Society for Applied Anthropology, Annual Meeting, Seattle, WA

Session (F-72) Design and Risk in Problem Resolution, Friday, April 1, 2011

CHAIR: **GAMST, Frederick C.** (U Mass-Boston)

GAMST, Frederick C. (U Mass-Boston) **fcgamst@aol.com**

The Designer as Phantom Crewmember in Human-Machine Systems, Including Those Computer Controlled

> In a way . . . every accident is due to an error of some sort by someone: by the person, usually a manger or supervisor, who decides what to do; by the person, often a designer, who decides how to do it; or by the person, usually an operator or maintenance worker, who has to do it.
> (Kletz 2001:328)

DRAFT

In our advanced industrial world, we strive to enhance operational safety. The design of machines and procedures for their use can affect human tasks to result in operator errors and accidents. Systemically viewed, designers and their design flaws can constrain correct operator action and thus be causal in operations resulting in human errors and, additionally, in physical failures. We discuss the North American railroad industry. There, we could posit an invisible designer as a phantom member of every railroad crew (i.e., team) in the movement of locomotives and railcars. This also holds for the jobs of other railroaders but here we limit to train crews.

We have long known, "By designing machine components in either this way or that, the [designer], in effect, changes the job for the human operator" (Chapanis 1965:23). "Mistakes appearing in the human part of the system often have their origins in design flaws. These can have a significant impact on . . . operations…" (GTRI 1999:1-5). The consequences of the designer's flaws are born by the operator. Uninformed outsiders judge as self-serving any operator's complaints about designer's constraints on behavior.

Advanced technological systems with computer-control features can have an unanticipated "brittleness." "This brittleness can arise because of the inability of the designer to anticipate and design for all the scenarios that could arise during use of the system, a deliberate decision by the designer to use an oversimplified model of the decision task (due to cost, time or technological limitations), a failure of the designer to correctly anticipate the behavior of the system in certain situations, or failure to correctly implement the intended design" (Smith et al. 1997:360). A designer might not understand the entire range of variation of his system's operation in the rail world. However, the designer must consider all the performance shaping factors (PSFs) affecting system use. PSFs are a

complex of elements including, "especially equipment design and the written procedures or oral instructions," affecting an operator's performance (Bahr 1997:153).

In the now ubiquitous computerized machine systems, the operator is a member of a new kind of decision-making team. Sharing decision-making is the team of active operator, active control computer, and latent (upstream) designer, (Czaja 1997:23; DeGreen 1991).

A designer's decisions for a computerized machine system limit the operator and control computer decisions. The question is, In the dynamic *open* railroad environment of switching railcars, to what extent *does* and *can* the operator know the limits of his decision-making ability? In other words, What is the boundary between operator reliability and control computer reliability, as set by the designer?

For brevity, we focus on the burgeoning use, since 2002, of the radio remote control locomotive (RCL) and its attending crew of one or two remote control operators (RCOs). An RCO operates an RCL using controls and displays on a body-mounted box called an operator control unit (OCU). Via coded, digital radio signals, the OCU communicates with the RCL's onboard control computer (OCC), which executes tractive power, braking, and other RCL functions. For various designed reasons an OCC could command a stop, e.g., in a radio communication break with its OCU.

A human-automation interface (HAI) is a critical part of today's steadily developing and enveloping human-machine interface (HMI). [i] As noted by Christoffersen and Woods (2002) and Woods et al. (2010:141-170), problems can exist, generated by the uncertainties of interfaces of human operators and computer-based automated systems.

In what ways do these problems of interface exist in RCL automation? What we must question is, How close is a particular subsystem of automation to the limits of its competence? Furthermore, although designers intend automation to reduce human

mental and physical workload, Does it ever increase either of the two and, if so, under what circumstances (cf. Harris, Hancock, Arthur and Caird 1995)? [2] Let us turn to issues of switching cars with an RCL in the RCO's railroad work environment.[3]

A railroader comments on an autonomous, designed stop causing slack action: "Another incident in 'VBN' caused broken ribs and lacerations when an [RCO] helper who was riding the point of a long cut of cars experienced a comm[unication] break. The [RCL] responded as it had been programmed, and applied full independent and automatic brake. When the slack ran out, the helper was thrown from the end of the cars." The phantom crewmember had struck.

