System Reliability, Availability, and Maintainability

Lead Authors: *Paul Phister, David Olwell*

Reliability, availability, and maintainability (RAM) are three system attributes that are of tremendous interest to systems engineers, logisticians, and users. They are often studied together. Collectively, they affect economic life-cycle costs of a system and its utility.

□

Contents

Overview

Reliability, maintainability, and availability (RAM) are three system attributes that are of great interest to systems engineers, logisticians, and users. Collectively, they affect both the utility and the life-cycle costs of a product or system. The origins of contemporary reliability engineering can be traced to World War II. The discipline's first concerns were electronic and mechanical components. (Ebeling 2010) However, current trends point to a dramatic rise in the number of industrial, military, and consumer products with integrated computing functions. Because of the rapidly increasing integration of computers into products and systems used by consumers, industry, governments, and the military, reliability must consider both hardware, and software.

Maintainability models present some interesting challenges. The time to repair an item is the sum of the time required for evacuation, diagnosis, assembly of resources (parts, bays, tool, and mechanics), repair, inspection, and return. Administrative delay (such as holidays) can also affect repair times. Often these sub-processes have a minimum time to complete that is not

zero, resulting in the distributions used to model maintainability having a threshold parameter.

A threshold parameter is defined as the minimum probable time to repair. Estimation of maintainability can be further complicated by queuing effects, resulting in times to repair that are not independent. This dependency frequently makes analytical solution of problems involving maintainability intractable and promotes the use of simulation to support analysis.

System Description

This section sets forth basic definitions, briefly describes probability distributions, and then discusses the role of RAM engineering during system development and operation. The final subsection lists the more common reliability test methods that span development and operation.

Basic Definitions

Reliability

Reliability is defined as the probability of a product performing its intended function under stated conditions without failure for a given period of time. (ASQ 2022) A precise definition must include a detailed description of the function, the environment, the time scale, and what constitutes a failure. Each can be surprisingly difficult to define precisely.

Maintainability

The probability that a given maintenance action for an item under given usage conditions can be performed within a stated time interval when the maintenance is performed under stated conditions using stated procedures and resources. Maintainability has two categories: serviceability (the ease of conducting scheduled inspections and servicing) and repairability (the ease of restoring service after a failure). (ASQ 2022)

Availability

Defined as the probability that a repairable system or system element is operational at a given point in time under a given set of environmental conditions. Availability depends on reliability and maintainability

and is discussed in detail later in this topic. (ASQ 2011)

Failure

A failure is the event(s), or inoperable state, in which any item or part of an item does not, or would not, perform as specified. (GEIA 2008) The failure mechanism is the physical, chemical, electrical, thermal, or other process that results in failure (GEIA 2008). In computerized systems, a software defect or fault can be the cause of a failure (Laprie 1992) which may have been preceded by an error which was internal to the item. The failure mode is the way or the consequence of the mechanism through which an item fails. (GEIA 2008, Laprie 1992) The severity of the failure mode is the magnitude of its impact. (Laprie 1992)

Probability Distributions used in Reliability Analysis

Reliability can be thought of as the probability of the survival of a component until time *t*. Its complement is the probability of failure before or at time *t*. If we define a random variable *T* as the time to failure, then:

```
<math>
       R(t)=P(T>t)=1-F(t)
       </math>
```

where *R(t)* is the reliability and *F(t)* is the failure probability. The failure probability is the cumulative distribution function (CDF) of a mathematical probability distribution. Continuous distributions used for this purpose include exponential, Weibull, log-normal, and generalized gamma. Discrete distributions such as the Bernoulli, Binomial, and Poisson are used for calculating the expected number of failures or for single probabilities of success.

The same continuous distributions used for reliability can also be used for maintainability although the interpretation is different (i.e., probability that a failed component is restored to service prior to time *t*). However, predictions of maintainability may have to account for processes such as administrative delays, travel time, sparing, and staffing and can therefore be extremely complex.

The probability distributions used in reliability and maintainability estimation are referred to as models

because they only provide estimates of the true failure and restoration of the items under evaluation. Ideally, the values of the parameters used in these models would be estimated from life testing or operating experience. However, performing such tests or collecting credible operating data once items are fielded can be costly. Therefore, approximations sometimes use data from “similar systems”, “engineering judgment”, and other methods. As a result, those estimates based on limited data may be very imprecise. Testing methods to gather such data are discussed below.

