fouls the track with movable equipment without touching the rails, the PTC system is inoperable during maintenance, a train not equipped for PTC must be run, a PTC-equipped trainexperiences bad-order PTC equipment, and a PTC command requires stopping a train in a hazardous place, e.g., in the vicinity of a leaking tank car or burning gasoline truck.

Furthermore, a PTC system cannot monitor and control the range of failures of the dynamic brake, the pressure maintaining feature, and the automatic braking system (including excessive piston travel, kinked air hose, and ice blockage of train line). Given that accurate, detailed train consist data are required for accurate PTC operations, how are the consist data assured regarding their safety-critical quantities? Communication failures and informational errors regarding train consist and tonnage are not rare events. Under restrictive speed, in foggy or other vision-blocking weather, how does PTC judge stopping within the rule-mandated one-half the range of vision? Currently, under some such restrictions, the LE must not move his train until a flagman has been sent ahead to view the obscured track to be occupied. It might well be that with certain mechanical and communication failures found in railroading, and just enumerated, the PTC braking paradigm on grades of about 2 percent could sometimes have a stopping distance of infinity--that is, an unstoppable runaway train.

In each of these just-enumerated, safety-critical events, the C and LE must react promptly and correctly to the stimuli they rapidly approach with great kinetic energy. Such reaction is only afforded by skills maintenance of the C and LE.

In the open railroad environment, we find that in 1997, more than half of the 3,446 train-automotive vehicle collisions involved grade crossings equipped with active warning devices. Motorists simply did not heed them. During 1997, Amtrak passenger trains were in 245 collisions with automotive vehicles, and 183 were attributable to motorist inattention or impatience. Each year, the number of automotive vehicles, including heavy trucks, increases and the number of passenger trains (largely commuter and regionally financed) grows. Thus the potential for deadly accidents in the open railroad environment grows, from just this narrow range of inputs. The cheap and easy fixes for eliminating grade-crossing collisions, by now, are almost exhausted. Under the worthy FRA aegis, some 33,000 little-used, unsignaled, grade crossings have been closed to highway traffic. But the average cost of a grade separation is $3 to 5 million, and more in a built-up area (Coston, 1999; FRA, 1998; GAO, 1995). Thus closing crossings will provide less and less of a solution for decreasing deadly accidents at grade crossings.

Furthermore, about 60 percent of grade crossings have no active warning device. Perhaps as many as 20,000 crossings need at least some kind of active warning devise (Savage, 1999:58, 1998: chapter 8; FRA, 1998). The enormous cost of installing such devices means that, even with some kind of a fully-automated PTC, innumerable grade crossings can still be heedlessly and inattentively occupied by motorists and pedestrians who put themselves in a danger not protected by PTC. And this does not take into account the innumerable, customary trespassers walking across and along live tracks, which might be subjected to

rules-permitted blind shoves of a train. Motorist inattentiveness and heedlessness plus their lack of confidence in active warning devices has long been demonstrated. Additionally, motorists exhibit an uncertainty in decision making at grade crossings (Wilde, Cake, and McCarthy, 1975; Aurelius and Korobow, 1971). Motorists decisions at grade crossings are thus less predictable than in other driving situations.

4.2 Achieving Safety through a Human-Centered PTC

"Human-centered" means that human operators are an integrated part of the problem solving process, and they are not automated out of the system. Maintaining the judgments and skills promotes knowledgeable assessment for action and informed compliance with the governing rules during times of any failure of the PTC system and in times of potentially hazardous extraneous events not controlled by this system. Therefore the PTC should not be totally automated. It should provide cognitive tools that assist the human operators (C and LE) in making decisions and solving problems in operations, and should provide a level-6 safeguard of last resort in operations.

A potential exists for an overall reduction in system safety, at times, with the introduction of PTC, especially if it becomes either inoperable or unreliable. Human-centered PTC systems should recognize the LE as providing coverage for system failures and for the unpredictable open railroad environment. In no way should our advocacy of PTC diminish that ability. Why is this potential for reduction in system safety extant? The reasons are inherent in advanced safety technology, as follows.

The benefits of technology always balance against the costs. Technological innovations such as the aircraft Traffic Alert and Collision Avoidance Systems, TCAS, (warning aircraft that they are closing upon one another and coordinating the responses by directing pilots to perform specific evasive maneuvers) are promoted for safety. The application of the new, advanced technology, however, produces profound reverberations that may introduce new risks -- especially when the technology is the sort of automation that has been labeled strong, silent, and hard to direct. Why is advanced automation often difficult to direct?

