1

Resilient Systems

1.1 Introduction

One of the most tragic accidents is that of a commercial passenger aircraft crash. Picturing the death of tens of children, women, and men is extremely horrifying and dreadful. Even though commercial passenger aircrafts are constructed with the utmost reliability with very low accident statistics, the occurrence of even one accident is not acceptable. A survey of aircraft crashes shows that most accidents occur near origin or destination airports. This fact leads to the necessity for a very important capability of the aircrafts: resilience. If the airplane is resilient it can withstand faults until a safe landing point is found. This safe point is usually the nearest airport. Figure 1.1 shows a conceptual diagram about this situation. The good path is for the aircraft with a resilient capability as this aircraft is able to protect its passengers. However, a non-resilient aircraft flies through the bad path and can lead to a tragedy.

In this example, three concepts are seen:

- A system with a critical mission
- A faulty condition
- Resilient operation of the system

The aircraft here is a mission critical system (with the safety of hundreds of lives) and the resilience capability helps to pass the mission after a faulty condition. It is the key phrase of this book: *Passing the faulty condition without failing in the mission*. This means that the topic of this book is not about reliable systems! The topic is about the reliable systems that have the capability to survive a faulty situation. The above-mentioned aircraft may be very reliable, which means that it has very rare faults, but this does not mean that it is necessarily resilient. A reliable and non-resilient system may not necessarily finish its mission in a faulty condition as even its faults have a low probability of occurrence.

As this chapter deals with resilience in its general form, we continue with an explanation about the definition of systems and their characteristics. To enter the subject of resilience, these concepts are now described.

1.2 Definition of a System

Our world consists of systems. A system is an integrated collection of various parts to meet a goal. The goal of the system usually appears in the output(s) of the system. The systems also accept one or more inputs that provide the required information and energy for the system [1]. The system

Resilient Power Electronic Systems, First Edition. Shahriyar Kaboli, Saeed Peyghami, and Frede Blaabjerg.

Companion website: www.wiley.com/go/kaboli/resilientpower

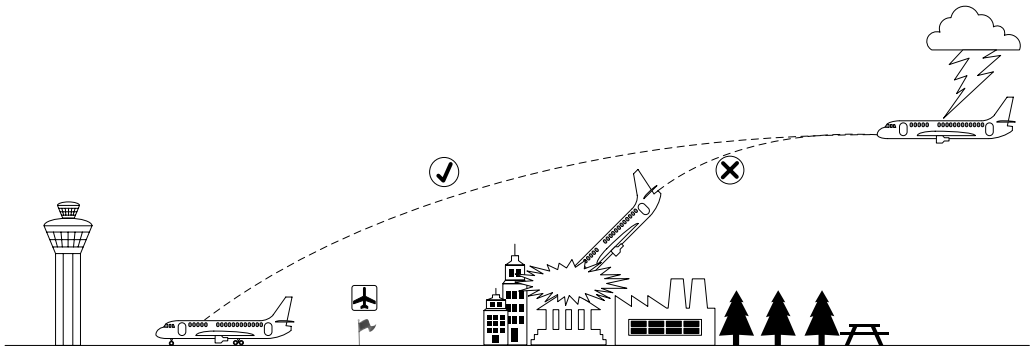

Figure 1.1 A basic diagram about the resilience concept for a mission critical system.

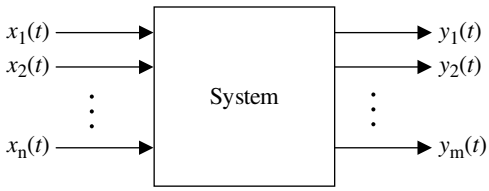

Figure 1.2 A system block diagram with some inputs and outputs.

inputs and outputs determine the system boundaries, as shown in Figure 1.2. In this figure, the shown system has n inputs, i.e. $x_1(t)$ to $x_n(t)$, and m outputs, i.e. $y_1(t)$ to $y_m(t)$. The inputs and outputs may be constant or time variant.

1.2.1 Elements of the System

The systems may be very simple and consist of a few parts. For example, a heater is a simple system consisting of a resistor. The input voltage is dissipated in the resistor and generates an amount of heat as the system output. On the other hand, there are more complex systems with many parts. A complex system may consist of some smaller systems where each acts as a part of the complex system [1]. Figure 1.3 shows a complex system consisting of some smaller systems. Each of these smaller systems may include other smaller systems. For example, a computer is a complex system consisting of several smaller systems: the mother board, memories, hard disk, graphic peripherals, monitor, and power supply. Figure 1.4 shows a Laptop as a system that consists of some smaller systems, such as memory, power supply, etc. Decomposition of a system into the smaller sections (systems) leads to the elements. An element is defined as a part that is not decomposable to smaller sections [1]. For example, in the power supply of a computer, transistors of the voltage regulators are considered as elements. It is obvious that the system decomposition can be continued to much lower layers of the system. A transistor can be considered as a system consisting of layers of semiconductors. Each semiconductor layer can be decomposed to atoms if it is considered as a system. Therefore, an important question is: what is the stop point of this system? The answer comes from another question: what is the required system study level? We can stop this process if the defined elements satisfy the accuracy of the study [1].

1.2.2 System Performance Criteria

The systems are designed based on the required mission profile(s). A high-quality system tries to close its output(s) to the planned mission target as much as possible [2]. System performance

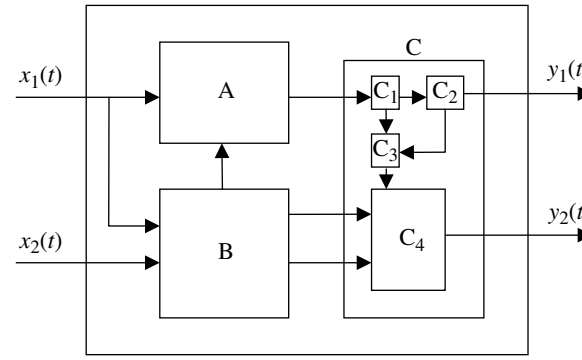

Figure 1.3 A system consists of some subsystems.

