Technical English

For Information and Communication Engineering

2011/9/11

Unit Eighteen

Human Error and Computer System Design

概述

- 人为错误和系统故障
- 系统设计中，人的因素和人机关系
- 如何消除人为因素对系统问题的不利影响
- 计算机工业如何吸取其他工业的成功经验

Mars	火星
malignant - benign	恶性的 – 良性的
tumble	摔跤
deviant	不正常的
corrupt	使腐烂，腐败的
err	犯错误
plausible	貌似合理的
attest	表明，作证
incompetence	无能
dour	阴沉的，严厉的
ACM: Association for Computing Machinery	（美国）计算机协会
inadvertently	漫不经心地，非故意地
scapegoat	替罪羊
sparse	稀疏，稀少

authoritative	权威性的
discipline	学科
administer	管理
moderate	主持（会议等）
anonymity	匿名
regulatory	调整的，控制的
cockpit	驾驶舱
sanitize	消毒，使无害
impartial	公正的，不偏不倚的
statute	法令，成文法律
culpability	有过失，有罪
litigious	好诉讼的，好争论的
initiative	主动的行动
elevate	提升

In 1988, the Soviet Union’s Phobos 1 satellite was lost on its way to Mars. Why? According to *Science* magazine, “not long after the launch, a ground controller omitted a single letter in a series of digital commands sent to the spacecraft.

地面控制中心在发往飞船的一系列数字指令中略去了一个字母

使代码被误译，从而触发了测试序列

And by malignant bad luck, that omission caused the code to be mistranslated in such a way as to trigger the test sequence" (the test sequence was stored in ROM, but was intended to be used only during checkout of the spacecraft while on the ground). Phobos went into a tumble from which it never recovered.

福波斯折载沉沙，就此无法恢复。

What a strange report. “Malignant bad luck”? Why bad luck: why not bad design? Wasn’t the problem the design of the command language that allowed such a simple deviant event to have such serious consequences?

难道不是是命令语言设计的问题使这样一起异常事件导致了如此严重的后果?

The effects of electrical noise on signal detectability, identification, and reliability are well known. Designers are expected to use error-detecting and correcting codes. Suppose interference from known sources of electromagnetic noise had corrupted the signal to Phobos. We would not blame the ground controllers: we would say that the system designers did not follow standard engineering practice, and we would reconsider the design of the system so as to protect against this problem in the future.

系统的设计者没有遵从标准的工程惯例

People err. That is a fact of life. People are not precision machinery designed for accuracy. In fact, we humans are a different kind of device entirely. Creativity, adaptability, and flexibility are our strengths. Continual alertness and precision in action or memory are our weaknesses. We are amazingly error tolerant, even when physically damaged.

我们容忍错误的能力是惊人的，甚至在有物理损伤也如此。

We are extremely flexible, robust, and creative, superb at finding explanations and meanings from partial and noisy evidence. The same properties that lead to such robustness and creativity also produce errors. The natural tendency to interpret partial information — although often our prime virtue — can cause operators to misinterpret system behavior in such a plausible way that the misinterpretation can be difficult to discover.[1]

解释不完整信息的本能虽然是我们的基本优势，却可以使一名操作者以这样一种貌似有理的方式误解系统的行为，从而使这种误解难以被发觉。

人类所犯的好几类错误已经得到确认和研究，可以事先确定，在什么情况下发生错误的可能性会增加。

Quite a lot is known about human performance and the way it applies to system interaction. Several classes of human error have been identified and studied, and conditions that increase the likelihood of error can be specified in advance.[2] Communication systems can be designed to be error-tolerant and error-detecting or correcting. In a similar way, we could devise a science of error-tolerant, error-detecting or minimizing interactions with human operators.

类似地，我们可以发明一种容错、检错或使人机交互降至最小的科学。

Many advances have been made in our understanding of the hardware and software of information processing systems, but one major gap remains: the inclusion of the human operator into the system analysis. The behavior of an information processing system is not a product of the design specifications: it is a product of the interaction between the human and the system.