An RCO explains a design flaw: "The locomotive [RCL] could run up against an obstacle, or could even pull a cut of cars with a derailment down in the string. It would keep adding throttle amps attempting to attain the [OCU's] set speed until it was unable to move. Only then would it interpret a problem condition, cut throttle, apply brakes, and transmit a 'locomotive movement failure' radio alert, requiring further action from the RCO."

Regarding designed detrimental OCC autonomy, an RCO recognizes, "the consequences of ceding braking decisions to the RCL computer, for example on a grade where the choice may be to reserve braking capability rather than regulate for a particular set speed." The phantom can take too much control.

An RCO explained that another RCO was making a drop when his RCL experienced communication failure and the OCC, as designed, immediately killed tractive power and applied the air brakes. The car cut off in motion in the drop then collided with the stopped RCL, which could not run in the clear of this car as intended to do by the RCO. In its designed "safety" logic, through the OCC, the phantom made an unsafe decision.

A railroader comments on what could be seen as a loophole in the designed RCL safeguards: "The 'GHJ RR' had a fatality involving RCL that was at least in part, the result of equipment failure. The [RCO] foreman was controlling the movement while the [RCO] helper was lining switches ahead of the [RC] locomotive [and its cars]. The movement stopped, and the helper's secondary OCU [RCD] indicated a comm[unication] break. The helper was unable to contact the foreman by radio, and [the foreman] found that [his helper] had been run over by the cut of cars he had been controlling. When [the helper] fell, he hit the on/off power switch on his OCU, preventing it from initiating a man-down alarm and emergency stop. The carrier quickly said the foreman should have been more aware of his surroundings, and issued a safety bulletin to other carriers."

One RCO with a 3-point stance on the side of a moving railcar experienced an OCC's autonomous stopping action by design and the consequent slack action threw him from the car side, fortunately, clear of the movement. This autonomous action of the phantom could also have thrown this RCO into the path of the movement. The movement continued for two car lengths before coming to a stop.

The RCL system's logic cannot always negate human error. When, an RCO erroneously transmits to his RCL a signal for direction of movement that is the opposite of what he wants, the RCL cannot correct that error. The RCL's OCC can have no judgment about such human action. Given the constant changes in rail switching, the direction of movement constantly changes. On this point, an RCO said: "The reason I'm mentioning this is because with Remote Control, the RCL will never (repeat, NEVER EVER!) question whatever command it's given. It'll do exactly as it's told 100% of the time." The phantom's judgment is limited in safety-critical situations.

A good number of RCOs have commented that the phantom, through the OCC, can make an autonomous stop that is hazardous given a particular circumstance. As one RCO comments, "There are times when dead in the water is the last thing you want to be. . . . Cars rolling back out of tracks to foul the lead, unexpectedly meeting a train coming at you, racing to catch a car that got loose down the wrong track." Phantom, do not thus stop the RCL!

A railroader summarizes regarding some aspects of phantom control: [4]

> "The software simply cannot anticipate grades or adjust to changing conditions as well as a human can. Speed regulation is specified at plus or minus 1 mph, however in reality, 3-4 mph variations are common. At times, the locomotive will seem to be unresponsive to commands sent from the OCU. In the incidents I am familiar with, this was the result of either a comm.[unication] loss or the locomotive attempting to adjust to an increased load. During a comm[unication] loss, the [RCL] will not receive or respond to a command for up to 5 seconds. If a crew is attempting to spot an industry track, this may be an excessive amount of time to be out of touch with the locomotive. And if the operator is not aware of the locomotive's response to changing load, it could result in a personal injury or fatality. For example, let's assume an operator couples into a cut of three cars that have air or handbrakes applied. The movement stops, and the operator forgets to place the speed selector lever in stop position before going between the cars to release a handbrake or adjust a drawbar. At some point, one of several things will happen: In 50 seconds, the alertness monitor will begin to sound, and in 10 more seconds, it will stop the movement. Within that 50-second window, the amperage on the locomotive will continue to build until the unit is able to move the cut of cars, possibly running over the operator in the process."