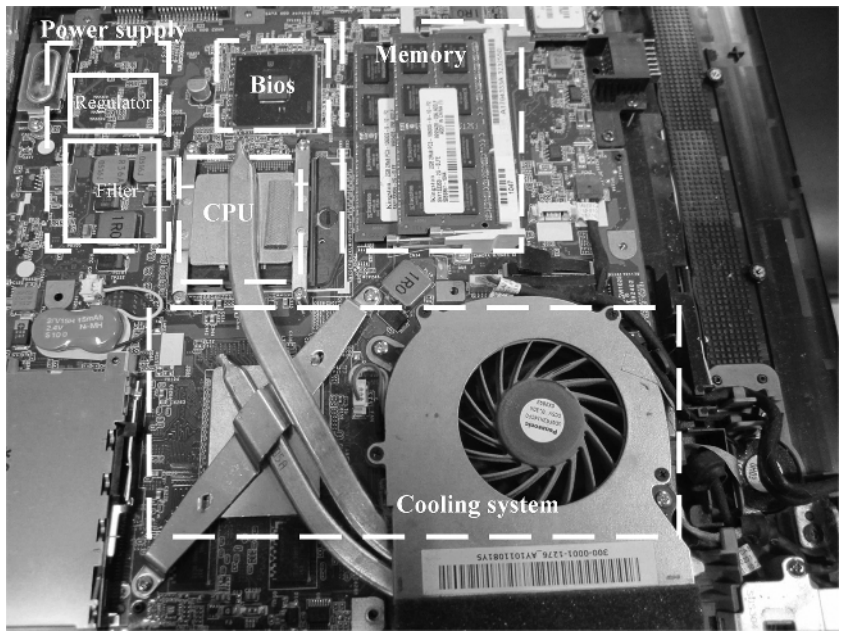

Figure 1.4 Various subsystems in a laptop.

criteria are quantitative indices used to characterize the performance of the system relative to its alternatives [2]. The difference between the pre-defined value of a system performance index and its respective actual value is the system error. A high-quality system keeps its errors close to zero. There are three different categories of system performance indices, as listed in the following:

- The indices about the system output(s)
- The indices about the system input(s)
- The indices about the relation between the system input(s) and output(s)

Figure 1.5 shows two different cars at the same level. Table 1.1 summarizes the performance indices of these cars in order to compare them [3]. The power is the performance index of the cars. The mileage is the index about the relation between the cars' input, the fuel volume, and the cars' output, the passed distance.

(a) (b)

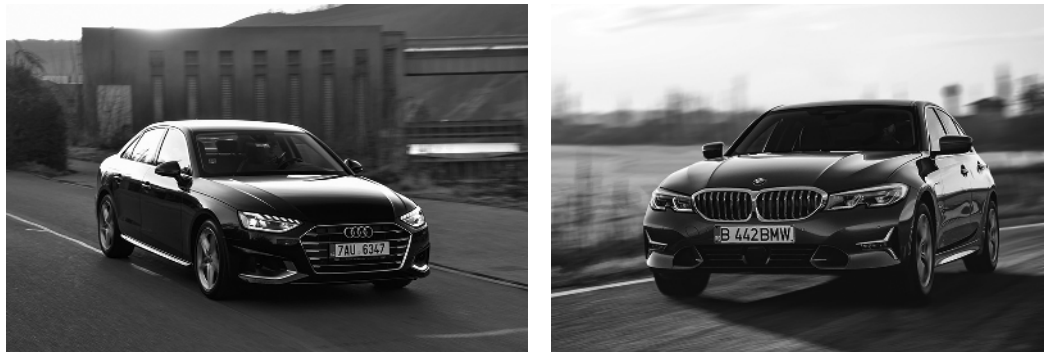

Figure 1.5 Two different cars at the same level. *Sources:* Jan Kliment/Adobe Stock; Gabriel/Adobe Stock.

Table 1.1 A comparison between the characteristics of two cars.

	Audi A4	**BMW 3 Series**
Power (bhp)	188	255
Mileage (km l^{-1})	17.84	16.13
Engine (cc)	1984	1998

1.2.3 System Useful Life and Reliability

The system useful life is an estimate of the time it is likely to remain in service. It is important to have an expectation about the useful life of a system before its construction or even its remaining useful life during its operation [4]. The useful life prediction is a tool for this goal. The useful life can be defined based on the performance degradation of the system. In this definition, the useful life is defined as the time interval to the point where the system performance falls below a threshold, as shown in Figure 1.6. In many cases, the useful life is defined as a probability. The useful life is the probability of performing adequately to achieve the desired aim of the system. There are useful life prediction techniques that depend on the knowledge about design. As more details of the design are known, more accurate methods become available. These methods use part failure rate models, which predict the failure rates of parts based on various part parameters, such as technology, complexity, package type, quality level, and stress levels. Predictive methods attempt to predict the useful life of a part based on some model typically developed through empirical studies and/or testing [5, 6]. An attempt is made to identify critical variables such as materials, application environmental and mechanical stresses, application performance requirements, duty cycles, and manufacturing techniques. Typically, a base failure rate for the component is assigned, which is then multiplied by factors for each critical variable identified. Some predictive models assume a constant failure rate over the lifetime of a product. This ignores higher failure rates typically seen at the beginning and end of the component life, infant mortality, and wear-out, respectively [6]. Predictive methods can provide a relatively accurate reliability estimate in cases where good studies have been done to analyze field failures. Reliability is the probability of performing adequately to achieve the desired aim of the system. This can be mentioned as a time-dependent equation. The reliability concept has more importance in specific applications, such as in space and military

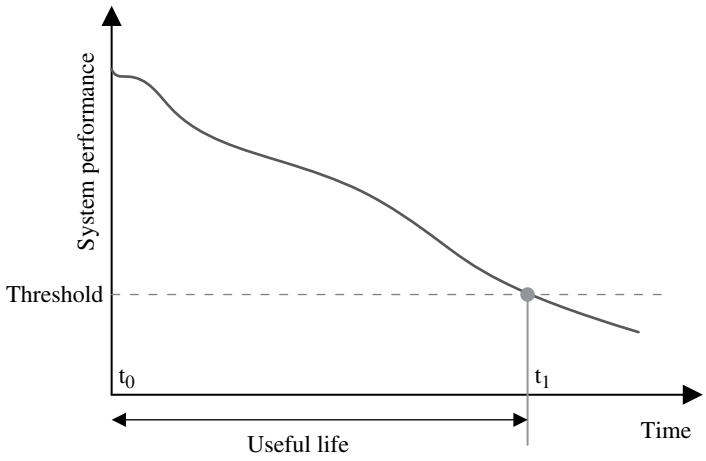

Figure 1.6 Definition of the useful life concept base on the system performance degradation.

equipment, where on a mission equipment can hardly be replaced or be performed by another system instead of the failed part. In order to improve the system reliability, different research has been carried out and several methods have been introduced. Fault occurrence is a relatively random phenomenom. Randomness means a lack of pattern or predictability in events. Therefore, essential methods of reliability prediction are based on probability analysis. In statistics, a random variable is an assignment that has a numerical value for each possible outcome of an event space. This association facilitates the identification and the calculation of probabilities of the events. Random variables can appear in random sequences. A random process is a sequence of random variables describing a process whose outcomes do not follow a deterministic pattern, but follow an evolution described by probability distributions [7]. These and other constructs are extremely useful in probability theory and the various applications of randomness. It is usual for some kinds of merits such as efficiency to be widely accepted by many users. However, reliability is less applicable than these labels.

