1

WHAT IS RELIABILITY?

1.1 RELIABILITY AS A PROPERTY OF TECHNICAL OBJECTS

Reliability of a technical object is its ability to perform required operations successfully. Usually, it is assumed that an object is used in accordance with its technical requirements and is supported by appropriate maintenance.

One of the outstanding Russian specialists in cybernetics, academician Axel Berg, has said: "Reliability is quality expanded in time."

Reliability is a broad concept. Of course, its main characterization is the failure-free operation while performing required tasks. However, it also includes such features as availability, longevity, recoverability, safety, survivability, and other important properties of technical objects.

Speaking of reliability, one has to introduce a concept of failure. What does it mean—"successful operation?" Where is the limit of "successfulness?"

Probabilistic Reliability Models, First Edition. Igor Ushakov.

In reliability theory, usually one analyzes systems consisting of units, each of which has two states: operational and failure. If some "critical" set of units has failed, it leads to system failure. However, a unit's failure does not always lead to "total" system failure; it can decrease its ability, but main system parameters still could be in appropriate limits.

However, such "instantaneous" failure is only one of the possibilities. The system can fail due to monotonous drifting of some parameters that can bring the entire system to the unacceptable level of performance.

In both cases, one needs to formulate failure criteria.

1.2 OTHER "ILITIES"

Reliability itself is not the final target of engineering design. An object can be almost absolutely reliable under "greenhouse conditions"; however, at the same time, it can be too sensitive to real environment. Another situation: an object is sufficiently reliable but during operation it produces unacceptable pollution that contaminates natural environment.

Below we discuss some properties closely connected to the concept of reliability.

- *Maintainability.* Failure-free operation is undoubtedly a very important property. However, assume that a satisfactorily reliable object needs long and expensive restoration after a failure. In other words, maintainability is another important property of recoverable systems. Maintainability, in turn, depends on multiple factors.

  The quality of restoration of an object after failure as well as time spent on restoration significantly depends on repairmen qualification, availability of necessary tools and materials, and so on.
- *Safety.* Development of large-scale industrial objects attracts attention to safety problem. It is clear that not only an object has

to perform its main operating functions, but it is also very important that the "successful operation" is not dangerous for personnel's health and does not harm ecology.

One of the most tragic events of this kind occurred in 1984. It was the Bhopal Gas Tragedy—one of the world's worst industrial catastrophes. It occurred at the Union Carbide India Limited pesticide plant in India. The catastrophe led to almost immediate death of about 7000 people and about 8000 died from gas-related diseases. In addition, over half a million people got serious injuries.

Then, in 1986 explosion and fire occurred at the Chernobyl Nuclear Power Plant in the former Soviet Union. Large quantities of radioactive contamination were released into the atmosphere, which spread over much of Western USSR and Europe. It is considered the worst nuclear power plant accident in history. Thousands of workers were killed almost instantaneously, and about 1 million cancer deaths occurred between 1986 and 2004 as a result of radioactive contamination.

Actually, problem of safety appears not only in the context of failures. A number of "reliable" industrial plants are extremely unsafe for the people who work there or live in the area (Figure 1.1).

- *Survivability.* The problem of survivability is very close to the reliability and safety problems. This is an object's property to survive under extreme natural impacts or intentional hostile actions.

In this case, nobody knows the moment of disaster, so an object has to have some "warranty level" of safety factor. In our time, the survivability problem is extremely important for large-scale terrestrial energy systems.

The 1999 Southern Brazil blackout was the largest power outage ever. The blackout involved Sao Paulo, Rio de Janeiro, and other large Brazilian cities, affecting about 100 million people.

Then in 2003 there was a widespread power outage known as the Northeast blackout. It was the second most widespread blackout in history that affected 50 million people in Canada and the United States.

FIGURE 1.1 Typical “industrial landscape” with terrible air pollution.

On March 11, 2011, a ferocious tsunami spawned by one of the largest *earthquakes* ever recorded slammed Japan’s eastern coast. This earthquake, officially named the Great East Japan Earthquake, was 9 magnitudes on the Richter scale. Tsunami waves reached up to 40 meters, struck the country, and, in some cases, traveled up to 10 kilometers inland in Japan. States of emergency were declared for five nuclear reactors at two power plants. There were some severe damages, although consequences were much less than those after Chernobyl.

Problem of survivability has become essential in our days when unpredictable by location and strength terrorist acts are initiated by religious fanatics.

- *Stability.* An object performs under unstable conditions: environment can change, some simultaneously performing operations can conflict with each other, some disturbances can occur, and so on. An object has to have an ability to return to normal operational state after such inner or outer influences.
- *Durability.* Reliability as a concept includes such a property as durability. For instance, mechanical systems, having some fractioning parts, can be very reliable during the first several hundred hours; however, after some period of time due to wearing out

processes they fail more and more frequently, and became unacceptable for further use.

- *Conservability.* This is the property of the object to continuously maintain the required operational performance during (and after) the period of storage and transportation. This property is important for objects that are kept as spares or are subjects of long transportation to the location of the use.

1.3 HIERARCHICAL LEVELS OF ANALYZED OBJECTS

Analyzing reliability, it is reasonable to introduce several hierarchical levels of technical objects. Below we will consider systems, subsystems, and units. All these terms are obvious and understandable; nevertheless, we will give some formal definitions for further convenience.