In conclusion, a phantom crewmember's (i.e., designer's) automatically autonomous and/or authoritarian actions through the OCC could be seamlessly hidden and thereby rendered opaque to an RCO. Such occurrence has resulted in a number of kinds of hazard enacted by a designer crewmember. Unforeseen hazards could well exist.

[i] Human-Machine Interface (HMI): We could consider the HMI as an abstract plane across which operator and machine exchange information. HMI, then, involves study and application regarding factors of interaction between human operator(s) and a machine including human, perception, decision-making, information-processing, capabilities and performances, task procedures, reactions to equipment layout and design, and integrations of physical stimuli and learning experiences. Hence, the designation HMI is often indistinguishable from human factors. A human's interface with a machine could be with a machine to variable degrees autonomous and even authoritarian.

Autonomous control system: An automated system can be to varying degrees or entirely autonomous, where it functions independently without control by a human operator. Thus, the system independently executes actions without immediately preceding specific human commands. In advanced automated systems, the human operator shifts tasks from active to supervisory control of the machine. Such system might also be to varying degrees or entirely authoritarian in not providing adequate or any feedback to the human operator regarding his supervisory freedom for independent judgment and action. For an operator, seamlessly hidden and thereby rendered opaque to him could be an automated system's autonomous action and, additionally, its physical failure resulting in autonomous "fail-safe" action that cannot guarantee operational safety. Autonomous authoritarian systems are often tightly coupled. Christoffersen and Woods hold that the central issue is not the levels of autonomy and authority but, instead, the amount of coordination between the human and machine components of an automated system (2002).

Specifically, HMI is a human's interaction with a machine through controls, displays, and data input devices. When an RCO does a task involving direct contact with a device, such as an OCU, the components of the OCU that he manipulates and/or observes are his HMI, for the task duration.

[2] Expanding on these thoughts, in complex automated systems, the direct operating team consists of human(s) and control computer. For such systems, increasingly, a human communicates with as well as operates a machine. Automated systems have been implemented which are more autonomous and authoritarian than previously, while giving the human operator inadequate feedback (Billings 1997:4). In these systems, What are the limitations of the role of the operator in executing control actions? The machine in the system is not a passive but an agent-like device functioning at high levels of autonomy and authority. This machine can autonomously operate without an immediately preceding operator input and can authoritatively override operator intention. Such operating can engender novel responsibilities and events for the operator. These events can include sometimes-serious problems of breakdowns in interactions of the human and the control computer. Root causes of the events go beyond just the operator at the point of control and reach up to include the limitations set by the suppliers and the manager-implementers of a system. Implementers of a system could find unexpected consequences because their system did function as a team player (Norman 1990; Sarter and Woods 1995, 1997; Sarter, Woods, and Billings 1997; Mitchell and Sunström 1997).
The key issue with automation autonomy in a system is, How does it interact with operators and how might it enhance or degrade their performance? Does autonomous computer control shape the actions and thoughts of operators in ways unforeseen by its designers and managers who implement it (cf. Parasuraman and Riley 1997)? To what extent, if any, do inadequacies in the HMI as designed foster accidents and near misses? Does the placing of automation between the RCO and his RCL, at times, remove him from the elements of operation?

[3] This long endnote 3 is about the intricate, demanding nature of railroad switching work in North America. The work is different from such tasks studied abroad, e.g., in Eritrea, Ethiopia, Germany, and the United Kingdom.

Some human-factors literature deals not, as traditional, with an individual operator but with a team of operators, as in process industries such as a power plant or petroleum refinery. In such studies and also with individual operator studies, the analyst investigates layout of (fixed) equipment and workstations crewed with reference to these fixities. Among other things, in team studies, the analyst reviews amounts of compatibility among team members and the fixities. In switching, no fixities of rolling equipment or workstations exist. All

are dynamic, in myriad, transient permutations. Accordingly, physical anchoring points in analysis are ephemeral.