RAM Considerations during Systems Development

RAM are inherent product or system attributes that should be considered throughout the development lifecycle. Reliability standards, textbook authors, and others have proposed multiple development process models. (O’Connor 2014, Kapur 2014, Ebeling 2010, DoD 2005) The discussion in this section relies on a standard developed by a joint effort by the Electronic Industry Association and the U.S. Government and adopted by the U.S. Department of Defense (GEIA 2008) that defines 4 processes: understanding user requirements and constraints, design for reliability, production for reliability, and monitoring during operation and use (discussed in the next section).

Understanding User Requirements and Constraints

Understanding user requirements involves eliciting information about functional requirements, constraints (e.g., mass, power consumption, spatial footprint, life cycle cost), and needs that correspondent to RAM requirements. From these emerge system requirements that should include specifications for reliability, maintainability, and availability, and each should be conditioned on the projected operating environments. RAM requirements definition is as challenging but as essential to development success as the definition of general functional requirements.

Design for Reliability

System designs based on user requirements and system design alternatives can then be formulated and evaluated. Reliability engineering during this phase seeks to increase system robustness through measures

such as redundancy, diversity, built-in testing, advanced diagnostics, and modularity to enable rapid physical replacement. In addition, it may be possible to reduce failure rates through measures such as use of higher strength materials, increasing the quality components, moderating extreme environmental conditions, or shortened maintenance, inspection, or overhaul intervals. Design analyses may include mechanical stress, corrosion, and radiation analyses for mechanical components, thermal analyses for mechanical and electrical components, and Electromagnetic Interference (EMI) analyses or measurements for electrical components and subsystems.

In most computer-based systems, hardware mean time between failures are hundreds of thousands of hours so that most system design measures to increase system reliability are focused on software. The most obvious way to improve software reliability is by improving its quality through more disciplined development efforts and tests. Methods for doing so are in the scope of software engineering but not in the scope of this section. However, reliability and availability can also be increased through architectural redundancy, independence, and diversity. Redundancy must be accompanied by measures to ensure data consistency, and managed failure detection and switchover. Within the software architecture, measures such as watchdog timers, flow control, data integrity checks (e.g., hashing or cyclic redundancy checks), input and output validity checking, retries, and restarts can increase reliability and failure detection coverage (Shooman 2002).

System RAM characteristics should be continuously evaluated as the design progresses. Where failure rates are not known (as is often the case for unique or custom developed components, assemblies, or software), developmental testing may be undertaken to assess the reliability of custom-developed components. Evaluations based on quantitative analyses assess the numerical reliability and availability of the system and are usually based on reliability block diagrams, fault trees, Markov models, and Petri nets. (O'Connor 2011) Markov models and Petri nets are of particular value for computer-based systems that use redundancy. Evaluations based on qualitative analyses assess vulnerability to single points of failure, failure containment, recovery, and maintainability. The primary qualitative methods are the failure mode effects and criticality analyses (FMECA). (Kececioglu 1991) The development program Discrepancy Reporting (DR) or Failure Reporting and Corrective Action System (FRACAS) should also be used

to identify failure modes which may not have been anticipated by the FMECA and to identify common problems that can be corrected through an improved design or development process.

Analyses from related disciplines during design time also affect RAM. Human factor analyses are necessary to ensure that operators and maintainers can interact with the system in a manner that minimizes failures and the restoration times when they occur. There is also a strong link between RAM and cybersecurity in computer-based systems. On the one hand, defensive measures reduce the frequency of failures due to malicious events. On the other hand, devices such as firewalls, policy enforcement devices, and access/authentication serves (also known as "directory servers") can also become single points of failure or performance bottlenecks that reduce system reliability and availability.

Production for Reliability

Many production issues associated with RAM are related to quality. The most important of these are ensuring repeatability and uniformity of production processes and complete unambiguous specifications for items from the supply chain. Other are related to design for manufacturability, storage, and transportation. (Kapur 2014; Eberlin 2010) Large software intensive information systems are affected by issues related to configuration management, integration testing, and installation testing. Testing and recording of failures in the problem reporting and corrective action systems (PRACAS) or the FRACAS capture data on failures and improvements to correct failures. Depending on organizational considerations, this may be the same or a separate system as used during the design.