一个信息处理系统的行为并不（只）是设计指标的产物，而是人和系统交互作用的产物。

The designer must consider the properties of all the system components — including the humans — as well as their interactions. The various technical publications of the field attest to a concern with software and hardware, but emphasis on human functionality and capability is lacking. Many failures of information systems are attributed to human error rather than to the design. We are going to suffer continued failures until we learn to change our approach.

这一领域的各种技术出版物表明了对软件和硬件的关注，可是缺乏对人类功能和能力的强调。

我们称之为人为错误的行为和系统噪声一样地可预测，也许更甚。

One of the first things needed is a change in attitude. The behavior we call human error is just as predictable as system noise, perhaps more so: therefore, instead of blaming the human who happens to be involved, it would be better to try to identify the system characteristics that led to the incident and then to modify the design, either to eliminate the situation or at least to minimize the impact for future events.[3]

试图找出导致事故的系统特性，然后修改设计以消除相应危险，或者至少将它对未来事件的影响减至最小

One major step would be to remove the term “human error” from our vocabulary and to re-evaluate the need to blame individuals. A second major step would be to develop design specifications that consider the functionality of the human with the same degree of care that has been given to the rest of the system.[4]

将人的作用考虑在内，并赋予它和系统其他部分相同的重视程度

好像是控制人员的无能造成了事故

In the case of the Soviet Mars probe, the American journal *Science* wrote its report as if the incompetence of the human controller had caused the problem. *Science* interviewed Roald Kremnev, director of the Soviet Union’s spacecraft manufacturing plant. Here is how *Science* reported the discussion:

“What happened to the controller who made the error? Well, Kremnev told *Science* with a dour expression that he did not go to jail or to Siberia. In fact, it was he who eventually tracked down the error in the code. Nonetheless, said Kremnev, he was not able to participate in the later operation of Phobos”.

正是他最终找到了程序中的错误

prone to … 易于…，有…倾向的

He is prone to anger. 他容易发怒。

Both the reporter's question and the answer presuppose the notion of blame. Even though the operator tracked down the error, he was still punished (but at least not exiled). But what about the designers of the language and software or the methods they use? Not mentioned. The problem with this attitude is that it prevents us from learning from the incident, and allows the error-prone situation to remain.

它使我们不能从事故中学到什么，使错误潜伏的情况依旧

Stories of related failures of computer systems due to “human error” are easy to find in every industry: nuclear power, aviation, business, the stock market, and, of course, the computer industry itself. In the August, 1989 issue of the *Communications of the ACM*, the following item appeared in the section News Track:

Communications of the Association of Computing Machinery

漫不经心地销毁了数以千计文件的电脑拷贝，这些文件中包含与阿拉斯加石油溢出有关的重要信息

“A computer operator at Exxon’s Houston headquarters has been fired for inadvertently destroying computer copies of thousands of documents with potentially important information relating to the Alaskan oil spill. The ex-employee, however, says he is being used as a scapegoat and that none of the tapes he erased were labeled *Do Not Destroy* ”.

在他删除的磁带中没有任何一盘标明为“不得销毁”

The information provided about this incident is too sparse to form a conclusion, but if the system had been designed with the characteristics of human operators in mind, the preservation of tapes would not depend upon the existence of a simple (human-generated?) label “do not destroy.”[5]

如果系统设计中将人的因素考虑了进去，那么磁带的保留就不会仅仅依赖于一条“不得销毁”的（人为）标签了

Thus, either the incident would not have happened, or the excuse would not have been plausible. Perhaps it is time for the ACM to take the lead in this matter for the design of computational systems. There is considerable expertise among its members, including the Committee on Computers and Public Policy and one special interest group devoted to related issues (SIGCHI, the Special Interest Group on Computer-Human Interaction).

也许现在是ACM在这一方面带头在计算机系统设计方面采取措施的时候了。

Peter Neumann主持着一个很有意义的论坛，即关于计算机和相关系统中公众所面临风险的论坛，作为ACM计算机和公众政策委员会的一项活动。

There is also a convenient place to start. On the electronic computer networks, Peter Neumann moderates the valuable Forum on risks to the public in computers and related systems, labeled as an activity of the ACM Committee on Computers and Public Policy. This RISKS forum collects, reports, and comments on incidents that include human error and design, but these are not sufficiently precise or authoritative to be used for professional advancement of the field.