The Open Physical Environment of Switching

Most human factors studies of a workplace discuss environmental elements such as levels of illumination, noise, and temperature as well as flow of fresh air, exhaust venting of any dust and toxins, removing floor clutter, the condition of restrooms, and the amenities of the cafeteria. Analysis concerns flow of work past machines and operators along with the nature of firsthand supervision. None of these environmental elements apropos of fixed plants obtain in railroad switching's outdoor, all weather, mobile, 24/7/365, highly dynamic moving of heavy equipment on track, sometimes in thousands of tons per single movement. In a word, railroad switching is a different kind of work.

Human factors applications also abound having physical barrier safeguards to prevent or lessen an accident in a plant. Gilbert Marshall discusses these barrier safeguards, in his "Principles of Machine Guarding." The safeguards include enclosure of a machine or its moving parts, interlockings where a body part cannot be inserted when a machine operates, and automatically imposed safeguards (Marshall 1982:341-369). These cannot obtain in rail switching because the essence of the work is to move in the open huge rolling equipment, singly and in varying numbers. As Kjellén notes regarding certain industries: "Traditional safety measures such as guards, will in many cases be unfeasible" (1987:172). Marshall also lists for discussion "fail-safe brakes" as a physical safeguard but says that "they can hardly be called guards" (1982:352). This is because when a so-called fail-safe brake fully stops all motion, a loss might have occurred during the stopping duration.

In North America, railroad switching occurs within the confines of a central or satellite yard of a terminal, from a main track both within and outside of main-track yard limits, and in settings of industrial yards and spurs apart from a terminal's central yard. Both road freight-train crews and yard switch-engine crews do switching (marshalling). Crews conduct switching every day of the year, around the clock. Thus, switching is in fair weather, subfreezing cold, torrid heat, intense wind, rain, snow, fog, and blowing dust, including in poor-illumination and pitch-black settings. At times, background noise can drown out sounds of rolling equipment. All tracks are "live," i.e., can have rolling equipment moving in any direction at any time by one's own or another engine and, accordingly, a track must not be fouled by one's body except when required by a task. Clearances between tracks are close and, at switches, narrow down to space not permitting presence of a human body. "Kicked" free rolling cars are usually quiet in their approach and thus railroaders sometimes call them "silent death." A single car's weight can range from about 23 tons empty to over 130 tons loaded and may move in "cuts" (drafts) of several hundreds to many thousand tons and in lengths of up to a mile, or more. Footing can be insecure, with rough crushed rock ballast, depressions in the ground, debris strewn between tracks, and possible icy and slippery surfaces. Configurations of locations to place one's body on different kinds of freight cars vary regarding grab irons, foot stirrups, ladders, and platforms.

Operating railroaders must react to and attempt to control myriad kinds of events occurring, some intruding, into a railroad's ubiquitous, open physical environment. In the sciences, a closed system is considered as isolated from the environment. An open system is not isolated. The railroad-switching environment is an open system. As such, 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-occurring, varying numbers of often-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. Thus, a particular final state can be reached from different initial conditions, and the same initial conditions can result in different final states.

The Switching Tasks, an Overview

Many variably sequentially interacting and simultaneous tasks compromise a crewmember's situational awareness while on the ground switching. A crewmember responds to many cues, some gross, some subtle, and some for which he might not be fully or at all aware.

Switching tasks include reading and comprehending a switch list (of cars to be moved to a particular location); giving and receiving manual signals by hand, lantern, and fusee (flare); giving and receiving voice-radio signals; monitoring voice-radio traffic to help maintain situational awareness; hanging on to the side of rolling equipment; climbing on and dismounting from such equipment; applying and releasing car hand

brakes; aligning track switches and derails; kicking cars; dropping cars; riding cars to a coupling; reading car identifying letters and numbers; judging the speed and closing distance of cars to be coupled to other cars, often while riding on the side of the lead car of a movement; observing close clearances and obstacles such as switch stands, rails, gates, and walls; safeguarding pedestrians and automotive vehicles in the vicinity; handling hazardous loads; knowing the location of other crewmembers and other impacted railroaders; thinking about particular chess-like moves in the efficient switching of cars; thinking about an overall schedule for the day's work to be done; assessing movements of other engines, road trains, occasional nonrevenue equipment such as roadway vehicles on flanged wheels, and fouling rubber-tired vehicles; always thinking about tasks with reference to the complex code of railroad operating rules; at rare times, being the person on the scene who has to attend to an injured or killed human, employee or other; and walking and standing in the dynamic, open switching environment. When no yardmaster is on duty in a yard, a conductor or engine foreman engaged in switching might also work as a footboard yardmaster. Then, he must direct, other movements such as trains and engines, including their rail traffic control, entering, leaving, or performing work in that yard, as well as monitor the voice-radio for any problems. When a Remote Control Zone is established, he must also provide protection for or respect that zone.