Monitoring During Operation and Use

After systems are fielded, their reliability and availability are monitored to assess whether the system or product has met its RAM objectives, identify unexpected failure modes, record fixes, and assess the utilization of maintenance resources and the operating environment. The FRACAS or a maintenance management database may be used for this purpose. In order to assess RAM, it is necessary to maintain an accurate record not only of failures but also of operating time and the duration of outages. Systems that report only on repair actions and outage incidents may not be sufficient for this purpose.

An organization should have an integrated data system that allows reliability data to be considered with logistical data, such as parts, personnel, tools, bays, transportation and evacuation, queues, and costs, allowing a total awareness of the interplay of logistical and RAM issues. These issues in turn must be integrated with management and operational systems to allow the organization to reap the benefits that can occur from complete situational awareness with respect to RAM.

Reliability and Maintainability Testing

Reliability Testing can be performed at the component, subsystem, and system level throughout the product or system lifecycle. Examples of hardware related categories of reliability testing are detailed in Ebeling (2010) and O'Connor (2014).

- **Reliability Life Tests:** Reliability life tests are used to empirically assess the time to failure for non-repairable products and systems and the times between failure for repairable or restorable systems. Termination criteria for such tests can be based on a planned duration or planned number of failures. Methods to account for "censoring" of the failures or the surviving units enable a more accurate estimate of reliability. (Meeker, Escobar, Pascual 2022)
- **Accelerated Life Tests:** Accelerated life testing is performed by subjecting the items under test (usually electronic parts) to increased stress well above the expecting operating range and extrapolating results using model such as an Arrhenius relation (temperature acceleration), inverse power law (voltage), or a cumulative damage model (non-constant stress). (Meeker, Escobar, Pascual 2022)
- **Highly Accelerated Life Testing/Highly Accelerated Stress Testing (HALT/HASS):** is performed by subjecting units under test (components or subassemblies) to extreme temperature and vibration tests with the objective of identifying failure modes, margins, and design weaknesses.
- **Parts Screening:** Parts screening is not really a test but a procedure to operate components for a duration beyond the "infant mortality" period during which less durable items fail and the more durable parts that remain are then assembled into the final product or

system. This is also known as "burn-in."

- **System Level Testing:** Examples of system level testing (including both hardware and software) are detailed in O'Connor (2014) and Ebeling (2010).
- **Stability Tests:** Stability tests are life tests for integrated hardware and software systems. The goal of such testing is to determine the integrated system failure rate and assess operational suitability. Test conditions must include accurate simulation of the operating environment (including workload) and a means of identifying and recording failures.
- **Reliability Growth Tests:** Reliability growth testing is part of a reliability growth program in which items are tested throughout the development and early production cycle with the intent of assessing reliability increases due to improvements in the manufacturing process (for hardware) or software quality (for software). Also known as "Test-Analyze-And-Fix (TAAF)." (NRC 2015)
- **Failure/Recovery Tests:** Such testing assesses the fault tolerance of a system by measuring probability of switchover for redundant systems. Failures are simulated and the ability of the hardware and software to detect the condition and reconfigure the system to remain operational are tested.
- **Maintainability Tests:** Such testing assesses the system diagnostics capabilities, physical accessibility, and maintainer training by simulating hardware or software failures that require maintainer action for restoration.

Because of its potential impact on cost and schedule, reliability testing should be coordinated with the overall system engineering effort. Test planning considerations include the number of test units, duration of the tests, environmental conditions, and the means of detecting failures.

Data Issues

True RAM models for a system are generally never known. Data on a given system is assumed or collected, used to select a distribution for a model, and then used to fit the parameters of the distribution. This process

differs significantly from the one usually taught in an introductory statistics course.

First, the normal distribution is seldom used as a life distribution, since it is defined for all negative times. Second, and more importantly, reliability data is different from classic experimental data. Reliability data is often censored, biased, observational, and missing information about covariates such as environmental conditions. Data from testing is often expensive, resulting in small sample sizes. These problems with reliability data require sophisticated strategies and processes to mitigate them.

One consequence of these issues is that estimates based on limited data can be and usually are very imprecise.

