Automation, Interaction, Complexity, and Failure: A Case Study

Robert L Wears, MD, MS
Dept. of Emergency Medicine, University of Florida, Jacksonville, Florida, USA
and
Clinical Safety Research Unit, Imperial College, London W2 1NY
wears@ufl.edu

Richard I Cook, MD
Cognitive Technologies Laboratory, University of Chicago, Chicago, Illinois, USA
ri_cook@uchicago.edu

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 complexity of the health care workplace creates vulnerabilities and problems for system designers. In particular, some forms of failure emerge from the interactions of independently designed and implemented components. We present a case study of such an emergent, unforeseen failure and use it to illustrate some of the problems facing designers of applications in health care.

Keywords: health care, accidents, emergent properties, interactive complexity

Introduction

Efforts to improve patient safety often focus on automation (Leapfrog Group 1999) 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 (Cook and Woods 1996).

A difficult problem with the design of automation is the unanticipated interaction of multiple different automation systems. This paper discusses an archetypal case involving the failure of an automated drug-dispensing unit in an emergency department due to such an interaction, its local consequences and some of the implications for proposals to use automation to advance patient safety (Perry, Wears *et al* 2005). Our purpose is not to present a comprehensive analysis of this specific system, but to use this case to illustrate more general issues common in the introduction of advanced technology into the complex work environment of health care.

Case Description

A critically ill patient presented to a busy emergency department (ED) serving a large urban, indigent population. Intravenous access was obtained and a variety of pharmacologic agents 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 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 the sought after drugs. 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; she survived and was later discharged from the hospital.

Reconstruction of 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. (The sequence is summarized in schematic form in Table 1). 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 monitoring the system 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 occurred on the internet (CERT Coordination Center 2001); 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

Many factors contributed to this near miss, at multiple levels. While the complexity of the work environment is high, and the design issues involved in anticipating what systems might interact and especially how they might be affected by transient failures are difficult, there are many additional dimensions that are important to consider in the larger picture of designing for resilience in complex worlds.

Organisational issues: The organisation conducted minimal planning for potential failure. No formal risk assessment was undertaken, and what planning occurred, occurred because of objections raised from relatively marginalized groups within the organization. It was acknowledged that a mechanical failure might prevent the ADU from dispensing drugs, but that eventuality was minimized because most drug administration is not highly time critical, and because a separate system, the "crash cart" was already in

existence. The crash cart system is a manual chest, mounted on wheels, that contains drugs necessary for the management of cardiac arrest. It did not occur to the planners that cases such as this one – not (yet) in cardiac arrest, but with highly time critical need for drugs – might occur. No scenario-based planning was done, which might have generated example cases that could have led to anticipatory changes in the crash cart (for example, stocking additional drugs that might *forestall* cardiac arrest). The organisation at this time was in a severe financial crisis, and the organisational leadership seemed blinded by the potential for savings represented by the ADU system. Objections on safety grounds tended to come from nurses or emergency physicians, who were not part of the formal planning team, and were tagged as obstructionist, non-team players, so their objections were treated as theoretical at best and specious or manipulative at worst.

The organisational response to the event is telling. Parts of the organisation believed the incident showed that the system was safe, since the nursing and pharmacy staff were able to overcome the problem and since no harm resulted. Nurses, on the other hand, began hoarding drugs as they did not trust the system, thus subverting one of its major organisational goals (inventory control). These disjoint views led to repeated conflict in the organization as more and more drugs and supplies in other locations were moved into similar controlled dispensing devices, often with little communication prior to changes.

Emergent phenomenon: The crux of this incident was the unanticipated interaction of two nominally separate computer systems. The HIS – ADU system was intentionally limited to certain parts of the hospital, but "spilled over" to involve ADUs in the ED, which never were part of the HIS – ADU axis. This, and the co-residence of all these systems on a common Ethernet backbone, was a source on inapparent coupling. By virtue of increased "coupling" between components of the system, automation generates opportunities for a complex systems failure, a "normal accident" (Cook and Woods 1994; Perrow 1999). The incident emerged from the interaction of major and minor faults which were individually insufficient to have produced this incident. The design problem here is that validation of individual device design is an insufficient basis from which to conclude that use in context will attain the design performance levels.

Properties of the health care sector: The case illustrates several aspects of the health care industry that make it peculiarly vulnerable at this stage in its history. First, the application of complex computer technology to certain aspects of technical work in health care is relatively new. Until recently, the majority of technological applications in healthcare were in the form of embedded systems that were highly task specific (*eg*, infusion pumps, or imaging devices). This has shifted in recent years, from systems that are narrowly focused on a specific (typically clinical) task, to systems that are more broadly aimed at solving organizational problems, such as billing, inventory control, accounting, *etc*, and are only secondarily (if at all) directed at supporting clinical work. The relative youth of the field means there is a relatively meagre infrastructure (people, procedures, resources) available for assessing the impact of technological change.