Switching tasks of one individual might be dependent on the actions of another person on the same crew, on a different crew, or of a railroad employee not on any crew, or, perhaps, of a nonrailroader, e.g., a "civilian" waving his arms violently near the tracks, falling across a track, or fouling a track with his vehicle. Thus an operator's error resulting in an accident or near miss could be, in whole or in part, from an error of commission, omission, or extraneousness or a violation by another individual or team. Accordingly, for every case, an analyst cannot simply decompose an accident or near miss into the actions and HMIs of a single railroad employee. The actions might be dependent upon the actions of another or others. Dependency could also be considered as an aspect of the open environment of railroad operations.

Human Interaction with Tasks and Physical Environment
(This subsection benefits from discussions with nuclear engineers who have assessed power plant and other nuclear reactors.)

For switching work, the potential events could be considered randomly or almost randomly occurring. Randomness is from the huge range of human interactions with the many above single task and environmental variables and with the interfacing combinations among these variables. Accordingly, with these dynamically combinative variables as initiating events for a switching error, no overall structure for potential events in the rail world can be readily ascertained to use in the calculation of probabilities of human error and dependencies related to an error.

In comparison, when studying human error and consequent risk regarding work with nuclear power plants, we find the physical environment is one of a secured, sequestered, highly managed and controlled, and industrially hygienic setting. Moreover, many possible operator errors and rule bendings and breakings in performance of tasks are “locked out” in the design of the human-machine interface and also recorded. For nuclear reactors, the number of combinations among human tasks and physical environmental factors is far more limited than for switching. Consequently, the number of potential kinds of error-producing events from performing human tasks and interaction with the physical environment are far more limited than for switching.

A railroader notes: “I am continually challenged when it comes to applying mathematical models to predict probability for human error in the railroad industry. The variables found in the railroad work are too variable to give me confidence in a result based on mathematics. I can see where plugging a number in somewhere along the equation to account for these uncertainties may address the concern. Knowing where and when to put the number in the equation is important to avoid skewing the result. The dynamic railroad environment does not lend itself to the techniques used in other industries.”

A railroader comments on the necessary local variations of switching practices because of particular local characteristics: "With both ends of the yard a 1% down grade, kicking cars in that yard meant revving up and getting a cut up to 15 mph, and then maybe the cars would clear in the track. Of course, they were just as likely to come right back at you at the same speed unless tied down with good handbrakes. After kicking one car, you always had to pull forward because of the grade."

Similarly, an RCO reports: "The RCL accident had everything to do with the more subtle aspects of car handling like which tracks do you have to watch closely because the cars will come back at you. I always point out these sorts of dangers to the students but then they give you that glassy eyed look that tells you they won't remember anything in the morning." (An RCO, remote control operator, is a switchman, brakeman, conductor, or locomotive engineer who operates a remote control locomotive, RCL, via processor-mediated coded digital radio signals from a remote control device mounted on his/her body.)

A railroader reports regarding an RCL roll out of cars: "[Job designation and location] struck two cars that had rolled out of an adjacent track. After shoving a cut into Track [1] to a spot on the west end, the crew cut off four excess cars and set them to Track [6]. While pulling out of Track [6] with the light engine, crew was riding on rear platform and did not see that the cars they had left in Track [1] had rolled out. The RCL struck the two cars while moving at an estimated speed of 8 MPH, derailing the robot and the two cars."