Discipline Management

In most large programs, RAM experts report to the system engineering organization. At project or product conception, top level goals are defined for RAM based on operational needs, lifecycle cost projections, and warranty cost estimates. These lead to RAM derived requirements and allocations that are approved and managed by the system engineering requirements management function. RAM testing is coordinated with other product or system testing through the testing organization, and test failures are evaluated by the RAM function through joint meetings such as a Failure Review Board. In some cases, the RAM function may recommend design or development process changes as a result of evaluation of test results or software discrepancy reports, and these proposals must be adjudicated by the system engineering organization, or in some cases, the acquiring customer if cost increases are involved.

Post-Production Management Systems

Once a system is fielded, its reliability and availability should be tracked. Doing so allows the producer/owner to verify that the design has met its RAM objectives, to identify unexpected failure modes, to record fixes, to assess the utilization of maintenance resources, and to assess the operating environment.

One such tracking system is generically known as a FRACAS system (Failure Reporting and Corrective Action System). Such a system captures data on failures and improvements to correct failures. This database is separate from a warranty database, which is typically

run by the financial function of an organization and tracks costs only.

A FRACAS for an organization is a system, and itself should be designed following systems engineering principles. In particular, a FRACAS system supports later analyses, and those analyses impose data requirements. Unfortunately, the lack of careful consideration of the backward flow from decision to analysis to model to required data too often leads to inadequate data collection systems and missing essential information. Proper prior planning prevents this poor performance.

Of particular importance is a plan to track data on units that have not failed. Units whose precise times of failure are unknown are referred to as censored units. Inexperienced analysts frequently do not know how to analyze censored data, and they omit the censored units as a result. This can bias an analysis.

An organization should have an integrated data system that allows reliability data to be considered with logistical data, such as parts, personnel, tools, bays, transportation and evacuation, queues, and costs, allowing a total awareness of the interplay of logistical and RAM issues. These issues in turn must be integrated with management and operational systems to allow the organization to reap the benefits that can occur from complete situational awareness with respect to RAM.

Discipline Relationships

Interactions

RAM interacts with nearly all aspects of the system development effort. Specific dependencies and interactions include:

- **Systems Engineering:** RAM interacts with systems engineering as described in the previous section.
- **Product Management (Life Cycle Cost and Warranty):** RAM interacts with the product or system lifecycle cost and warranty management organizations by assisting in the calculation of expected repair rates, downtimes, and warranty costs. RAM may work with those organizations to perform tradeoff analyses to determine the most cost-efficient solution and to price service contracts.

- **Quality Assurance:** RAM may also interact with the procurement and quality assurance organizations with respect to selection and evaluation of materials, components, and subsystems.

Dependencies

- **Systems Safety:** RAM and system safety engineers have many common concerns with respect to managing the failure behavior of a system (i.e., single points of failure and failure propagation). RAM and safety engineers use similar analysis techniques, with safety being concerned about failures affecting life or unique property and RAM being concerned with those failures as well as lower severity events that disrupt operations. RAM and system safety are both concerned with failures occurring during development and test – FRACAS is the primary methodology used for RAM; hazard tracking is the methodology used for system safety.
- **Cybersecurity:** In systems or products integrating computers and software, cybersecurity and RAM engineers have common concerns relating to the availability of cyber defenses and system event monitoring. However, there are also tradeoffs with respect to access control, boundary devices, and authentication where security device failures could impact the availability of the product or system to users.
- **Software and Hardware Engineering:** Design and RAM engineers have a common goal of creating dependable products and systems. RAM interacts with the software and hardware reliability functions through design analyses such as failure modes and effects analyses, reliability predictions, thermal analyses, reliability measurement, and component specific analyses. RAM may recommend design changes as a result of these analyses that may have to be adjudicated by program management, the customer, or systems engineering if there are cost or schedule impacts.
- **Testing:** RAM interacts with the testing program during planning to assess the most efficient (or feasible) test events to perform life testing,

failure/recovery testing, and stability testing as well as to coordinate requirements for reliability or stress tests. RAM also interacts with the testing organization to assess test results and analyze failures for the implications on product or system RAM.

- **Logistics:** RAM works with logistics in providing expected failure rates and downtime constraints in order for logistics engineers to determine staffing, sparing, and special maintenance equipment requirements.