Second, these new types of systems, such as the one discussed here, are highly conflicted, because they advance organizational goals but impress an already beleaguered group of workers into servicing them, without providing the workers a commensurate benefit. Grudin's Law (Grudin 1994) still applies, although the managers and purchasers of such systems do not seem to be aware of it.

Third, health care has been historically a relatively insular, isolating field. There is a broad, general lack of awareness of large bodies of knowledge in design and engineering that might usefully be applied to health care problems. Thus, even if thoughtful managers in health care organizations wonder about the potential adverse effects of a new technology, they are generally unaware that methods and expertise are available upon which they might call; instead, they would more likely convene a group of their own workers, who might be well-intended but not well-versed in technology or risk assessment.

Fourth, health care organizations, at least in the US, are in a sense, barely organizations at all, but rather tense social webs of sometimes competing, sometimes cooperating groups, whose governance seems best modelled by the feudal system (Lorenzi, Riley *et al* 1997; Wears 2001). The relations among physicians, nurses, pharmacists, technicians, and administrators are complex and tense (Nemeth, Cook *et al* 2004).

Because information about risk in such a setting might easily be subverted to advance a group agenda, it is frequently not sought, suppressed, or "interpreted in light of the source."

Finally, there is little or no formal, regulatory pressure to encourage the prior or ongoing evaluation of these systems. While the US Food and Drug Administration does evaluate medical devices, their definition of a medical device is purposely narrow, and would not include systems such as the ADU devices illustrated here. In addition, the FDA would not be well-positioned to evaluate a device such as an ADU in its environment; thus emergent vulnerabilities would likely be missed, even if such evaluations were mandated.

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. Emergent vulnerabilities, such as arise from the interaction among disparate, independently designed components, seem almost impossible to foresee in anything other than the most general terms. Health care seems especially vulnerable to these sorts of threats for several reasons: 1) The relative youth of complex computer application is the field; 2) The general unfamiliarity of health professionals and managers with methods for reducing vulnerabilities; 3) The fragmentary nature of health care "organizations"; 4) The potential subversion of risk information into internal, conflicting agendas; and 5) And a lack of formal or regulatory frameworks promoting the assessment of many types of new technologies. These factors are as much social-organizational as they are technological. As we consider increased automation in health care, we should pay as much attention to anticipating new vulnerabilities and the social component of the sociotechnical system, and to introducing well-established design and engineering risk assessment methods into the field as we do to the anticipated benefits (Nemeth, O'Connor *et al* 2004).

References

CERT Coordination Center. (2001). "Denial of Service Attacks." Retrieved 12 December 2001, 2001, from http://www.cert.org/tech_tips/denial_of_service.html.

Cook, R. I. and D. D. Woods (1994). Operating at the sharp end: the complexity of human error. Human Error in Medicine. M. S. Bogner. Hillsdale, NJ, Lawrence Erlbaum Associates**:** 255-310.

Cook, R. I. and D. D. Woods (1996). "Adapting to new technology in the operating room." Hum Factors **38**(4): 593-613.

Grudin, J. (1994). "Computer-supported cooperative work: history and focus." IEEE Computer **27**(5): 19 - 27.

Leapfrog Group. (1999). "Leapfrog initiatives to drive great leaps in patient safety." Retrieved 17 October 2000, from http://www.leapfroggroup.org/safety1.htm.

Lorenzi, N. M., R. T. Riley, *et al* (1997). "Antecedents of the people and organizational aspects of medical informatics: review of the literature." J Am Med Inform Assoc **4**(2): 79-93.

Nemeth, C., M. O'Connor, *et al* (2004). "Crafting information technology solutions, not experiments, for the emergency department." Academic Emergency Medicine **11**(11): 1114-1117.

Nemeth, C. P., R. I. Cook, *et al* (2004). "The messy details: insights from the study of technical work in health care." IEEE Transactions on Systems, Man, and Cybernetics: Part A **34**(6): 689 - 692.

Perrow, C. (1999). Normal Accidents: Living With High-Risk Technologies. Princeton, NJ, Princeton University Press.

Perry, S. J., R. L. Wears, *et al* (2005). "The role of automation in complex system failures." Journal of Patient Safety **xxxx (in press)**.

Wears, R. L. (2001). Oral remarks as symposium discussant: Challeges to building safe healthcare organizations: from the inside looking out. Washington, DC, Academy of Management.

Table 1. Time Sequence of Events

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.

Approximate Time	Patient Events	Clinical Staff Actions	Automation Events
- 1 month	Sustains cardiac arrest and successful resuscitation in ED		
- 2 weeks			HIS software upgrade begins
- 11 days			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)

Approximate Time	Patient Events	Clinical Staff Actions	Automation Events
+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 improve		(ADU non-functional)
+ 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		