In order to improve system reliability, different research projects have been done and several methods have been introduced. Many of these methods need information about the failure rate of the system. Each system contains a number of components. One method to enhance reliability is improvement of component reliability. This goal may be achieved by component-specific derating or by improvement of component specifications. At this level, the failure rate of the components should be modeled properly. The other method is to use a redundant or fault-tolerant system in which, after a partial fault, the rest of the system can work adequately to achieve the goal of the whole system. At this level, a systematic analysis of reliability is necessary. For example, a systematic analysis indicates that one problem of using a redundant system is load balancing. The other method that may be useful is a comparison of various possible topologies or different operating conditions to choose a proper state to achieve the goal of design. Because some systems are not available to be repaired or maintained, maintenance can rarely be used in these systems. Also, this method is not meaningful for each system element. For example, only a fan can be maintained to work properly and do its duty for cooling a car engine while for an injector, maintenance does not have a practical meaning. Rather than a theoretical reliability evaluation with standards, there are some accelerated or aging tests that manufacturers use to evaluate the reliability of their products.

In this method, at each test, one or some parameters of environmental conditions are stressed more than a typical state in order to reduce the test time less than the real state. There are some determined relations between these accelerated test results and typical condition results that are used for finding failure rates and reliability evaluations.

1.3 Resilience Concept

In a system, resilience is defined as the capability to recover from an abnormal state to another state where this new state guarantees the continuance of the operation of the system. According to this definition, there are some key points in the resilience concept:

- Normal state
- Abnormal state
- New state

In an ideal condition, the new state is the previous state of the system before failure. However, as shown in Figure 1.1, the new state is defined based on the mission profile of the system. It may be just a safe point in a damaged aircraft. The bomber B-17 shown in Figure 1.7 is a very famous example of this situation. The B-17 Flying Fortress became symbolic in the United States of America's air power and many of them came back to the origin points in a huge damaged state, as shown in Figure 1.8. The *All American* was a World War II Boeing B-17 Flying Fortress bomber aircraft that was able to return safely to its base after having its rear fuselage nearly cut off by an in-flight collision with a German BF-109 over enemy-held territory. The bomber's flight is said to have yielded one of the most famous photographs of World War II, as shown in Figure 1.9 [8].

In the fields of engineering and construction, resilience is the ability to absorb or avoid damage without suffering complete failure and is an objective of design, maintenance, and restoration for buildings and infrastructure, as well as communities. In this regard, resilience has a close meaning to availability. The concept of availability was originally developed for repairable systems that are required to operate continuously and are at any random point in time either operating or down because of failure and are being worked upon so as to restore their operation in a minimum time. Availability means the probability that a system is operational at a given time, i.e. the amount of

Figure 1.7 The famous Bomber B-17. *Source:* Carlo Borella/Unsplash.com.

(a) (b)

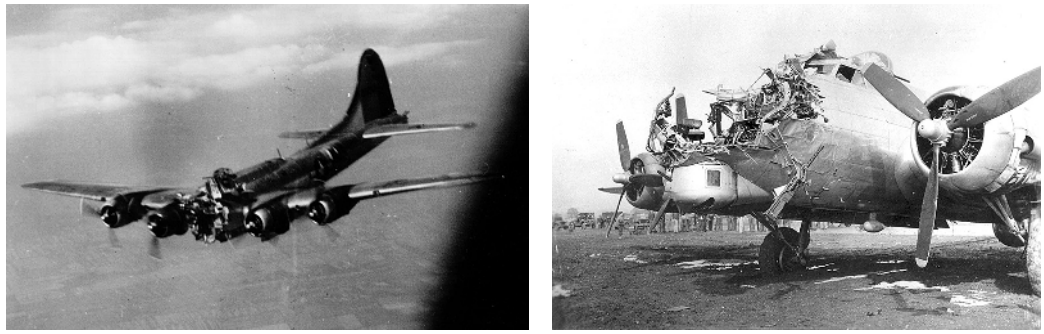

Figure 1.8 Two damaged B-17 bombers that came back to the origin airport, (a) during flying, (b): after landing. *Sources:* Aviation C2017/Alamy Images; US Air Force/Wikipedia Commons/Public Domain.

Figure 1.9 The *All American* Flying Fortress bomber aircraft. *Source:* US Air Force/Wikipedia Commons/Public Domain.

time a device is actually operating as the percentage of total time it should be operating. High-availability systems may report availability in terms of minutes or hours of downtime per year. Availability features allow the system to stay operational even when faults occur. A highly available system would disable the malfunctioning portion and continue operating at a reduced capacity. In contrast, a less capable system might crash and become totally non-operational. Availability is typically given as a percentage of the time a system is expected to be available. Availability of a system is typically measured as a factor of its reliability—as reliability increases, so does availability. A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. In computer networking, resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

Figure 1.10 shows the time diagram of a resilient system. When a fault occurs in a system, the system performance index falls down. Both the resilient system and fault-tolerant systems try to keep the index during the fault and then try to recover the system performance index. The key differences between a resilient system and a fault-tolerant system are the value of the system performance index drop and the time of adaptation and recovery phases. In a mission critical system, the values of this index drop and time interval are very important. For example, in a power supply, the recovery time of the output voltage after a short-circuit fault determines whether the system is resilient or just fault tolerant.

Resilience has two important aspects: (i) system performance and (ii) transition time. Figure 1.10 shows the phases of resilience during a fault. The vertical axis shows the level of resilience, while time describes the transition time as:

- Phase 1: Resilient State
  The resilience begins before the fault. Reducing the impact of the fault helps the system to reduce its quality drop and the transition time.
- Phase 2: Post-event Degraded State
  In this phase, the system performance falls and resilience determines its depth. The system capabilities for resilient operation such as redundancy and reconfiguration reduce the system degradation.
- Phase 3: Restorative State
  In the restorative state, the key factors are fast response and short recovery time.
- Phase 4: Post-restoration State
  After the restorative actions, the system enters into a post-restoration state. It may take a longer time depending on the impact of the fault.