First, the technology itself is often frangible (breakable because of the use to which the item is subjected) in ways that produce new forms of failure. In the case of hard-to-direct automation, these new forms of failure are often difficult for operators to anticipate, detect, or accommodate. Thus pilots may receive commands for instant action that do indeed require immediate acts in order to be safe but that result in behavior sometimes incorrect for the desired safety.

Second, the "safety" that new technology seems to produce frequently becomes dissipated in increases in production or efficiency of operations. Thus the ability of TCAS to warn the pilots is one factor that encourages planners to move to a system with less separation between aircraft. This inevitably erodes safety margins, something the planners reject as a valid assessment of their planning outcomes.

In all, the kinds of outcomes possible with advanced technology are many. However, new information technology -- including control information, and use of flexible blocks on fixed guideways --inevitably will create new forms of failure difficult to foresee, detect, and accommodate. Moreover, it will simultaneously encourage more efficient (that is, less costly) approaches which could diminish safety in ways difficult to anticipate, until accidents make them quite apparent.

4.3 Implications of the Great Western Accident

We have learned limited information about the tragic, two-train collision on October 5, 1999 just outside of London's Paddington Station, on the privatized Great Western, resulting in as many as 100 deaths by incineration. Detailed information now becomes available from the investigation of the two-train collision during 1997 in the same area on the same passenger carrier, as follows (BBC, 1999):

"The driver of the high-speed passenger train that crashed in 1997 killing 7 and injuring 150 had been seen earlier on that trip with both feet up on the dashboard of his cab, leading to speculation that he had weighted down the dead-man's switch. He later drove through two [amber] warning signals and a red stop signal before colliding with a freight train crossing the line in front of him at Southall, in West London, en route to Paddington Station in London. The inquiry has now finally begun. The inquiry heard that the train's Automatic Warning System (AWS) -- which sounds a klaxon when the train goes through danger lights -- had been switched off after apparently malfunctioning earlier in the day. The train was also fitted with Automatic Train Protection (ATP), but this was also switched off because the engine driver who had been in charge of the train earlier in the day was not trained to use it; that system would have automatically prevented the train from running the stop signal. Great Western was already fined a record 1.5M pounds for a breach of the Health and Safety Act [for this accident]."

The account of the Great Western collision of 1997 reported in the news media, above, stated simplistically that three safety subsystem were made inoperable. Such a statement focuses attention on the engine driver. Why would he cut out and his supervisors allow these vital safety features to be negated? A fully informing -- and safeguarding-- investigation into the social factors of the Great Western accident reveals more than single operator error. The accident indicated errors by the human operator and supervisors (defeating the deadman feature and cutting out the ATP system). Further investigation also shows that in commuter and other passenger rail service having tight headways and brief platform dwell times great performance pressures exist upon operators of equipment and local supervisors to keep the trains moving--even if this means cutting out technological safety features. After all, without a balancing informed reflection on the potentially catastrophic nature of an accident, the probability of such event is correctly judged by involved actors to have a quite low incidence. On the Great Western line having the 1997 accident, day after day, the various safety subsytems prevented collisions of trains. With complacency involved (as discussed in sections 3.2 and 3.3 above), actors had little or no experientially-based fear of defeating safety subsystems on a train. Accordingly, the various safety subsystems in place on most trains would prevent collisions, or so it was reasoned. What is the remedy to prevent involved actors from defeating safety subsystems for the movement of a train?

Rail safety subsystems could be designed so that cutting them out is impossible, and a failsafe design could not be compromised. The operational costs of doing this are considerable, and rail safety systems are ordinarily designed to be cut out, to permit the authorized moving of trains under most circumstances of single or multiple faults. The great intricacy of modern safety systems means that designers do not mandate a system dependent on all components functioning as intended.

Thus far, then, the investigation of the Great Western collision of 1997 is incomplete. Safety questions must still be answered, among these are the following. During failure of rail safety subsystems, in what ways do operators and their supervisors react locally, to obey and infract the rules? What are the varied local, property-specific, incentives for maintaining

productivity -- keeping the trains moving and traffic fluid? Does such "make-do" reacting render failure of the entire system --for rail passenger service, always in the media spotlight--an infrequent event? How well do the local operators and supervisors understand all of the systemic safety-critical variables of the potentially catastrophic operating world in which they work and react to ever-changing problems? These are the often-unfathomable questions in the real world of rail operations, as opposed to a designer's analytic world in which many key variables are excluded--by accident or design.