A *unit* is an indivisible ("atomic") object of the lowest hierarchical level in the frame of current reliability analysis.

A *system* is an object of the highest hierarchical level destined for performing required tasks.

Of course, concepts of unit and system are relative: a system in one type of analysis can be a unit in consideration of a large-scale object, and vice versa. In addition, sometimes it is reasonable to introduce an intermediate substance—subsystem. It can be a part of a system that is destined for performing a specific function or a separate constructive part.

System reliability indices can be expressed through corresponding indices of its units and subsystems.

1.4 HOW CAN RELIABILITY BE MEASURED?

Reliability can be and has to be measured. However, what measures should be used for reliability?

Distance can be measured in kilometers and miles, weight in kilograms and pounds, and volume in liters and gallons. What kinds of index or indices are appropriate for reliability?

Of course, reliability index depends on the type of a technical object, its predestination, and regime of operating, as well as on some other factors that are usually rather individual.

Generally speaking, all technical objects can be divided into two main classes: unrecoverable and recoverable. All single-use technical objects are unrecoverable. For instance, anti-aircraft missile is used only once. It can be characterized by the probability that the required operation is completed.

A reconnaissance satellite is also a single-use object. However, for this object the best reliability index is an average time of operating without failure: the more time the satellite is in the orbit, the more useful information will be collected.

Most of technical objects we are dealing with are recoverable ones: they can be restored after a failure and can continue their operations.

Let us consider a passenger jet. It is almost obvious that the most important reliability index is the probability that a jet successfully completes its flight. Of course, one should think about longevity and convenience of technical maintenance, although these indices are undoubtedly secondary.

Let us note that the same object may be considered as recoverable or not depending on the concrete situation. It is clear that for the same passenger jet some critical failure, having been occurred during the flight (for instance, engine failure), cannot be corrected. Thus, in this case a jet should be considered as unrecoverable during a flight.

Anti-missile defense systems work in regime “on duty”; that is, they have to be in an operational state at any arbitrary chosen moment of time. For an airport dispatcher system, it is very important to be in an operational state at some required moment of time and successfully operate during an airplane landing. Thus, for such systems the most important property is availability.

For a passenger bus, probably one of the main reliability characterizations is the duration of failure-free operation because it means that the number of unexpected stops due to failures is minimal. Same reliability index is convenient for trucks: it delivers the best economical efficiency during operations.

For most home appliances, cars, and technical equipments, durability is very important because it saves money of the user. At the same time, one does not need “immortal” personal computer because in 2–3 years it will be anyway obsolete and should be replaced by a modern one. There are several commonsense rules that one should keep in mind while choosing reliability indices:

1. They have to reflect specificity of the object and its operating process.
2. They have to be simple enough and should have an understandable physical sense.
3. They have to be calculable analytically or numerically.
4. They have to be empirically confirmed by special tests or during real exploitation.

The number of indices chosen for characterization of reliability of a technical object should be as limited as possible, since multiple indices can only lead to confusion. Do not use “weighted” indices because they usually have no physical sense.

1.5 SOFTWARE RELIABILITY

Software reliability is a special topic. Frankly speaking, there is too much confusion and misunderstanding.

Nobody doubts that reliability in technical context is a concept associated with time and randomness. If there is an object (especially, immaterial) that exists in sense “beyond the time” and its failure does not occur randomly, how we can talk about reliability?

Take a look: what is software? It is a set of commands arranged in a special order. It reminds of a book “written” for a “hardware reader” that can “read” it when and if needed.

Is it possible to say about “reliability of a book,” keeping in mind its contents? Of course, a book can contain errors (“failures”) but these errors are everlasting property of this specific book! These errors can be deleted in the next edition of the book but they are and they will remain forever in this particular edition.

The same picture we observe with software if some "inner programs conflict" or "inconvenient" set of input data appears again and again, which will lead to repeating failures. And it does not depend on current time, and it is not random at all.

For software, we should say about quality, which depends on programmer's qualification and carefulness of testing. To say about "frequency of software failures" is hardly correct.

1.5.1 Case Study: Avalanche of Software Failures

In 1970s, the author, being an engineer at R&D Institute of the former Soviet Union, participated in the design of an automatic control system for missile defense. Reliability requirements for the system were extremely high.

After design completion, long and scrupulous tests began. Hardware and software were multiply checked and rechecked: the system seemed "absolutely reliable." But all of a sudden, a long series of software failures occurred in a row!

Acceptance Commission was in panic . . .

After careful analysis, it was found that a young lieutenant who was working as an operator mentioned that some sequence of specific commands led to computer fault. He made a corresponding note in a Test Protocol though, being too much curious, continued to try the same commands multiply.

Definitely, recording several tens of faults was unreasonable. Only one fault of software was recorded. Afterward, the software had been corrected . . .

However, there is a question: how you should characterize software reliability? The only fault has been recorded during 50 hours of testing. May you say that the software failure occurs once in 50 hours on average? Moreover, the program had been "repaired." So, does it mean that after this the software became "absolutely reliable"?

Who knows when and how next time such "inconvenient" circumstances may occur in real operating regime?