Thus, a resilient system should consider the resilience level and transition time between each phase. The resilience of a system could be improved by reducing the degradation depth and reducing the transition time.

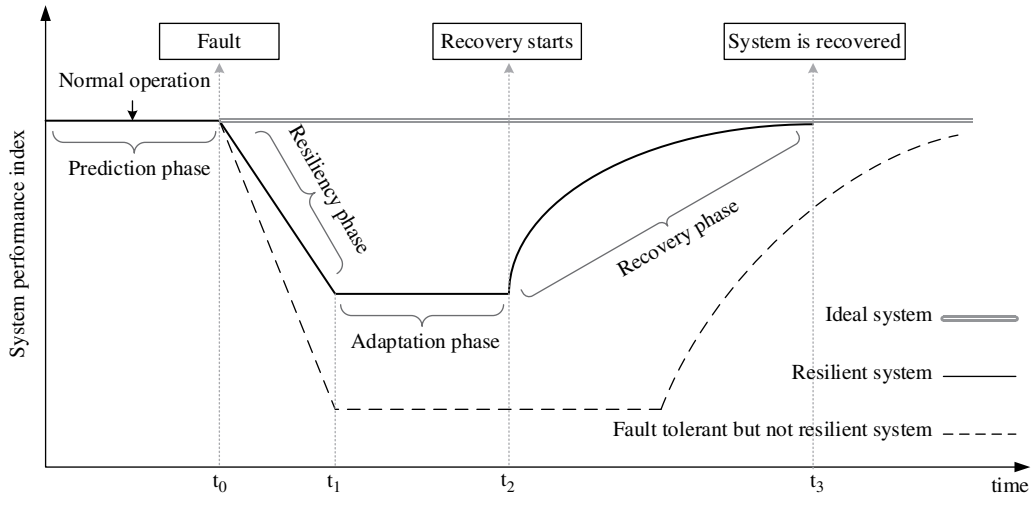

Figure 1.10 Time diagram of a comparison between a resilient system and a fault tolerant system.

Like a fault-tolerant system, there are some solutions for a resilient system. For example, redundancy is a solution. However, redundancy brings a number of penalties: an increase in weight, size, power consumption, cost, as well as time to design, verification, and test. Therefore, a number of choices have to be considered to determine which components should be redundant. These are critical operations of the component, probability of the component failure and its cost.

The focus of some methods in the design stage is on the element's stress reduction in the design process. Reliability of a system increases if it operates at a set point with low stress. It is assumed that the system is under a design process or operates without fault. In the field of power electronics, methods for reducing an electric field are described at both the system and printed circuit board levels. Low temperature operating conditions for an electric power converter are described and tools for this goal are presented. Series connection for voltage sharing and parallel connection for current sharing is explained. Novel control methods of power converters for reducing the complexity and reliable operation are presented. Control of an inrush current as a typical transient problem in electric power converters is presented. Methods for preventing the high stress condition on the components in faulty cases are described. Techniques for reducing mechanical and environmental stress are expressed. Mechanical dampers for preventing high amplitude vibration and insulating colors against humidity are presented.

Another technique for resilience is derating. Within the topic of derating, uninterrupted operation of a faulty system with catastrophic damages in some of its parts is investigated. A faulty system can continue to work with degraded specifications. This technique can be used for both a faulty system because of its uninterrupted operation and a normal system because of its extensive lifetime. Here, the question is: what is the level of derating? If this derating level meets the required performance index of the system, the system is resilient. If not, the system may be fault tolerant but not within the acceptable margins of the system performance indices.

Resilience always has a conflict with the protection system. Protection systems act when a fault occurs in a converter. Their performance is very important; isolation of the converter is not always the best choice because this strategy has a bad effect on the availability of the converter. Protective device coordination is the process of determining the "best fit" timing of interruption when abnormal electrical conditions occur. It is about a solution too close to resilience. The goal is to minimize an outage to the greatest extent possible.

Resilience is a time-dependent factor: the level of resilience during the fault determines the recovery time of the system. In a power electronic converter, resilience can be considered at various levels. In the component level, application of more resilient components leads to resilience of the system. This means that a diode-based rectifier has lower performance indices than a modern synchronous rectifier, but it shows more resilience than the synchronous rectifier.

However, the topic of this book relates to the system performance after the fault occurrence when the protection system acts, when the concept of derating, availability, and fault tolerance are presented, and when the system recovery is important. In stress reduction, we tried to postpone the failure time by reducing the stress on the converter. However, the converter must operate and it is logically affected by stress. It is true that we reduce the stress, but the stress still exists and causes failure in the long term. Suppose that we are faced with a fault in the converter. What should we do? One of the methods for preventing catastrophic damage in faulty converters is to use protection systems. However, the protection system usually causes the system to shut down. The main question is what is the recovery time and the degrading level of the system during the fault? A system can be very reliable but not resilient. Here, reliability means that there are low probability faults in the system and none of them leads to permanent damage. However, these are not

enough reasons for resilience. The time of recovery and the level of system performance degrading are the main factors. Protection techniques prevent catastrophic failures in electric power converters. However, as described previously, protection systems cannot prevent every fault. There are two main approaches to a faulty converter. Isolating the faulty converter is one of the approaches and is used when the converter mission can be interrupted for repair and maintenance. If the mission of the converter is important at the time of failure, users should use another method. Derating is a method for allowing the faulty converter to continue its mission. The derating concept is a commonly used technique for faulty systems. Under this topic, uninterrupted operation of a faulty power conversion system with catastrophic damages in some of its parts is investigated. It is shown that a faulty electric power converter can continue to work with degraded specifications. This algorithm is named "derating for accessibility." This technique can be used for both a faulty system because of its uninterrupted operation and a normal system because of its extensive lifetime. Although the derating technique allows the system to operate after faulty conditions, the system degradation may be as high as the unacceptable performance. On the other hand, the system recovery time is also important, which is not considered in the derating methods.