4.4.   What Kinds of Distraction Matter?

It should be noted that many displays are present in the LE's workspace and any amount of added/overlay PTC displays could arguably be cited as the final straw that overburdened the camel. The overlay, in this instance, would be in some degree of partial PTC --automation level 5 or lower. For example, a modern locomotive has the normal, either analog or integrated, cab electronics (ICE) screen displays for running the engine and handling the train. These normal items include those for using the end-of-train-device, which itself has a number of displays to be monitored. In addition, the locomotive could have displays and controls for distributive power (for controlling from the head-end locomotive a number of remote locomotive consists distributed throughout the length of the train). Distributive power can be operated by the LE in two modes. In the synchronous mode, all sets of entrained locomotives receive the same commands from the LE, for example, throttle run-7 or, perhaps, minimum dynamic brake. In the nonsynchronous mode, if, for example, the LE has two sets of locomotives further back in the train, when cresting a mountain grade, he might have his head-end set, which he occupies, increasing toward full dynamic braking, his mid-train or "swing" set gradually throttling down from run-8 to idle, and his rear-end set shoving in run-8 to keep slack bunched. The locomotive could have displays for electronically controlled electro-pneumatic ECP brakes. In ECP braking, air brakes--using ordinary brake cylinders and brake rigging--are electrically controlled and the brake pipe serves as an air-reservoir supply pipe, permitting the reservoirs always to be charged fully.

What practicing LEs have concern about is not distraction with a PTC failure on level 6 or higher, but, instead, manually operating with some form of partial PTC and still having all of the normal functions noted in the previous paragraph. Then, some of the ordinary range of variation of PTC displays and other alerts could cause a task overload. We emphasize the distinction between (1) overload/distraction with full PTC and (2) overload/distraction within a range of partial kinds of PTC (including most overlays) added to normal functions, where the latter may be the worse culprit.

4.5.   Practical Understanding of the Issues, and Discussion of the Levels of Intended Design Reliance on PTC

Current plans for PTC, as they relate to the reliance and distraction effects, have not been sufficiently clarified and formatted because there is no clear understanding of the levels of automation in the speculated systems. To develop a clear understanding of this automation requires analyses of typical operating procedures in the railroad environment. We have thus chosen a scenario of civil speed restriction (CSR) on four levels of automation and discuss their implications.

Most present-day methods of operation under CSR work similar to the following:

(1) CSR is one assigned to a specific limit within a specified segment of track.

(2) The LE and C are usually advised of the limits and speed requirement in a mandatory directive. A mandatory directive means any movement authority or speed restriction that affects a railroad operation. It may be found in a track bulletin, special instruction, timetable, Superintendent's notice or some other authorized and written form.

(3) It may be preceded with advance warning signs or flags.

(4) There are rules requiring train crews to discuss the existence of the CSR at timely intervals to assure compliance.

(5) It is the train crew's responsibility to comply with all mandatory directives assigned to them as well as all track flags associated with the movement of the train.

(6) The LE exercises the skills required to bring the train within the limits established in the CSR. That performance is based on the LE's skill level/knowledge of the territory and train handling information, compliance to all rules governing operations and air brake/train handling and factors associated with equipment, weather, track condition, and the LE's knowledge associated with those variables.

Included in this operating rules scheme are several redundant features that, if complied with, greatly limit the probability of over speed in the CSR.

All hazards associated with the CSR are mitigated by this skills/rule knowledge based operating system if there is compliance. With no PTC available and where the skill/rule/knowledge-based system, as we know it today, is not changed we can assume the reliance effect to be 0 (zero).

If we look at the same operating scenario of CSR regarding a PTC system where the evolution of the automation is extremely limited in its capacity as it relates to control, and, incrementally, to a system where the train's behavior is fully automated by the system. We can then speculate as to the numerical value of the intended "design-reliance" effect.

Reliance level 1. To the existing method of operation described above we add a system component that provides an audible warning in advance of a CSR (For discussion purposes the train's speed is not enforced by a wayside or on-board component or subsystem.) The audible warning adds a level of safety but does not replace any of the required rules or does not control the train's brakes. The reliance on that audible warning would be assigned a one.