这一“风险”论坛收集、报告、评论各种包括人为错误和设计问题的事故

The sources of the information are often reports in the media, reports that are incomplete, usually written before all relevant information is gathered, and subject to other sources of inaccuracies and biases.[6] (The items from *Science* and the *CACM*'s News Track that I cited exhibit all these sources of unreliability.)

… 传媒的报告，而这些报告是不完整的，通常是在全部有关信息收集齐全之前写就的，并受到其他不准确的和有偏向的消息来源的影响

There is a lot of potential benefit to be gained through the careful study of design failures: other disciplines have learned to benefit through such careful review and analysis. In reviewing the cases presented in the RISKS forum, why not use them as guides to better design?

其他学科领域学会了通过仔细检讨和分析而受益

航空界一个有价值的主要咨询信息源是称为航空安全报告系统（ASRS）的事故汇集（信息库），这是由美国宇航局Ames研究中心（NASA-Ames）运作的，带有Battelle公司管理的计算机可读取的数据库。

There are several existing systems used in other industries that could provide a model. One major source of valuable advice in the aviation community is a collection of incidents known as ASRS, the Aviation Safety Reporting System, run by NASA-Ames, with a computer-readable database administered by Battelle.

Batelle is a global science and technology enterprise headquartered in Columbus that develops and commercializes technology and manages laboratories for customers.

见证或发生错误或其他有关问题的航空界人员

Here, people in the aviation community who witness or commit errors or other related problems write a description of the incident and their interpretation and mail them to ASRS. The ASRS investigators may call back to check on accuracy or get more information, but once the information has been confirmed and clarified, the part of the form that contains the submitter’s identification is returned to that individual.

表格中包含提供信息人员身份的有关部分就被返回本人

保证数据库准确性和完整性的关键

ASRS also removes all identifying information to make it impossible for the particular submitter or incident to be determined. This anonymity is critical to the accuracy and completeness of the database. Because NASA has no regulatory power and has a good record for keeping the sources confidential, this database has become trusted by the aviation community.

People are now willing to describe their own actions if they believe the report will be useful for the improvement of aviation safety. Many improvements in cockpit and other parts of aircraft design have been made by designers who have studied the patterns of errors that can be seen in this database.

A critical aspect of the ASRS system is that the reports are not seen by any supervisors of the submitters. Similar attempts in other industries have failed because their reports were submitted through a chain of authority that included the person's supervisor or plant management — people who have biases to sanitize the report or to form negative judgements of the reporter.[7]

他们的报告是通过一系列的权威机关提交的，其中包括有关人员的上司或工厂管理层，他们是有偏向的，或者对报告进行处理以减轻责任，或者做出对报告的否定判断

Thus, the incident reporting system for the nuclear industry is not an impartial guide to actual operating practices. Anonymity and self-report have worked well, along with a system of verification and clarification such as is performed by the NASA ASRS team (mostly composed of retired aviation professionals).

连同确认和澄清体系一起，匿名制度和自行报告制度起到了它的作用，正如美国宇航局的ASRS团队所做的那样。

In similar fashion, the United States National Transportation Safety Board (NTSB) performs a detailed analysis of transportation accidents (aviation, highway, marine, railroad, and pipeline). These reports are extremely valuable and are a major force in the improvement of safety in the relevant industries.

对交通事故的详细分析

根据法令，NTSB报告不得用于确定事故责任的司法程序。

(The NTSB reports are, by statute, not allowed to be used in legal proceedings to determine culpability for an event. This kind of protection is essential in today’s litigious society to allow the investigation to proceed without fear that the results will be misinterpreted or misused.)

在当前这种动不动就诉诸法律的社会中

Should the ACM sponsor similar initiatives? I don’t know, for its issues are different from those faced by other industries. But I propose that the ACM investigate the possible ways of improving this part of the profession. The ACM could take the lead in establishing some positive, constructive actions to elevate the human side of computing to a level of concern and respectability equal to that of the physical and symbolic side.[8]

ACM可以采取某种积极的，建设性的行动，提升计算机系统中对人的作用的重视，使之与硬件和软件所引起关注和重视具有等同的水平。

结合课文的思考题

- How do human errors cause system failure?
- What can we do to avoid problems due to human errors in important projects such as space mission?
- What is the practice in aviation industry in learning lessens of major accidents?
- Can the computer industry learn something from other industries?