1.3.1 Mission Profile

In the field of reliability, the mission profile has been one of the key concepts since the start of the scientific examination of the subject of reliability. Mission profiling is the process of creating an overview of all the influences that a product is subjected to throughout its life cycle, which typically comprises transport, storage and use environments [9]. A mission profile takes the following into account: field of application, geographical area, user impact, and use profile. A mission profile contains both environmental impacts, such as thermal, mechanical, humidity, water, dust, chemical, electromagnetic impacts, and functional influences related to the pattern of use. Mission profiles are an important part of the product development process and form the basis of product requirements. Together with acceleration models, mission profiles also form the basis for accelerated life testing and other relevant tests. A mission profile is a simplified representation of relevant conditions that the system in focus will be exposed to in its intended application. In photovoltaic systems, the mission profile can be defined as a dataset of annual power generation, energy estimation, and environmental and graphical results; from these, designers are able to extract the minimum, average, and maximum current, voltage, and temperature values in which the photovoltaic system will operate and build a relevant operation map. Figures 1.11 and 1.12 shows two mission profiles for a human and a solar plant, respectively. A mission profile directly affects the useful life of the system. In the example of a human mission profile, it is accepted that a human without a good sleep program ages faster than one with a good and enough sleep program.

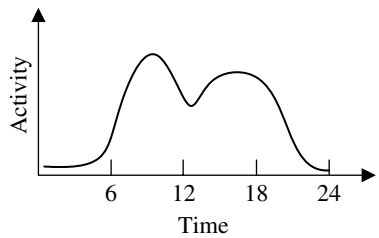

Figure 1.11 Mission profile of a human during one day.

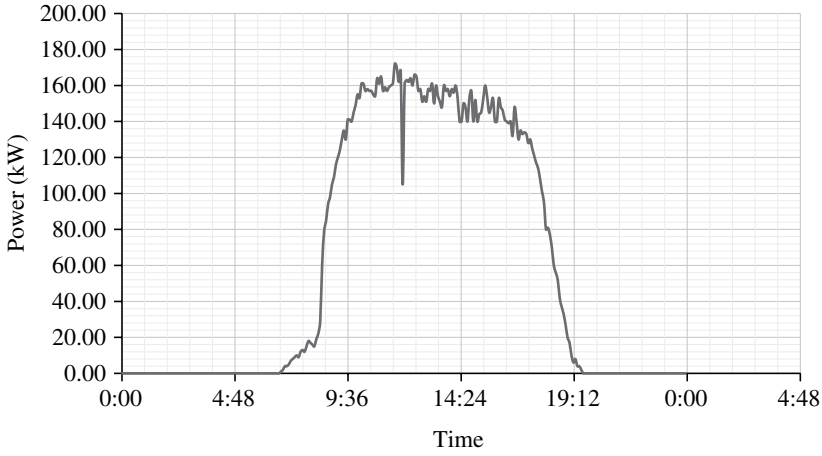

Figure 1.12 Mission profile of a solar plant during one day.

1.3.2 Mission Critical

The topic of this book is resilience in power electronics. Resilience is often supposed to be fault tolerance. However, there is an important difference between a fault-tolerant system and a resilient system. This difference is mission critical considerations, which become more important in applications involving critical missions. These systems are named mission critical systems. A mission critical system is a system that is essential to the survival of a mission [10]. As an example, databases and process control software are considered mission critical to a company that runs on mainframes or workstations. Emergency call centers, computerized hospital patient records, data storage centers, stock exchanges, and other operations dependent on computer and communication systems have to be protected against breakdowns due to the system's mission critical functions. In each of these cases, the failure of a mission critical service can cause severe disruption of services, heavy financial losses, and even danger to people. Many essential functions depend on electricity. When a mission critical system fails or is interrupted, system operations are significantly impacted. Mission essential equipment and mission critical applications are also known as mission critical systems. Mission critical systems are well known in business and organizations. Examples of mission critical systems are: an online banking system, railway/aircraft operating control systems, electric power systems, and many other computer systems that will adversely affect business and society when they fail. As an example, an aircraft is highly dependent on its navigation system. Another example is a nuclear plant. A nuclear reactor controls and contains the sustained nuclear chain reaction. It is usually used for generating electricity. Nuclear reactors have been one of the most concerning systems for public safety worldwide because the malfunction of a nuclear reactor can cause serious disasters. Figure 1.13 shows various applications with mission critical systems. An aircraft is a very visible example. Aircraft reliability programs are essential to ensure safety and dependability. To achieve the highest level of aircraft dispatch reliability at the lowest cost, it is essential to use operational data, pilot reports, and assess the effectiveness of maintenance and training programs.

This is the most important part of this section. The difference between the fault-tolerant systems and resilient systems comes from attention to the concept of mission critical. In other words, the

Figure 1.13 Some applications with mission critical. (a) surgery room, (b) air craft, (c) nuclear plant. *Sources:* Pfree2014/Wikipedia Commons/CC BY-SA 4.0; papazachariasa/Pixabay; (c) ITAR-TASS News Agency/Alamy Images.

time needed for survival of the mission of the system determines its level of resilience. As an example, consider a power supply in an aircraft. This converter can be fault tolerant in the ground base with a long time for recovery. However, this converter must supply the loads in the aircraft without being absent for a long time. The reason is obvious: if the power supply of the aircraft fails for a long time, it will be damaged! As a famous historic example, the Japanese men's gymnastics team in the 1976 Montreal Olympics is presented in reference [11]. In this Olympics, the Japanese men's gymnastics team won five consecutive gold medals in the team event for the first time in Olympic history. The team members were Hiroshi Kajiyama, Eizo Kenmotsu, Hisato Igarashi, Sawao Kato, Shun Fujimoto, and Mitsuo Tsukahara. Soon after Fujimoto stepped onto the mat for the preliminary floor exercise disaster struck. Landing awkwardly during a tumbling run, the Japanese gymnast shattered his kneecap—an excruciatingly painful injury that looked to have dashed his (and perhaps Japan's) Olympic dreams. The heroic gymnast decided against telling his teammates about his injury and continued on to the pommel horse and ring exercises—two events where clean dismounts are vital and where a painful impact to his broken knee could not be avoided. With his team trailing the Soviet Union by little more than a point, Fujimoto stepped up to the rings, where in order to play his part in Japan's victory, he would need to land a dismount from 2.4 m above the ground. Fujimoto's performances that day proved key to Japan's quest for gold, as shown in Figure 1.14.

Figure 1.14 The Japanese men's gymnastics team in 1976 Montreal Olympics; Shun Fujimoto with a broken knee is seen. *Source:* Don Morley/Hulton Archive/Getty Images.

1.4 Faulty Condition in a System

A faulty condition is a state of the system where the system mission is interrupted or the system quality is reduced to an unacceptable level. Faults are the factors generating the faulty condition in a system. In the general form, there are two types of faults: intrinsic (internal) faults and extrinsic (external) faults. These two categories of the faults occur together. External faults cause an increase in the stress on the system elements.