Reliance level 2. This system provides an audible warning in advance of the CSR and also meets the requirement of a PTC system in that the CSR will be enforced by a subsystem on board the locomotive. The crew's responsibility under the existing method of operation does not change in regard to the requirements for the CSR. The principal difference now becomes the LE's choice/ability to permit the PTC on-board components to control the train's speed to comply with the CSR and what other information may be delivered to the LE from the on-board sub-system. That information may include distance to target or the civil speed directive. Assign a two for reliance in this case.

Reliance level 3. The same PTC system exists as above. A principal difference is there are no mandatory directives issued and/or there are no requirements for conversing among the crew members regarding the existence of any CSR. An audible warning may be received in the locomotive cab and there may be an advance directive for speed or distance to target but no other form of advance warning. The automation now becomes depended on for most train control functions regarding the CSR. The LE's role will be to monitor the system performance.

Reliance level 4. The PTC system is considered the preferred method of operation. The operating skills/rules/knowledge required by the LE pertain solely to automatic system with manual control of the locomotive/train, the skills/rules/knowledge-based train handling and operating rules would again come into play. The reliance on the system at this level is absolute. It is now necessary to provide for a rule set that prohibits manual operation except in very limited circumstances.

Each system, sub-system or component could be evaluated for its potential to develop a reliance effect by determining: (1) its purpose and function as a replacement for a task performed by the LE or C; (2) the performance reliability; (3) the accuracy at which the component/sub-system performs; (4) the difficulty level of the task; (5) the motivation of the LE or C to allow/deny the component to operate: (6) the requirements established by the system/railroad for allowing/denying the LE or C from operating the locomotive/train. **We currently recommend that the "designed reliance" of a PTC system be at level 2, as defined above. The actual automation of PTC would then work in the background at level 6, as described in section 2.4 on page 3.**

4.6 Warning Before PTC Enforcements

The LE must have suitable warning before the PTC system imposes an enforcement. "Suitable" depends on the particular event to be enforced. In all instances a distinctive audible enforcement alarm should be sounded prior to enforcement. In addition, some kind of graphic display, on a cathode ray tube or other kind of visual presentation, for the algorithm braking/deceleration distances should be used The display should at least show the deceleration of the train, the point at which deceleration or stop must be completed, and calibrations in wayside mile posts and their fractions in tenths of miles. A display of percentage of gradient could also be useful. Such a display would be essential for PTC warnings requiring either decelerating or stopping the train, but could be useful in general, when no PTC alarms are present.

The PTC systems, subsystems, and components on board a locomotive should be designed to ensure necessary functions can be performed by alternative means, such as manual control, when the automation fails.

Automated control actions and out of tolerance conditions or failures in any system, subsystem, or component should be announced to the LE and C.

Transient faults associated with control automation should not fail passively or silently. There should be established a tolerance level for determining when the automation is no longer reliable because of either the frequency of the transient faults or the safety-critical nature of the systems from which the faults originate. The failure of such automation should be announced with a clear and distinctively sound-coded alarm, in such a way as to permit the LE to immediately take control of the locomotive and its train including all on-board PTC systems, subsystems, and components. When transient faults occur, they should be recorded regarding their kind and time in the locomotive event recorder.

5. TRAINING FOR PTC

There is general agreement that training needs increase with increasing automation, and PTC is no exception. Training must include not only traditional skill maintenance, but also training in new skills and dealing with emergencies, particularly those likely to occur if the automation fails. (Details of PTC training are not regarded as part of the charge for this white paper.)

The design of a training program requires a thorough task analysis, emphasizing not only what displays the operator must observe but also what information is required to be gained and understood, and not simply what controls to operate but also what variables are to be controlled both by the automation and by the personnel according to what criteria. This should yield critical insights for setting training objectives, writing a syllabus, and specifying a specific plan for student testing and program evaluation.

5.1.   Classroom and written instruction

Training should include preliminary formal classroom instruction in the rules and practices for PTC. Merely posting bulletins or leaving a stack of governing rules for PTC in a crew register room will not do.

Written material should explain the overall characteristics of the particular on-property application of PTC and the expectations for employees and contractors involved with this form of PTC operation. This should be augmented by classroom presentation, discussion and testing to provide feedback to the students.

