The Role of Automation in Complex System Failures

Article *in* Journal of Patient Safety · March 2005

DOI: 10.1097/01209203-200503000-00010

3 authors:

Shawna J. Perry
75 PUBLICATIONS 1,264 CITATIONS
SEE PROFILE

Robert Wears
University of Florida
288 PUBLICATIONS 11,544 CITATIONS
SEE PROFILE

Richard Cook
Adaptive Capacity Labs
143 PUBLICATIONS 4,615 CITATIONS
SEE PROFILE

The Role of Automation in Complex System Failures

Shawna J Perry, MD

Assistant Professor

Department of Emergency Medicine

University of Florida Health Science Center

Robert L Wears, MD, MS

Professor

Department of Emergency Medicine

University of Florida Health Science Center

Richard I Cook, MD

Assistant Professor

Department of Anesthesiology and Critical Care

Director, Cognitive technologies Laboratory

University of Chicago

Address correspondence to Dr Perry at:

Department of Emergency Medicine
University of Florida Health Science Center
655 West 8th Street
Jacksonville, FL 32209
904-244-4405 (voice)
904-244-4508 (fax)
904-498-0443 (digital pager)
sperry@ufl.edu

Drs Wears and Perry were funded in part by Army Research Laboratory Contract DAAL01-96-C-0091. Dr. Cook was funded in part by the Department of Veterans Affairs through the Midwest Patient Safety Center of Inquiry (GAPS), Marta Render, MD, Director. The views, opinions, or findings herein are those of the authors and should not be construed as either Department of Defense or Department of Veterans Affairs position or policy.

Keywords: Automation, computer technology, systems failure

Word count: 3242

Abstract.

Although proponents of advanced information technology argue that automation can improve the reliability of health care delivery, the results of introducing new technology into complex systems are mixed. The new forms of failure that accompany automation challenge technical workers, often demanding novel approaches to recovering from failure and restoring system operations. We present a case where automation created a new form of failure that was not foreseen. In this case, human practitioners were the main source of robust and reliable healthcare delivery and were the primary agents in recovering from a life-threatening automation failure. The features of this case correspond closely to experience with new information technology in other domains and have implications for plans to improve patient safety using technology.

Introduction.

Efforts to improve patient safety often focus on automation [1] as a means for preventing human practitioner “error”. Technological change in an ongoing field of activity, however, produces a complex set of organizational reverberations that are difficult to anticipate or predict and may go far beyond the expectations of designers [2]. Although some evidence suggests that information technology can defend against some types of failure [3], the impact of automation on system performance is a mixture of desirable and undesirable effects. In commercial aviation, for example, cockpit flight management systems have changed the nature of the pilot’s work, creating new tasks and shifting workload from slack to already busy times [4,5]. Although automation may reduce workload in one area within healthcare (*eg*, transcribing orders), it will also generate new workload (*eg*, navigating through multiple displays, or restructuring work around computer terminals rather than at the bedside).

Automation is rarely deployed as an appendage to ordinary work. To achieve its benefits, automation needs to be inserted into the operations of the system, becoming intimately woven into the system itself. Often it replaces some part of the predecessor system, making any retreat to the ‘old way’ of doing things difficult or impossible. Once automation and system operations are coupled, critical system operations then become vulnerable to automation failure[6]. These unexpected effects are most readily seen in work settings where serious consequences, time pressure, and semantic complexity combine. Here, rapidly evolving situations place a premium on smooth integration of human and machine agents into a working team capable of quick, decisive action [7]. Examples of such work settings include the operating room, the intensive care unit, and the emergency department. This paper reports an archetypal case involving the failure of an automated drug-dispensing unit in an emergency department, its local consequences and some of the implications for proposals to use automation to advance patient safety.

Case Description.

The incident occurred in a 450-bed teaching hospital with a busy emergency department (ED) serving a large urban, indigent population. During the late evening hours, a 29-year-old woman with a history of asthma, hypertension, congestive heart failure, chronic renal failure requiring hemodialysis, and human immunodeficiency virus (HIV) infection presented to the ED complaining of shortness of breath. After some time in the ED she became acutely agitated, diaphoretic and had marked tachypnea and tachycardia. Her O_2 saturation by pulse oximeter was 90% while breathing 100% F_iO_2 by mask. Intravenous access was obtained and continuous beta-agonist nebulization with albuterol, subcutaneous terbutaline, intravenous corticosteriods, and intravenous magnesium sulphate were ordered.