1.4.1 Internal Faults

Intrinsic faults are triggered by internal failure causes in the system. Failures of the elements and subsystems are the reason for system intrinsic faults. Figure 1.15 shows an example of an internal fault in an aircraft.

1.4.2 External Faults

On the other hand, extrinsic faults are forced from outside of the system. They are applied to the system via inputs and outputs of the system. On 15 January 2009, US Airways Flight 1549, an

Airbus A320 on a flight, struck a flock of birds shortly after take-off, losing all engine power. Unable to reach any airport for an emergency landing due to their low altitude, pilots glided the plane to a ditching in the Hudson River off Midtown Manhattan. All 155 people on board were rescued by nearby boats, with a few serious injuries, as shown in Figure 1.16. This water landing of a powerless jetliner with no deaths became known as the Miracle on the Hudson [12]. In this example, the birds were the reason for the external fault.

Figure 1.15 Internal fault in the engine of an aircraft. *Source:* aapsky/Adobe Stock.

Figure 1.16 Miracle on the Hudson. *Source:* Greg L/Wikimedia Commons.

1.4.3 Malfunctioning

The internal and external faults may act as the factors that force the system to work in an abnormal state. In this state, the system works but its outputs are not acceptable. No system element nor subsystem is damaged in this condition but they are forced to work abnormally. False data are the main reason for this malfunctioning. Air France Flight 447 was a scheduled international passenger flight from Rio de Janeiro, Brazil, to Paris, France. On 1 June 2009, the Airbus A330 serving the flight stalled and did not recover, eventually crashing into the Atlantic Ocean, as shown in Figure 1.17. Temporary inconsistency between the measured speeds was likely to have been the result of an obstruction of the pitot tubes by ice crystals [13].

1.5 System Health Awareness

One of the most important requirements of a system for resilient operation is the system health awareness. Thus, the sign of the faults can be detected at an earlier time and make the system ready for reacting. As an example, in biology, the nervous system is a highly complex part of an animal that coordinates its actions and sensory information by transmitting signals to and from different parts of its body. The nervous system detects environmental changes that impact the body and then works in tandem with the endocrine system to respond to such events. Neurons have special structures that allow them to send signals rapidly and precisely to other cells. They send these signals in the form of electrochemical impulses traveling along thin fibers called axons, which can be directly transmitted to neighboring cells through electrical synapses or cause chemicals called neurotransmitters to be released at chemical synapses. A cell that receives a synaptic signal from a neuron may be excited, inhibited, or otherwise modulated. The connections between neurons can form

Figure 1.17 Air France Flight 447. *Source:* Alamy Images/Abaca Press.

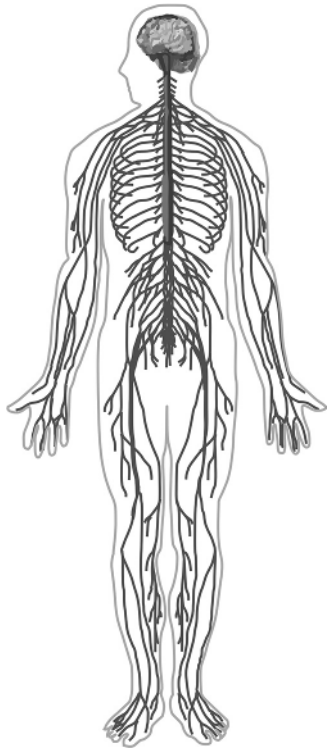

Figure 1.18 The human nervous system.

neural pathways, neural circuits, and larger networks that generate an organism's perception of the world and determine its behavior. (Figure 1.18).

1.5.1 System Condition Monitoring

Condition monitoring is the process of monitoring a parameter of condition in the systems to identify a significant change that is indicative of a developing fault. The use of conditional monitoring allows maintenance to be scheduled or other actions to be taken to prevent failure and avoid its consequences. Condition monitoring allows information to be obtained about the growth of failure in the systems. Our decision about this failure is related to the data that are obtained from the condition monitoring system. For example, monitoring of a long-term high-output current beyond the nominal specification of a power electronic converter usually causes the protection system to operate and take it out of service. There are two main approaches for condition monitoring: sensor-less and sensor-based methods. In sensor-based methods, a physical sensor is used to measure and monitor the desired parameter or variable. In the sensor-less method, the job is done based on calculations. Sensor-based methods are historically the first method for condition monitoring. They have some features and advantages that allows them to be still applicable in power converters. Faster access to data derived from online measurements provides a more efficient response. Although the benefits and even the necessity of using online sensors are recognized, several factors need to be considered prior to their installation in industrial applications. Typical industrial environments often involve fluids, temperatures, pressures, and flows that could be harmful to the delicate electronic sensor components. Sensor-less methodology is a solution for eliminating the physical sensors required for the control process.

It is historically applied to servomotor systems for controlling goals. However, sensor-less methods are also used for normal condition monitoring. Monitoring the state of mechanical machine tool components is of growing importance for increasing machine tool availability and reducing inspection efforts and costs. Figure 1.19 shows some examples of condition monitoring systems.

1.5.2 Fault Prognosis

Prognosis is the capability to use the observations to predict the future states of a machine or forecast a fault before its occurrence. Engineering systems, such as aircraft, industrial processes, manufacturing systems, transportation systems, electrical and electronic systems, etc. are becoming more complex and are subjected to failures that impact adversely their reliability, availability, safety, and maintainability. Such critical assets are required to be available when needed, and

(a)

(b)

Figure 1.19 Some examples of the condition monitoring systems. (a): in a plant, (b): in a car. *Sources:* RGtimeline/Adobe Stock; Pexels/Pixabay.

maintained on the basis of their current condition rather than on the basis of scheduled or breakdown maintenance practices. Moreover, online, real-time fault diagnosis and prognosis can assist the operator to avoid catastrophic events. Recent advances in condition-based maintenance and prognostics have prompted the development of new algorithms for fault, or incipient failure, diagnosis, and failure prognosis aimed at improving the performance of critical systems. Potential benefits to industry include reduced maintenance costs, improved equipment uptime and safety. As an example, the Cooper test shown in Figure 1.20 was one of the most commonly used fitness tests to measure the fitness levels of both amateur and professional football referees. Another example is the blood test for illness prognosis as shown in Figure 1.21.

Figure 1.20 The Cooper test. *Source:* mainathlet/Pixabay.

Figure 1.21 Blood test as a prognosis of the human illness. *Source:* Photographee.eu/Adobe Stock.