5.2.   Locomotive simulator instruction

Locomotive simulators have been found to be of great value to train and test the LE for some three decades. They have also been used to conduct experiments of the LE on safety related issues, test the ability of different braking systems, and as tools for accident investigation. They could be useful for PTC-related training. This would be especially so for some elements of skills maintenance. Simulators also offer an opportunity to train the LE through exposure to rare but possible events that can occur in the railroad environment. The initial teaching of PTC operations would also profit from simulator training.

Simulators vary greatly in their sophistication and ability to mimic real world stimuli.

They have been classified in 49 CFR (Code of Federal Regulations) Part 240 as a Type I Simulator which means a replica of the control compartment of a locomotive with all associated control equipment that:

(1) Functions in response to a person's manipulation and causes the gauges associated with such controls to appropriately respond to the consequences of that manipulation;

(2) Pictorially, audibly and graphically illustrates the route to be taken;

(3) Graphically, audibly, and physically illustrates the consequences of control manipulations in terms of their effect on train speed, braking capacity, and in-train force levels throughout the train; and

(4) Is computer enhanced so that it can be programmed for specific train consists and the known physical characteristics of the line illustrated.

A Type II Simulator means a replica of the control equipment for a locomotive that:

(1) Functions in response to a person's manipulation and causes the gauges associated with such controls to appropriately respond to the consequences of that manipulation;

(2) Pictorially, audibly, and graphically illustrates the route to be taken;

(3) Graphically and audibly illustrates the consequences of control manipulations in terms of their effect on train speed braking capacity, and in-train force levels throughout the train; and

(4) Is computer enhanced so that it can be programmed for specific train consists and the known physical characteristics of the line illustrated.

A Type III Simulator means a replica of the control equipment for a locomotive that:

(1) Functions in response to a person's manipulation and causes the gauges associated with such controls to appropriately respond to the consequences of that manipulation;

(2) Graphically illustrates the route to be taken;

(3) Graphically illustrates the consequences of control manipulations in terms of their effect on train speed braking capacity, and in-train force levels throughout the train; and

(4) Is computer enhanced so that it can be programmed for specific train consists and the known physical characteristics of the line illustrated (56 FR [Federal Register] 28254, June 19, 1991, as amended at 58 FR 19002, Apr. 9, 1993; 60 FR 53133, Oct. 12, 1995).

In the order of their ability to simulate the operation of a locomotive in the most realistic manner, the Type I simulator is superior to the Type II , which is superior to Type III. The Type II and Type III simulators have some limited value for maintaining skill levels of the experienced LE. Their use, however, for initial training of persons who have never been at the controls of a moving train may improperly prepare them for the task of actual operation. Actual train movements provide an array of powerful stimuli that reinforce train handling assumptions for the LE. These stimuli tend to be learned over time, and have subtle distinctions meaningful only after developing a level of experience on a particular territory through repetition. Among these arrayed experiences are those tactile (providing a sensation by touch) and kinesthetic (providing a sensation of bodily movement, position, and tension). Both of these are necessary to provide feedback assurance to the LE that the choices made for handling the train are the right ones, including that they are in the correct temporal sequence, each choice further timed according to appropriate duration. This initial knowledge base, accordingly, must be developed with actual experience from handling a moving train.

The Type I simulator, also known as "a full-motion simulator" provides a more realistic experiential stimulation and operational feedback for the trainee. The simulator has a work setting of an actual locomotive cab mounted on a motion base of hydraulic legs with four degrees of freedom supplied through hydraulic actuators. Sideways force cues are provided as the simulation lurches through track switch turnouts. Lesser displacements of this kind, either to the left or right and return, are experienced by the trainee when passing over various simulated track structures such as frogs and railroad crossings at grade. The cab realistically rolls and sways while simulating running over the track.

The sway, at right angles to a longitudinal axis, can be up to 5 degrees to each side and reproduces the side sway of a unit as it moves. Other motion is felt longitudinally when pulling trailing cars (by rearward shock forces, or blows, to the cab) and when the slack of trailing cars runs in against the locomotive (by forward shock forces to the cab). Longitudinal motion of a simulator can be up to 6 inches. If the trainee handles the simulated train too roughly, then, he or she will experience quite severe shock blows while in the LE's cab seat, as simulations of improperly controlled slack run-ins or run-outs are reproduced. Realistic sound affects reproduce those of real operations and are exactly

synchronized to the back-screen projections for the simulation. There is no research that indicates a Type I simulator is superior to a Type II or Type III simulator, but it is generally believed by LEs that the realistic feedback provided by Type I simulators provides a superior learning environment.