Discipline Standards

Because of the importance of reliability, availability, and maintainability, as well as related attributes, there are hundreds of standards associated. Some are general but more are specific to domains such as automotive, aviation, electric power distribution, nuclear energy, rail transportation, software, etc.Standards are produced by both governmental agencies, professional associations and international standards bodies such as:

- The International Electrotechnical Commission (IEC), Geneva, Switzerland and the closely associated International Standards Organization (ISO)
- The Institute of Electrical and Electronic Engineers (IEEE), New York, NY, USA
- The Society of Automotive Engineers (SAE), Warrendale, PA, USA
- Governmental Agencies – primarily in military and space systems

The following table lists selected standards from each of these agencies. Because of differences in domains and because many standards handle the same topic in slightly different ways, selection of the appropriate standards requires consideration of previous practices (often documented as contractual requirements), domain specific considerations, certification agency requirements, end user requirements (if different from the acquisition or producing organization), and product or system characteristics.

Table 1. Selected Reliability, Availability, Maintainability standards (SEBoK Original)

Organization	Number, Title, and Year	Domain	Comment
IEC	IEC 60812, Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), 2006	General	
IEC	IEC 61703 Ed 2.0, Mathematical expressions for reliability, availability, maintainability and maintenance support terms, 2016	General	
IEC	IEC 62308, Equipment reliability - Reliability assessment methods, 2006	General	
IEC	IEC 62347, Guidance on system dependability specifications, 2006	General	
IEC	IEC 62278, Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS), 2002	Railways	
IEEE	IEEE Std 352-2016, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems and Other Nuclear Facilities, 2016	Nuclear Energy	
IEEE	IEEE Std 1044-2009, IEEE Standard Classification for Software Anomalies, 2009	Software	
IEEE	IEEE Std 1633-2008, IEEE Recommended Practice on Software Reliability, 2016	Software	

SAE	ARP 4754A, Guidelines for the Development of Civil Aircraft and Systems, 2010	Aviation	
SAE	ARP 5890B, Guidelines for Preparing Reliability AssessmentPlans for Electronic Engine Controls, 2018	Aviation	
SAE	J2940_202002, Use of Model Verification and Validation in Product Reliability and Confidence Assessments, 2020	General	
SAE	SAE-GEIA-STD-0009A, Reliability Program Standard for SystemsDesign, Development, and Manufacturing, 2020	General	Used by the U.S. Dept. of Defense as the primary reliability standard (replaces MIL-STD-785B)
SAE	JA 1002_201205, Software Reliability Program Standard, 2012	Software	
U.S. Government	NASA-STD-8729.1A, Planning, Developing and Managing an Effective Reliability And Maintainability (R&M) Program, 2017	Space Systems	
U.S. Government	MIL HDBK 470A, Designing and Developing Maintainable Products and Systems, 1997	Defense Systems	
U.S. Government	MIL HDBK 217F (Notice 2), Reliability Prediction of Electronic Equipment, 1995	Defense Systems	Although formally titled a “Handbook” and more than 2 decades old, the values and methods constitute a de facto standard for some U.S. military acquisitions

U.S. Government	MIL-STD-1629A (Notice 3), Procedures for Performing a Failure Mode Effects and Criticality Analysis - Revision A, 1998	The parent of FMEA standards produced by the IEEE, SAE, ISO, and many other agencies. Still valid and in use after 4 decades.

Personnel Considerations

Becoming a reliability engineer requires education in probability and statistics as well as the specific engineering domain of the product or system under development or in operation. A number of universities throughout the world have departments of reliability engineering (which also address maintainability and availability) and more have research groups and courses in reliability and safety – often within the context of another discipline such as computer science, systems engineering, civil engineering, mechanical engineering, or bioengineering. Because most academic engineering programs do not have a full reliability department, most engineers working in reliability have been educated in other disciplines and acquire the additional skills through additional coursework or by working with other qualified engineers. A certification in reliability engineering is available from the American Society for Quality (ASQ 2016). However, only a minority of engineers working in the discipline have this certification.