1.5.3 Fault Diagnosis

Fault diagnosis is determining which fault has occurred. Process fault diagnosis involves interpreting the current status of the plant from given sensor readings and process knowledge. Fault detection and diagnosis techniques are based upon the use of process models. Data from the plant is fed into these algorithms and the outputs are compared with the corresponding plant outputs. If there are discrepancies, it is an indication that at least one fault has occurred. The location of the fault is determined using a representative model. Figure 1.22 shows the diagnosis of a fault in a car brake disc.

1.6 Methods for Resilience

According to the above-mentioned explanations, any method that prevents a fault occurrence or fault influence (after an occurrence) can be defined as a method of resilience. Some of these methods help the systems to prevent the fault occurrence. Prevention cannot be ideally realized. This means that the methods reduce the failure rate of the system to such a low level that the system does not fail between two consecutive maintenance processes. However, in a very important mission critical system, even one fault is important. On the other hand, some faults are outside the control of the method used for fault prevention. Here, the other methods of resilience enter the problem. They act after the fault occurrence and keep the system performance at an acceptable level until the mission is passed.

1.6.1 Protection

The system must operate and it is logically affected by stress. It is true that we reduce the stress but the stress still exists and may cause failure in the long term. Then we are faced with a fault in the system. Protection systems act when a fault occurs in the system. Their performance is very important; isolation of the system is not always the best choice because this strategy has a

Figure 1.22 Inspection of a brake disc. *Source:* geraldoswald62/Pixabay.

bad effect on availability of the system. Protection methods save the system against non-catastrophic faults. However, this method saves the system but it also takes the converter out of service. If the protection system is very fast, it protects the system but conflict with noise is possible. Therefore, protection systems should be fast enough to protect the system but not so fast as to interrupt the operation. The protection system operates against both the external faults and internal faults. Examples of protection against external faults are the chest in a male body, shown in Figure 1.23, and the car guard, shown in Figure 1.24. An example of the protection against internal faults is the fire extinguisher of aircraft engines, shown in Figure 1.25.

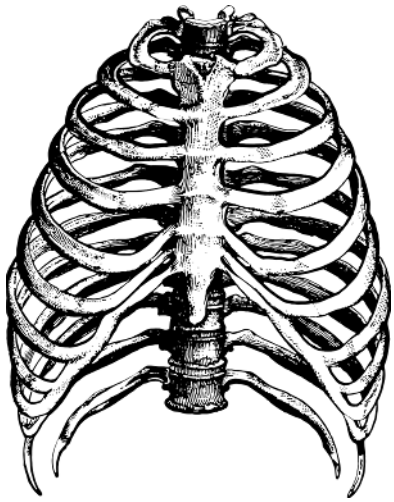

Figure 1.23 Chest as a protective part of the body. *Source:* StarGladeVintage/Pixabay.

Figure 1.24 Protective guard of a car. *Source:* Kruglovsasha/Wikimedia Commons.

Figure 1.25 Fire extinguisher of aircraft engines. *Source:* AviationNuggets.

1.6.2 Derating

Protection techniques prevent catastrophic failures in electric power converters. However, as described before, protection systems cannot prevent any fault. There are two main approaches to a faulty converter. Isolating the faulty converter is one of the approaches and is used when the converter mission can be interrupted for repair and maintenance. If the mission of the converter is important at the time of failure, users should use another method. Derating is a method for allowing the faulty converter to continue its mission. Although the derating method is mainly a method for faulty systems, it can also be used for extending life in normal cases. Component failure rates generally decrease as applied stress levels decrease. Thus, derating or operating components at levels below their ratings (for current, voltage, power dissipation, temperature, etc.) will increase reliability. Derating increases the margin of safety between part design limits and applied stresses, thereby providing extra protection for the part. By applying derating in an electrical or electronic component, its degradation rate is reduced and reliability and life expectancy are improved. As an example, aging is the process of becoming older. The term refers especially to humans and many other animals. In humans, aging represents the accumulation of changes in a human being over time and can encompass physical, psychological, and social changes. Reaction time, for example, may slow with age, as shown in Figure 1.26, while memories and general knowledge typically increase.

Another example is Alzheimer's disease, which is a neurodegenerative disease that usually starts slowly and progressively worsens. The most common early symptom is difficulty in remembering recent events. As the disease advances, symptoms can include problems with language, disorientation, mood swings, loss of motivation, self-neglect, and behavioral issues.

The heart attack is another example. A heart attack occurs when a coronary artery becomes completely blocked and a large portion of the muscle stops receiving blood. A serious heart attack

Figure 1.26 Aging as a derating process in a man. *Source:* FreeToUseSounds/Pixabay.

can cause significant damage. However, a heart attack may occur only partially and in this case the affected coronary artery is only partially blocked.

In industries, the Boeing 777 is a good example. The Boeing 777 is an American wide-body airliner, which is shown in Figure 1.27. It is the world's largest twin-engine jet aircraft and can fly with only one engine for three hours. These regulations allowed twin-engine airliners to make ocean crossings at up to three hours' distance from emergency diversionary airports.

1.6.3 Stress Reduction

Reliability of a system increases if it operates at a set point with low stress. The failure mechanism of a system is started immediately after the first operation. At the beginning, the system operates normally but under stress of failure factors:

- Power losses in the system cause the temperature to rise in various parts of the system.
- Applied voltage causes an electric field to be applied to insulators.
- Mechanical forces lead to vibrations.
- Environmental factors.

These factors act from the beginning of system application. In the long term, they cause the system to age and lead to its failure. The time interval for changing a stress factor to a failure factor is directly related to the amount of stress. Higher stress leads to a shorter time to failure and vice

Figure 1.27 Boeing 777: the largest twinjet aircraft that fly with one engine for three hours. *Source:* Aero Icarus/Wikipedia Commons/CC BY-SA 2.0.

Figure 1.28 An electric soft starter used for reducing the stress on the electric motors during power on. *Source:* Demjas/Wikipedia Commons/CC BY-SA 4.0.

versa. Thus, the first method of reliability improvement is reducing the stress factors on the system. As an example, a motor soft starter shown in Figure 1.28 is a device used with AC electrical motors to temporarily reduce the load and torque in the powertrain and electric current surge of the motor during start-up. This reduces the mechanical stress on the motor and shaft, as well as the electrodynamic stresses on the attached power cables and electrical distribution network, extending the lifespan of the system. It can consist of mechanical or electrical devices, or a combination of both. Mechanical soft starters include clutches and several types of couplings using a fluid, magnetic forces, or steel shot to transmit torque, similar to other forms of torque limiter. Electrical soft starters can be any control system that reduces the torque by temporarily reducing the voltage or current input, or a device that temporarily alters how the motor is connected in the electric circuit. A soft starter continuously controls the motor's voltage supply during the start-up phase. In this way, the motor is adjusted to the machine's load behavior. Mechanical operating equipment is accelerated smoothly. This lengthens service life, improves operating behavior, and smooths work flows.