The resuscitation nurse went to obtain medications from an automated dispensing unit (ADU), part of a computer-based dispensing system in use throughout the hospital. He found an uninformative error message on the computer screen ("Printer not available") and an unresponsive keyboard. The system did not respond to any commands and would not dispense the required medications.

The patient was well known to the ED staff. On a recent visit, she had deteriorated rapidly to cardiac arrest and had been successfully resuscitated. With this history fresh in mind, the primary ED nurse abandoned efforts to get the ADU to work and asked the unit clerk to notify the main pharmacy that the ADU was “down” and emergency medications were needed. He asked another nurse to try other ADUs in the ED. Other ED staff became aware of the problem and joined in the search for albuterol and magnesium sulphate ampoules. Some were discovered on top of another ADU in the ED, waiting to be returned to stock. Anticipating the patient’s clinical deterioration, the ED physicians opened the resuscitation cart (“crash cart”) and prepared to intubate the patient, using the medications and equipment stored there. A pharmacist came to the ED and examined the unresponsive ADU. He decided not to use the bypass facility for downtime access because neither the drawers nor the bins were labelled with the names of the medications they contained, and this information could not be obtained from a non-functioning unit. Instead, he arranged for the pharmacy staff to use runners to bring medications from the main pharmacy, one floor below, to the ED in response to telephone requests. The patient eventually received the requested medications; her condition improved transiently, but she was intubated four hours later. She survived and was later discharged from the hospital.

After the event, staff members were debriefed by the authors and the events of the incident reconstructed along the lines used to investigate other technology related events[8,9]. The ED staff were astonished to discover that there was no general way to access medications when the system was down, even for the pharmacist; they had taken for granted that such access must exist. Nursing staff generally viewed the ADUs as useful because they automated the tracking of controlled substances. Several expressed concern that a similar episode might lead to serious patient injury or death. Staff admitted that in the future they might keep reserves of important medications outside of the ADUs in order to have access to these drugs in case of another failure.

The Chain of Events.

A series of interviews with the ED staff, pharmacists, computer specialists and the ADU manufacturer's representative enabled a reconstruction of the complex sequence of events leading to this incident (Table). The hospital had installed a popular computer-controlled automated dispensing system for drugs and supplies in 1994 to improve inventory tracking and reduce errors and pilferage, especially of controlled substances. The system was regarded as mature and reliable, and had been regularly upgraded. Other than a limited number of resuscitation drugs stored in "crash carts", all hospital medications were dispensed via this system. At the time of this incident, there were 40 ADUs linked to two centrally located computers by a general-purpose computer network that provided connectivity to the hospital information system (HIS).

To enhance safety within the hospital, the ADUs were programmed to deny access to a drug unless there was a current, valid, pharmacist-approved order for it in the HIS pharmacy subsystem. This safety feature was implemented by a software interlock mechanism between the HIS, the pharmacy computer, and the ADUs. When a user attempted to retrieve a drug for a patient from the dispensing unit, the ADU would query the HIS via the pharmacy computers and provide the medication only if a validated order could be found in the HIS. This feature was not activated in the ED because of the time constraints associated with ED drug orders and delivery.

About two weeks prior to the incident, the hospital began a major HIS software upgrade that was complicated by a sudden, unexpected hardware failure resulting in the complete loss of all HIS functions. In response, operators in the pharmacy disabled the safety interlock feature that required order checking before dispensing medications so that nursing staff on the wards could obtain drugs. As the HIS came back online, the pharmacy operators enabled this feature in order to restore normal operations. However, the HIS crashed repeatedly during this process, prompting the pharmacy operators to disable the safety interlock feature again.