Metrics

The three basic metrics of RAM are (not surprisingly) Reliability, Maintainability, and Availability. Reliability can be characterized in terms of the parameters, mean, or any percentile of a reliability distribution. However, in most cases, the exponential distribution is used, and a single value, the mean time to failure (MTTF) for non-restorable systems, or mean time between failures (MTBF for restorable systems are used). The metric is defined as:

```
  <math>
         \left \{ MTTF|MTBF \right \} =
 \frac{T_{op,Tot}}{n_{fails}}
         </math>
```

where T_{op},T_{ot} is the total operating time and n_{fails} is the number of failures.

Maintainability is often characterized in terms of the exponential distribution and the mean time to repair and be similarly calculated, i.e.,

```
<math>
        MTTR = \frac{T_{down,Tot}}{n_{outages}}
        </math>
```

Where $T_{down,Tot}$ is the total down time and $n_{outages}$ is the number of outages.

As was noted above, accounting for downtime requires definitions and specificity. Down time might be counted only for corrective maintenance actions, or it may include both corrective and preventive maintenance actions. Where the lognormal rather than the exponential distribution is used, a mean down time can still be calculated, but both the log of the downtimes and the variance must be known in order to fully characterize maintainability. Availability can be calculated from the total operating time and the downtime, or in the alternative, as a function of MTBF and MTTR (Mean Time To Repair.)

```
<math>
        A = \frac{T_{op,Tot}}{T_{down,tot} + T_{op,tot}}  =
 \frac{MTBF}{MTBF + MTTR}
        </math>
```

As was the case with maintainability, availability may be qualified as to whether it includes only unplanned failures and repairs (inherent availability) or downtime due to all causes including administrative delays, staffing outages, or spares inventory deficiencies (operational availability).

Probabilistic metrics describe system performance for RAM. Quantiles, means, and modes of the distributions used to model RAM are also useful.

Availability has some additional definitions, characterizing what downtime is counted against a system. For **inherent availability**, only downtime associated with corrective maintenance counts against the system. For **achieved availability**, downtime associated with both corrective and preventive

maintenance counts against a system. Finally, **operational availability** counts all sources of downtime, including logistical and administrative, against a system.

Availability can also be calculated instantaneously, averaged over an interval, or reported as an asymptotic value. **Asymptotic availability** can be calculated easily, but care must be taken to analyze whether or not a system settles down or settles up to the asymptotic value, as well as how long it takes until the system approaches that asymptotic value.

Reliability importance measures the effect on the system reliability of a small improvement in a component's reliability. It is defined as the partial derivative of the system reliability with respect to the reliability of a component.

Criticality is the product of a component's reliability, the consequences of a component failure, and the frequency with which a component failure results in a system failure. Criticality is a guide to prioritizing reliability improvement efforts.

Many of these metrics cannot be calculated directly because the integrals involved are intractable. They are usually estimated using simulation.

Models

There are a wide range of models that estimate and predict reliability (Meeker, Escobar, Pascual 2022). Simple models, such as exponential distribution, can be useful for "back of the envelope" calculations.

System models are used to (1) combine probabilities or their surrogates, failure rates and restoration times, at the component level to find a system level probability or (2) to evaluate a system for maintainability, single points of failure, and failure propagation. The three most common are reliability block diagrams, fault trees, and failure modes and effects analyses.

There are more sophisticated probability models used for life data analysis. These are best characterized by their failure rate behavior, which is defined as the probability that a unit fails in the next small interval of time, given it has lived until the beginning of the interval, and divided by the length of the interval.

Models can be considered for a fixed environmental

condition. They can also be extended to include the effect of environmental conditions on system life. Such extended models can in turn be used for accelerated life testing (ALT), where a system is deliberately and carefully overstressed to induce failures more quickly. The data is then extrapolated to usual use conditions. This is often the only way to obtain estimates of the life of highly reliable products in a reasonable amount of time. (Nelson 1990)

Also useful are **degradation models**, where some characteristic of the system is associated with the propensity of the unit to fail (Nelson 1990). As that characteristic degrades, we can estimate times of failure before they occur.

The initial developmental units of a system often do not meet their RAM specifications. **Reliability growth models** allow estimation of resources (particularly testing time) necessary before a system will mature to meet those goals. (Meeker, Escobar, and Pascual 2022, NRC 2015)

Maintainability models describe the time necessary to return a failed repairable system to service. They are usually the sum of a set of models describing different aspects of the maintenance process (e.g., diagnosis, repair, inspection, reporting, and evacuation). These models often have threshold parameters, which are minimum times until an event can occur.