Exercises

- **Theoretically a transmitter should only transmit electric signals and a receiver should only receive signals. Yet this hardly ever happens in the ordinary laboratory because a piece of electronic equipment can either transmit or receive electric energy.**
- 理论上发射机应该只发射电信号，而接收机只接收信号。可是在普通的实验室中几乎从来不是这样，因为任何电子设备总是既能发出电能，又能接收电能。

Exercises

- **Consequently, electronic equipment is constantly subjected to unwanted signals, and is constantly producing energy that adjacent equipment is not designed to accept. This is the basic problem of electromagnetic compatibility. The electronic equipment must operate in conjunction with other equipment without causing malfunction or degradation of operation of any of the associated equipment.**
- 因此，电子设备总是受到不希望有的信号影响，同时又总是产生一些附近设备不能接受的能量。这就是电磁兼容的主要问题。电子设备必须与其他设备协同工作，而不会使任何相关设备工作失常或性能下降。

Exercises

- **An ideally designed piece of equipment should not radiate any unwanted energy; nor should it be susceptible to any unwanted energy. To accomplish this, a medium would have to enclose the equipment so that unwanted energy either leaving or attempting to enter the equipment is effectively attenuated.**
- 一台设计得好的设备不应该辐射任何不希望有的能量，也不应该受到任何不该有的能量的影响。为了实现这一目标，必须有一个媒介将设备包围起来，使得离开或进入该设备的不想要的能量被有效地衰减。

Exercises

- **The term (coding) in the digital context can refer to several processes. For example, we may think in terms of making the message unintelligible to unauthorized users, or alternatively, the conversion of a simple binary signal to another digital form more suitable for transmission.**
- 在数字意义上这一术语可以指好几种过程。例如我们可以把它看作使信息不能被未经授权的用户所理解，或者是将一个简单的二进制信号转换为另一种更适合于传输的形式。

Exercises

- **Here we shall consider only the simple coding structures and mechanisms that are required to represent a particular analog value digitally. There are many different types of coding mechanisms, and to simplify our analysis it is useful to classify them.**
- 这里我们将只考虑用数字形式表示一个特定模拟值的简单编码结构和机制。有许多不同类型的编码机制，为了简化我们的分析，将它们分类是有益的。

Exercises

- **Since the step size is constant throughout the permitted amplitude range, the signal is said to be uniformly quantized.**

  A. designated [✓ B. allowed] C. permanent D. assigned

- **The amplitudes of the harmonics of the message signal are virtually unattenuated at the high frequency.**

  A. nearly B. normally [✓ C. factually] D. slightly

Exercises

- There is a one-to-one correspondence between every instruction in an assembly language program and its equivalent machine language program.

  A. similarity B. correlation C. efficiency D. identification

- The results of this analysis were then compared with the specification, and an error was usually indicated between them.

  A. requirement B. special aspect

  C. implication D. simplification

Exercises

- The second section describes quantization schemes that take account of the characteristics of speech.

  A. techniques B. systems C. mechanisms D. principles

- The approach differs from classical synthesis and design in that no formal design technique other than network analysis is required.

  A. strategy B. road C. scheme D. idea

Exercises

- The system capacity, or rate of information transmission through a communication system, is related to the rapidity with which signals may change with time.

  A. complexity B. rate C. clarity D. quickness

- The system impairments, other than quantization error, that may occur in practical equipment are then discussed.

  A. rather than B. besides C. as well as D. except

Exercises

- They are like the jumper manufacturer who discovers that it is more economical to mould jumpers, in one operation, from a wonderful new plastic, which looks and feels just like wool.

  A. take jumpers into shape B. give a shape to jumpers

  C. shape jumpers by using a mould D. model jumpers

- The third section describes quantization schemes that take account of the characteristics of speech.

  A. consider B. make use of C. count D. compute