In all, railroad switching consists of a large number of frequent cognitive and manual active interventions in the personally life-critical, operationally safety-critical work process. The interventions are not passive monitoring as frequently done in large-scale, automated process industries (cf. Moray 1997:1944-1949; Sharit 1997:316-317). Moreover, rail switching interventions are usually contingent upon and have consequence for similar interventions of others.

The Ever-Present Potential for Railroad Catastrophe Including in Switching

America's railroad industry constitutes a highly dispersed, potentially catastrophic worksite, with respect to its movement of trains and engines and the switching of rail cars. This linear worksite branches for 169,000 miles across forty-nine states, and pierces through the heart of most communities of any size. Operating crewmembers directly perform the potentially catastrophic work on railroads. (Catastrophe is as conventionally defined by the risk-assessment use of the federal MIL-STD-882)

Regarding the harmful results of railroad catastrophe, the U.S. General Accounting office reports, "thousands of people are evacuated from their homes as a result of the hazardous materials that are released during train accidents" (USGAO 1997:3). Between 1978 and 1995, about 261,000 persons were evacuated from their homes, nationwide, because of releases of rail-related hazardous materials. "Concerns remain about evacuations because the volume of chemical traffic increased by over one-third from 1976 to 1995," the GAO concludes (USGAO 1997:4, 36). As Railway Age editor John Armstrong writes regarding the issue of safety on railroads: "there's always a 'knock on wood' realization that a combination of events and circumstances can lead to a wreck of proportions sufficient to tarnish the best of records" (1982:32). John's experience led him to say that rail accidents come from a combination of events source, personal discussions).

The work of operating crewmembers is safety critical and involves mental and manual responsibilities and tasks for the mastering and safeguarding of movements on track of rolling equipment having great kinetic energy. The movements, although indeed potentially catastrophic, are only rarely disastrous because of these crewmembers' proper performing of tasks and proper fulfilling of responsibilities on the job. At its core, such safety-critical performing and fulfilling depends upon learned and maintained judgments and skills. Maintaining the experience-based judgment and skills for operating crews further lessens, always-unacceptable, catastrophic risk, thereby protecting railroader and public health and safety.

[4] We could go on with examples. Perhaps the following sums the issue of phantom crewmember. A number of RCOs report the RCL is exactly that, a locomotive remotely radio-controlled by an RCO--from any location. RCL operations, then, are not fully automated, i. e., handled entirely by the OCC. Accordingly, an RCL movement can exceed the design capacity of its independent brakes to stop in a safe distance. Stopping distance is, of course, relative to the variables of tonnage handled, gradient, speed, rolling resistance, number of operable engine brakes, and adhesion quality of the ball of the rails. An RCO's training, experience, and consequent judgment regarding these variables is the human safeguard for preventing such an unstoppable movement.

As CANAC wrote regarding a runaway RCL movement at Agincourt Yard on the Canadian Pacific: "There are clearly some misunderstandings about the LCS [RCL] system, and they should be rectified as soon as possible." Additionally, "Furthermore, the LCS Unit was never designed as a robotic automaton but as a Remotely Controlled Locomotive. The LCS [RC] Operator is still ultimately responsible for the consist

movement." Thus, “Having demanded a full 100% Independent Brake output, the MCU [OCC] could do no more.” CANAC concluded: "Therefore, the Grade Force exceeded the available Brake and Rolling Resistance Forces" (CANAC 1996). An RCO comments: "I don't like what this technology does to the work environment. I disagree with the basic assumption that the computer adequately takes over all the skill decisions."

Similarly, an RCO reports, a Primary RCO on an RCL pulled a long, heavy cut in a busy yard and misjudged the stopping distance of the cut. The RCO thereby fouled a lead on which rolling equipment was moving and collided with a car. Here, what could have been a more common near miss became an accident, owing to an error of commission. As with the Agincourt accident, Was this error entirely that of the RCO or also of a person or persons on a higher organizational or extra-organizational level? Was a phantom crewmember involved?

In other words, as an RCO says: An RCL is not like today's fully automated elevator, which was, in the past, manned by an elevator operator.

That is, the RCO cannot simply manipulate a control on the OCU and leave the movement and its safety for some period to the OCC. An RCO has continuous responsibility for the continuous informed, safe execution of operating tasks with his RCL.