The procedure for enabling and disabling the safety interlock feature entailed dialog between the pharmacy central computer and the ADU computers, which was conducted for each item in the inventory of each dispensing unit. When this procedure was started on the day of this incident, it unexpectedly created a storm of messages to and from the dispensing units. This message storm slowed the system response such that the individual units appeared to be unresponsive to keyboard commands from users. The pharmacy operators initially thought that network communication problems were causing the outage, but gradually came to realize that the network was functioning normally but that the ADUs were overwhelmed with messages. This phenomenon was essentially similar to denial-of-service attacks that have occured on the internet [10]; the ADUs were unavailable to the users because they were busy with a large number of messages. Eventually most of the ADUs appeared to resume normal operation. The operators had assumed that ED units would not be affected by this procedure because they did not use the order checking feature. The specific reasons for the message storm, and for why the ED unit did not resume normal operation could not be determined, leaving a residual and unremovable mystery about the system.

Discussion.

The introduction of new automation has multiple effects. Some of these are intended and anticipated while others are not. Significant and often unappreciated changes occur in the conduct of technical work; old tasks are modified or replaced with new ones. By changing the types of vulnerabilities present in the system, automation changes both the sorts of problems that arise and the ways that workers discover, understand, and cope with problems. By virtue of increased "coupling" between components of the system, automation generates opportunities for a complex systems failure, a "normal accident"[11,12]. It would therefore not be rational to view this incident as the result of " just another poor product choice" by a product selection committee. It would be also be short sighted to assume that failure mode and effects analysis could have anticipated this type of failure. Planners had anticipated several failure modes with the ADUs, (*eg*, jammed drawer or power failure), but thought that the availability of cardiac arrest medications in the "crash cart" would be sufficient compensation until down-time procedures could be established or the system restored to operation. The urgent (within minutes) need for non-cardiac arrest drugs was not anticipated and represented a latent vulnerability in the system.

In this case, a severe, potentially life-threatening event arose from the conjunction of the characteristics of the automation, the situation facing the technical workers, and the features of the organization in which the work took place. The genesis *and resolution* of the incident involved automation, human, and organizational factors.

Automation factors.

1. The failure sequence began in technical components that were distant in time and space from the place where the failure became manifest. Of particular note, the initial fault, (hardware failure in the HIS), occurred well before the consequences of that failure were experienced in the ED. This propagation of effects to distant times and places to create new problems is a characteristic of *tightly coupled* systems[11]. Because of the complex interdependencies of information technology, failure in one technological component rippled outwards to affect distant devices. Rather than being robust in performance, the automated dispensing process itself was exquisitely *contingent*, in that small changes in remote parts of the system resulted in large consequences elsewhere[13].

2. Ironically, the automation failure was a side effect of an effort to produce “safety” through automation. A design feature (the order interlock) was supposed to forestall a particular form of failure, *ie*, the “human error” of a nurse taking an unprescribed drug from the dispensing unit. An unintended consequence of this pursuit of technological safety was the

creation of the conditions necessary for a new and unexpected form of failure. The side effects of the pursuit of safety via automation may produce new forms of failure. Rather than being simply an unalloyed reduction of risk, the use of automation involves trading off of one set of risks for another. In this case, the risk of the wrong drug for one patient was traded off against the risk of no drugs for anyone. It is ironic that engineered safety devices sometimes contribute to accidents themselves, mostly by increasing the complexity of the system and the attendant potential for unexpected interactions[14]. Although the majority of ADUs currently in use in the US do not use order checking mechanisms [15,16], such mechanisms are needed if the full benefit of these devices is to be achieved.

3. The automation failure was *opaque* to the users. The ADU appeared to be working normally (the touch screen was lit), but it was unresponsive and its failure was not apparent to users until it was needed for a critical function. The operators of the HIS and pharmacy computers were not aware of the ADU problems until they began to receive calls about system unavailability and initially misdiagnosed the failure as a network problem. There was no way for end users to determine the cause of the failure or to devise means for overcoming it. This forced them to invent means for "working around" the automation. Significantly, because the failure was

opaque, there was no way to form reasonable expectations about its likely duration, so the users needed to prepare to employ these “work-arounds” indefinitely.

4. The automation was *brittle*. Rather than degrading gracefully, the breakdown was complete: it prevented access to *all* medications. Because is was intended to act as a “forcing function” to prevent errors [17], the system was an intentional ‘choke point’ in operations. This allowed close control of narcotics and controlled substances, but also meant that units were designed to fail in ways that would prevent access to drugs (rather than reverting to floor stock, for example).