One of the advantages of simulator training is an instructor at his accompanying computer console can add many changing variables to a simulated run. He can simulate any number of failures such as loss of dynamic brake, pneumatic control switch open, undesired emergency brake application, slack action, and a break in two of the train, as well as a change in tonnage or number of cars. The back-screen projected environment allows for a very large number of variations on events and conditions. Literally hundreds of permutations of the same route can be simulated thus preventing the trainee from memorizing "the same old film." For example, signal number 103.2 could be green over red, or dark, or red over yellow, the latter simulating movement over a diverging track. More advanced computerization is permitting the simulation of varying weather conditions and can inject realistic railroad operating scenarios to which the LE must react.

A sophisticated computerized locomotive simulator is demanding and, as in aircraft simulators, can afford training opportunities not allowable in the real world. A wide range of operationally difficult, cognitively taxing, and potentially dangerous simulations with different train profiles and locomotive consists can be experienced by the trainee. Thus various failure modes of PTC can be simulated and experienced. These failure modes can even be safely experimented with regarding LE reactions to them.

Problems of a LE transitioning from a locomotive having traditional analog displays to one having integrated-cab-electronics (ICE) screen displays for running an engine and handling a train could be prevented with training on a sophisticated simulator. Problems of transitions of the LE from non-PTC to PTC territory, and between differing kinds of PTC territories could similarly be prevented with training on a sophisticated simulator.

6. CONCLUSIONS

(1) Over-reliance on (or not knowing how much to rely on) automation, and added distraction of having to (or poor ability to) monitor automation, are well known problems in the human factors literature, but there are few easy remedies.

(2) Maintenance of the locomotive engineer's perceptual, decision-making and control skills is considered mandatory.

(3) A PTC system should provide an auditory warning of appropriate hazards and graphical information about stopping profiles from the given speed. Otherwise it should allow for manual operation, unless certain limits are exceeded, at which point automatic braking enforcement should go into effect.

(4) Failures of a PTC system should be announced by a clearly discernible auditory alarm, and the type and time of failure recorded on the locomotive event recorder.

(5) Special classroom and simulator training for PTC operation, including failure scenarios, should be given to LE, C and train dispatcher personnel. This should be based on a thorough task analysis of PTC operation and response to potential PTC failure.

7. REFERENCES

Aurelius, John P. and Norman Korobow (1971). The Visibility and Audibility of Trains Approaching Rail-Highway Grade Crossings. Final Report FRA-RP-71-2, May 1971.

BBC (1999). BBC website, 20 Sep.1999<http://news.bbc.co.uklhi/english/uk/newsid 4520001452732.stm>):

Coston, James E. (1999). The Next Degree of Separation, *Journal of Commerce*, May 12.

Desmond, P.A., Hancock, P.A. and Monette, J.A. (1998). Fatigue and automation-induced impairments in simulated driving performance. *Transportation Research Record* 1628. Washington, DC: National Academy Press.

Endsley, M.R. (1995). Towards a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32-64.

Endsley, M. R. and Kiris, E.G. (1995). The out-of-the-loop performance problem and level of control in automation. *Human Factors*, 37(2), 381-394.

Fitts, P.M. (1954). The information capacity of the human motor system in controlling the amplitude of movement. J. *Experimental Psychology* 47: 381-391.

FRA (U.S. Federal Railroad Administration) (1998). Railroad Safety Statistics: Annual Report 1997. Washington, DC: USDOT, FRA.

GAO (U.S. General Accounting Office) (1995). Railroad Safety: Status of Efforts to Improve Railroad Crossing Safety. Report GAOIRCED-95- 191. August 1995.

Getty, D.A., Swets, J.A., Pickett, R.M. and Gonthier, D. (1995). System operator response to warnings of danger: a laboratory investigation of the effects of the predictive value of a warning on human response time. *J. of Experimental Psychology Applied* 1(1) pp. 19-33.

Hale, A., and H. H. Jacobs (1975). Proposed Qualification Requirements for SelectedRailroad Jobs. Report No. FRAIOR&D-75/44. Washington, DC: DOT, FRA, Office of Research and Development.