1.6.4 Immunity Against False Data

Two approaches exist in this section: reducing the data rate in the case of an unknown data channel and shielding against false data. As an example, in electrical engineering, electromagnetic shielding is the practice of reducing the electromagnetic field in a space by blocking the field with barriers made of conductive or magnetic materials. Shielding is typically applied to enclosures to isolate electrical devices from their surroundings and to cables to isolate wires from the environment through which the cable runs.

1.7 Inherently Resilient Systems

Some of the systems reach to resilience by providing the no-fault state. Figure 1.29 shows two inherently resilient aircrafts. Lockheed aircrafts U-2 and SR-71 have an unattainable flying altitude and speed, respectively. Therefore, they are inherently resilient against any attack as the external fault.

Mongooses shown in Figure 1.30 are one of at least four known mammalian taxa with mutations in the nicotinic acetylcholine receptor that protect against snake venom [14]. Their modified receptors prevent the snake venom α-neurotoxin from binding.

Achieving the inherently resilient characteristic may be valid for a certain time interval. The kidney operation is an example. Most humans are born with two kidneys, shown in Figure 1.31, as the functional components of what is called the renal system, which also includes two ureters, a bladder, and a urethra. The kidneys have many functions, including regulating blood pressure, producing red blood cells, activating vitamin D, and producing some glucose. Most evidently, however, the kidneys filter body fluids via the bloodstream to regulate and optimize their amount, composition, pH, and osmotic pressure. Life is incompatible with a lack of kidney function. However, unlike the case with most other organs, we are born with an overabundant kidney capacity. Indeed, a single kidney with only 75% of its functional capacity can sustain life very well. If only one kidney is present, that kidney can adjust to filter as much as two kidneys would normally. In such a situation, the nephrons compensate individually by increasing in size—a process known as hypertrophy—to handle the extra load. This happens with no adverse effects, even over years.

(a) (b)

Figure 1.29 Two inherently resilient aircrafts, (a) U-2, (b) SR-71. *Sources:* (a) US Air Force/Wikipedia Commons/Public Domain; (b) USAF/Judson Brohmer/Wikipedia Commons/Public Domain.

Figure 1.30 Mongoose as an inherently resilient animal against external fault of the snake venom. *Source:* Dan Dennis/Unsplash.com/.

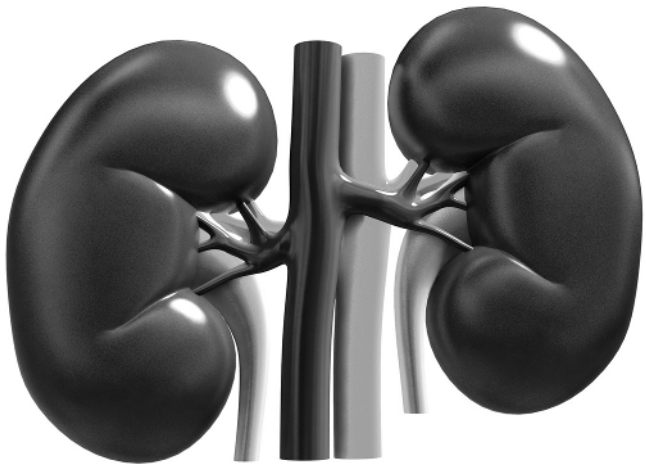

Figure 1.31 Most humans are born with two kidneys that they can operate redundantly for resilience. *Source:* abhijith3747/Adobe Stock.

1.8 Summary and Conclusions

In this chapter, a brief introduction of the concept of resilience in systems was presented. The necessity of resilience in systems and its requirements were described. The results of this chapter are summarized as follows:

1) The resilience concept is defined as the capability to recover from an abnormal state to another state where this new state guarantees the continuance operation of the system.
2) Resilient operation is defined in systems with a critical mission. A mission critical system is a system that is essential to the survival of a mission.

3) The requirements for resilient operation are system health monitoring, fault-tolerant characteristics, an intelligent protection system, and operation under low stress.
4) Some of the systems are inherently resilient. In these systems, the fault origins are removed by the advanced characteristics of the system.

References

1 Hitchins, D.K. (2007). *Systems Engineering: A 21st Century Systems Methodology*. Wiley.
2 Wasson, C.S. (2015). *System Engineering Analysis, Design, and Development: Concepts, Principles, and Practices*, 2e. Wiley.
3 www.drivek.co.uk/car-comparison-technical-details-features-dimensions, 2021.
4 Si, X., Wang, W., Hu, C. et al. (2012). Remaining useful life estimation based on a nonlinear diffusion degradation process. *IEEE Transactions on Reliability* 61 (1): 50–67.
5 Kapur, K.C. and Pecht, M. (2014). *Reliability Engineering*. Wiley.
6 Chung, H.S., Wang, H., Blaabjerg, F., and Pecht, M. (2015). *Reliability of Power Electronic Converter Systems*. IET Press.
7 Rohatgi, V.K., Md, A.K., and Saleh, E. (2015). *An Introduction to Probability and Statistics*, 3e. Wiley.
8 Boeing B-17F. National Museum of the U.S. Air Force. Archived from the original on August 8, 2016. Retrieved 8 August 2016.
9 Ma, K., Liserre, M., Blaabjerg, F., and Kerekes, T. (2015). Thermal loading and lifetime estimation for power device considering mission profiles in wind power converter. *IEEE Transactions on Power Electronics* 30 (2): 590–602.
10 Banerjee, A., Venkatasubramanian, K.K., Mukherjee, T., and Gupta, S.K.S. (2012). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proceedings of the IEEE* 100 (1): 283–299.
11 https://olympics.com/en/news/fujimoto-bravery-helps-japan-make-it-five-golds-in-a-row-gymnastics, 1976.
12 Clark, A. (2009). Plane crashes in Hudson River in New York. via www.theguardian.com.
13 Clark, N. (2017). Report on air france crash points to pilot training issues. *The New York Times*.
14 Barchan, D., Kachalsky, S., Neumann, D. et al. (1992). How the mongoose can fight the snake: the binding site of the mongoose acetylcholine receptor. *Proceedings of the National Academy of Sciences* 89 (16): 7717–7721.