5. The failure was *astonishing.* Until it actually happened, the breakdown appeared to be impossible [18]. This is in contrast to, for example, a failure from loss of electrical power, which fits well into users’ prior experience of “how things work.” A power failure would surprise but not astonish users because they can easily see how a power failure would make the unit stop working. Significantly, it is impossible to prepare for astonishing failures because, before they occur, they are literally incredible.

6. The incident occurred not at the height of the HIS crisis, but rather during the attempt to return to normal operations. A variety of other information

system failures have occurred in similar circumstances, notably the Thomas Street telephone switching outage [19] and the America On-Line e-mail outage [20], and the Tenerife disaster [21]. In each case, efforts to maintain or restore operations of the system led to the propagation of overt, large-scale failure. Complex technology is virtually always being upgraded or modified and the vulnerability that this activity produces is difficult to foresee.

Human factors.

1. Human practitioners as the source of system resilience. Confronted with brittle automation, the technical workers devised "work around" methods to make up for the failure. The design of the automation was predicated on the notion that workers are a potent source of failure ("human error") but in this case, successful recovery depended upon the very humans against whose "errors" the automation was supposed to defend.

2. Disturbance management. Workers quickly switched attention from fault diagnosis and correction (trying to make the dispensing unit work correctly) to disturbance management [22] (trying to keep the patient stable, preparing for intubation and resuscitation). The smooth shift between these two types of activity is a hallmark of expertise in process

control settings. When conditions change slowly and the consequences of faults are limited, effort can be focused on understanding and repair. But in high tempo settings where catastrophic failure looms, experts often must abandon lower level goals in order to preserve high level ones [12,23].

3. Anticipation and planning in the midst of crisis. High stakes and time pressure combine to limit the possible reactions to future events. The workers in this case anticipated future deterioration of patient's condition and prepared to cope. Their initial treatment plans thwarted by technical failure, the ED staff prepared to deal with the patient's expected deterioration by assembling the necessary tools and people to handle intubation and cardiac arrest. By mentally rehearsing the likely pathways the patient might take, they reduced the time required to react if it occurred. This rehearsal and visualization of future states is a consistent feature of expertise in multiple domains [24,25]. Time pressure significantly limits the ability to prepare for multiple future events, so strategic planning involves weighing the likelihood and consequences of future events and the effectiveness and costs of preparing responses.

4. Effective teamwork in the face of novel conditions. The ability to marshal, divide, and use both human and technical resources effectively is

a critical characteristic of successful coping with failure in complex systems. When catastrophic failure loomed, the workers were able to shift workload and devise novel strategies for coping with failure. The pharmacy runners for supplying drugs to the ED, the testing of other dispensing units, and the search for medications in the ED are all examples effective responses to failure that entail coordination among human practitioners. The communication between the workers that allowed sharing workload and the smooth organization of their responses is of particular note here. The ability to work cooperatively was attributed by several of the workers to teamwork training that preceded the event [26,27]. The contrast of human-human cooperation and the brittleness of the automation as demonstrated in this incident has been seen in other domains [5].

Organizational factors.

1. The automation failure demonstrates how the dispensing units served as a brittle bridge between pharmacy and nursing. These two parts of the organization need to interact in order for each to function. Using automation as their medium constrains their interaction to brittle, machine-based dialogs. These formal methods of communication are efficient and

cost effective but limited. Rather than welding the organisation into a seamless whole, automation here creates a brittle, narrow bridge that restricts communication. Handling events requiring organizational coordination requires workers to establish connections between other parts of the organisation – the system of runners in this case represents both a literal and figurative bridge between pharmacy and nursing.

2. The complexity of the technical and social system that delivers healthcare makes learning from failures difficult. Tracing the sequence of events and the reverberating consequences required substantial effort. The organizational response was muted; the causes of the failure, especially the automation, were regarded as beyond the reach of practitioners and not amenable to change. Ironically, some managers took the success of the practitioners in adapting to the failure of the automation as evidence of robustness of the larger system rather than of its vulnerability. ED staff learned very narrow lessons about how to cope with a particular form of failure; several indicated that they would maintain "off the record" supplies of certain medications as a defense against future failures, ironically countering one of the major organizational benefits of the ADUs. These disjoint views are remarkable; it is difficult to see how any effective organizational change could come from such disparity. In this

case, an effective organizational response did not begin until considerably after the reconstruction of the event chain above had been completed.