Hick, W. E. (1952). On the rate of gain of information. *Quart. J. Experimental Psychology* 4:11-26.

Lee, J. and Moray, N. (1992) Trust, control strategies and allocation of function in human-machine systems, *Ergonomics* 35(10), 1243-1270.

McDonnell Douglas Corporation (1972). Railroad Enginemen Task and Skill Study. Report No. FRA-OPP-73-2. Washington, DC: DOT, FRA.

Mackworth, J.F. and Taylor, M.M. (1963). d' measure of signal detectability. *Canadian J. of Pyschology*, 17, pp. 302-325.

Moray, N., "Mental Workload Since 1979 (1988). *International Reviews of Ergonomics* 2:2, 123-150.

Moray (1999). Personal communication.

Moray, N., Inagaki, T. and Itoh, M. (1999). Adaptive automation, trust, and self-confidence in fault management and time-critical tasks. *J. of Experimental Psychology:Applied*. (in press).

Mouloua, M. and Koonce, J.M. (1997). *Human-Automation Interaction*. Mahwah, NJ:Erlbaum.

Muir, B.M. & Moray, N. (1996). Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics* 39(3) 429-461.

Parasuraman, R. and Mouloua, M. (1994). *Automation and Human Performance*, Mahwah, NJ: Erlbaum.

Parasuraman, R., Hancock, P.A. and Olofinboba, 0. (1998). Alarm effectiveness in driver collision-warning systems. *Ergonomics*, in press.

Parasuraman, R., and Riley, V. (1997). Humans and automation: use, misuse, disuse, abuse. *Human Factors*, 39(2), 230-253.

RSAC (Railroad Safety Advisory Committee). (1999, July). Report to the Federal Railroad Administrator, Implementation of Positive train Control Systems.

Rasmussen, J. and Rouse, W.B. (1981). *Human Detection and Diagnosis of System Failures*. New York: Plenum Press.

Riley, V. (1994). A theory of operator reliance on automation. In M.Mouloua and R. Parasuraman (Eds). *Human Performance in Automated Systems: Recent research and trends*. Hillsdale, NJ: Lawrence Eribaum. 8-14.

Savage, Jan (1998). *The Economics of Railroad Safety*. Norwell, MA: Kluwer Academic Publishers.

Savage, Ian (1999). Railroad Safety and Public Policy, *Journal of the Transportation Research Forum*, 38:56-63.

Shannon, C. E. (1949). Communication in the presence of noise. *Proceedings of IRE* 37: 10-22.

Sheridan, T. B. (1970). On how often the supervisor should sample. *IEEE Trans. Systems Science and Cybernetics*. SSC-6: 140-145.

Sheridan, TB., Supervisory Control, in G. Salvendy, Ed., *Handbook of Human Factors*, New York: Wiley, 1987.

Sheridan, TB. (1992). Telerobotics, *Automation and Human Supervisory Control*. Cambridge, MA: MIT Press, p. 311).

Sheridan, T. B. and Simpson, R. W. (1979). Toward the Definition and Measurement of the Mental Workload of Transport Pilots. MIT Flight Technology Laboratory Report R79-4, January.

Sheridan, T. and Parasuraman, R. (1999). Human vs. Automation in Responding to Failures: An Expected-Value Analysis, submitted paper.

Sheridan, T. (1999).Weighing situation awareness against time to respond: a basis for allocating attention, submitted paper.

Swets, J. & Pickett, R. 1982. *Evaluation of diagnostic systems*. New York: Academic press.

Wickens, C.D. (1992). *Engineering Psychology and Human Performance*, 2nd Edition. New York: Harper-Collins.

Wiener, E. L. & Curry, R. E. (1980). Flight-deck automation: promises and problems. *Ergonomics*, 23(10), 995-1011.

Wilde, G. J. S., L. J. Cake, and M. B. McCarthy (1975). An Observational Study of Driver Behaviour at Signalized Railroad Crossings. Canadian Institute of Guided Ground Transport Report No. 75-16.

Williges, R. C. and Weirwille, W. W. (1979). Behavioral measures of aircrew mental workload. *Human Factors* 21: 549-574.

Woods, D.D. & Roth, E. M. (1988). Cognitive Systems Engineering. In M. Helander, (Ed). *Handbook of Human-Computer Interaction*. Amsterdam: North-Holland Elsevier.[end]