Conclusion.

Automation offers a variety of tangible benefits and is often proposed as a means to increase patient safety. But, as this case demonstrates, automation also creates new vulnerabilities, some with substantial consequences. Automation failures test the adaptive capability of practitioners. Significantly, the desire to forestall "human error" by practitioners can lead to brittle automation and new forms of failure that are difficult or impossible to foresee.

As in aviation, automation in healthcare produces mixed results [5]. Improving patient safety depends on creating robust and resilient systems of care. Although automation may play a part in such systems it is also a potent source of new vulnerability. Neumann points out that "over-endowing high-tech solutions is riskful in the absence of adequate understanding of the limitations of the technology and … human nature."[28] As we consider increased automation in health care, we should pay as much attention to anticipating new vulnerabilities and devising methods to detect and rapidly correct them as we do to the projected benefits.

Acknowledgement.

The authors would like to thank David D Woods, PhD, of Ohio State University for his insights and helpful comments during the investigation of the incident and preparation of this report.

References.

1. Leapfrog Group. Leapfrog initiatives to drive great leaps in patient safety. Business Roundtable. *http://www.leapfroggroup.org/safety1.htm*, accessed 17 October 2000.

2. Cook RI, Woods DD. Adapting to new technology in the operating room. *Hum Factors* 1996;38:593-613.

3. Bates DW, Teich JM, Lee J*, et al.* The impact of computerized physician order entry on medication error prevention. *J Am Med Inform Assoc* 1999;6:313-321.

4. Weiner EL. Human factors of advanced technology ("glass cockpit") transport aircraft. In: *NASA Technical Report 117528*. Moffett Field, CA: NASA Ames Research Center; 1989.

5. Billings CE. *Aviation Automation: The Search for a Human-Centered Approach*. Mahwah, NJ: Lawrence Erlbaum Associates; 1997.

6. Cook RI. Observations on RISKS and risks. *Communications of the ACM* 1998;40:122.

7. Woods DD, Roth EM. Cognitive engineering: human problem solving with tools. *Hum Factors* 1988;30.

8. Cook RI, Woods DD, Howie MB*, et al.* Case 2-1992. Unintentional delivery of vasoactive drugs with an electromechanical infusion device. *J Cardiothorac Vasc Anesth* 1992;6:238-244.

9. Klein GA, Calderwood R, MacGregor D. Critical decision method for eliciting knowledge. *IEEE Trans Syst Man Cybern* 1989;19:462-472.

10. CERT Coordination Center. Denial of Service Attacks. CERT. *http://www.cert.org/tech_tips/denial_of_service.html,* accessed 12 December 2001.

11. Perrow C. *Normal Accidents: Living With High-Risk Technologies*. Princeton, NJ: Princeton University Press; 1999.

12. Cook RI, Woods DD. Operating at the sharp end: the complexity of human error. In: Bogner MS, ed. *Human Error in Medicine*. Hillsdale, NJ: Lawrence Erlbaum Associates; 1994:255-310.

13. Bak P. *How Nature Works*. New York: Springer-Verlag; 1996.

14. Langewiesche W. The lessons of ValuJet 592. *Atlantic Monthly* 1998;281:81-98.

15. Survey of automated dispensing shows need for practice improvements and safer system design. *ISMP Medication Safety Alert* 1999;4:1-2.

16. Rich DS. Ask the Joint Commission: point -of-care automated dispensing devices. *Hosp Pharm* 1999;34:989-995.

17. Norman DA. *The Design of Everyday Things*. New York: Currency / Doubleday; 1988.

18. Sarter NB, Woods DD, Billings CE. Automation surprises. In: Salvend G, ed. *Handbook of Human Factors and Ergonomics*. 2nd ed. New York, NY: John Wiley & Sons; 1997:1926-1943.

19. Kuhn DR. Sources of Failure in the Public Switched Telephone Network. National Institute of Standards and Technology. *http://hissa.ncsl.nist.gov/kuhn/pstn.html*, accessed 11/15/1999.

20. Neuman PG. America Off-Line. The Risks Digest. *http://catless.ncl.ac.uk/Risks/18.30.html#subj1*, accessed 11/15/1999.

21. Weick KE. The vulnerable system: an analysis of the Tenerife air disaster. *Journal of Management* 1990;16:571-596.

22. Woods DD. Coping with complexity: the psychology of human behavior in complex systems. In: Goodstein LP, Andersen HB, Olsen SE, eds. *Task, Errors, and Mental Models*. New York, NY: Taylor and Francis; 1988:128-148.

23. Rochlin GI, La Porte TR, Roberts KH. Self-designing high reliability: aircraft carrier flight operations at sea. *Naval War College Review* 1987;Autumn:76-90.

24. Klein GA, Orasanu J, Calderwood R, Zsambok CE, eds. *Decision Making In Action: Models and Methods*. Norwood, NJ: Ablex Publishing Company; 1993.

25. Klein G. *Sources of Power*. Cambridge, MA: MIT Press; 1998.

26. Simon R, Morey J, Locke A, *et al.* Full Scale Development of the Emergency Team Coordination Course and Evaluation Measures. In. Andover, MA: Dynamics Research Corporations; 1997.

27. Risser DT, Rice MM, Salisbury ML, *et al.* The potential for improved teamwork to reduce medical errors in the emergency department. The MedTeams Research Consortium. *Ann Emerg Med* 1999;34:373-383.

28. Neuman PG. 11 September 2001 in retrospect. ACM Committee on Computers and Public Policy. *http://catless.ncl.ac.uk/Risks/21.66.html,* accessed 12 December 2001.

Table. Time Sequence of Events

Approximate Time	Patient	Clinical Staff	Automation
- 1 month	Sustains cardiac arrest and successful resuscitation in ED		
- 2 weeks			HIS software upgrade begins
- 11 days			Catastrophic hardware failure stops HIS functions
			ADU drug order interlock disabled
- 2 days			HIS function re-established
- 1 day			ADU drug order interlock enabled
- 1 hour	Arrives in ED, placed in routine bed		HIS crashes
- 30 minutes		Initial orders written and given orally to nurses	ADU drug order interlock disable procedure started
- 20 minutes	Gradual deterioration in respiratory status		ADUs begin to appear off-line. ADU non-functional in resuscitation area

Time 0	Placed in resuscitation for severe respiratory distress		(ADU non-functional)
+ 3 minutes		Emergency drug orders given verbally	(ADU non-functional)
+ 6 minutes		Nurse finds ADU non-functional in resuscitation area	(ADU non-functional)
+ 8 minutes		Clerk notifies pharmacy of emergency need for drugs, non-functioning ADU	(ADU non-functional)
		Additional nurses try other nearby ADUs	
		Additional nurses attempt to locate drugs from "likely sites"	
+ 12 minutes		Physicians realize drugs will be delayed, open crash cart and prepare for emergency intubation if needed	(ADU non-functional)
+ 13 minutes		Pharmacist arrives in ED, investigates ADU, arranges for runners to bring drugs in response to telephone	(ADU non-functional)
+15 minutes		Albuterol found in another ED treatment area, given to patient	(ADU non-functional)
+ 17 minutes		Runner system established and functioning	(ADU non-functional)
+ 20 minutes		Pharmacy operator arrives to investigate ADU problem	(ADU non-functional)
+ 30 minutes	All medications received, respiratory status begins to		(ADU non-functional)

	improve		
+ 45 minutes			ADU rebooted successfully, begins to function
+ 2 hours	Transferred to intensive care unit		
+ 4 hours	Intubated for respiratory failure		
+ 8 days	Discharged to home without sequelae		

Legend for Table.

The time course of patient events, staff actions, and system event is outlined here. Times are approximate as they were not always documented and were estimated by participants during debriefing. Time zero was assigned to the point at which severe respiratory distress requiring resuscitation was recognized; negative (-) times refer to events prior to this point and positive (+) to events afterward.