Logistical support models attempt to describe flows through a logistics system and quantify the interaction between maintenance activities and the resources available to support those activities. Queue delays, in particular, are a major source of down time for a repairable system. A logistical support model allows one to explore the trade space between resources and availability.

All these models are abstractions of reality, and so at best approximations to reality. To the extent they provide useful insights, they are still very valuable. The more complicated the model, the more data necessary to estimate it precisely. The greater the extrapolation required for a prediction, the greater the imprecision.

Extrapolation is often unavoidable, because high reliability equipment typically can have long life and the amount of time required to observe failures may exceed test times. This requires strong assumptions be made about future life (such as the absence of masked failure modes) and that these assumptions increase uncertainty

about predictions. The uncertainty introduced by strong model assumptions is often not quantified and presents an unavoidable risk to the system engineer.

There are many ways to characterize the reliability of a system, including fault trees, reliability block diagrams, and failure mode effects analysis.

A **Fault Tree** (Kececioglu 1991) is a graphical representation of the failure modes of a system. It is constructed using logical gates, with AND, OR, NOT, and K of N gates predominating. Fault trees can be complete or partial; a partial fault tree focuses on a failure mode or modes of interest. They allow "drill down" to see the dependencies of systems on nested systems and system elements. Fault trees were pioneered by Bell Labs in the 1960s.

A Failure Mode Effects Analysis is a table that lists the possible failure modes for a system, their likelihood, and the effects of the failure. A Failure Modes Effects Criticality Analysis scores the effects by the magnitude of the product of the consequence and likelihood, allowing ranking of the severity of failure modes. (Kececioglu 1991)

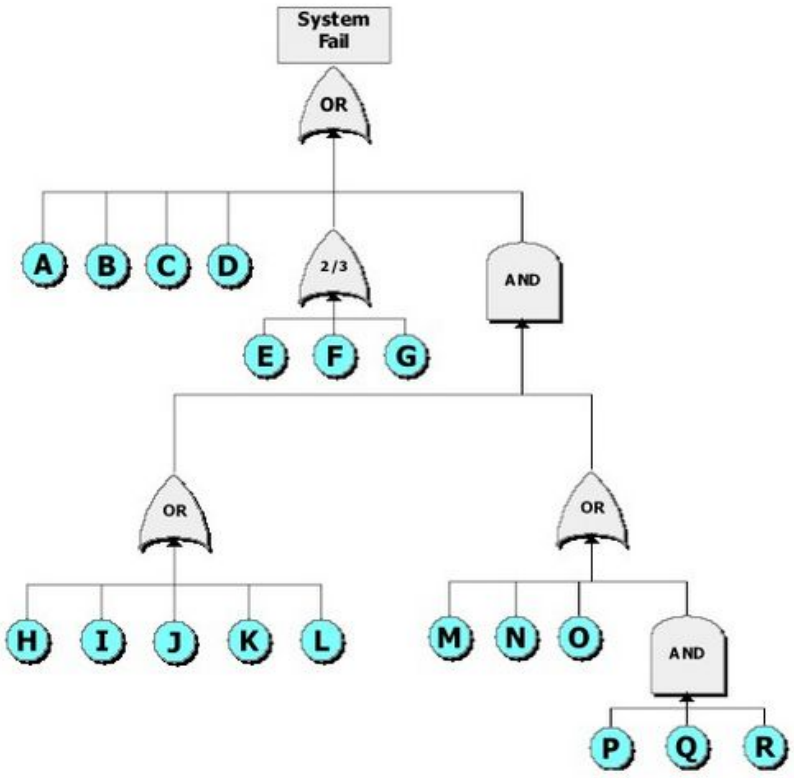

Figure 1. Fault Tree. (SEBoK Original)

A **Reliability Block Diagram** (RBD) (DOD, 1998) is a graphical representation of the reliability dependence of

a system on its components. It is a directed, acyclic graph. Each path through the graph represents a subset of system components. As long as the components in that path are operational, the system is operational. Component lives are usually assumed to be independent in an RBD. Simple topologies include a series system, a parallel system, a *k* of *n* system, and combinations of these.

RBDs are often nested, with one RBD serving as a component in a higher-level model. These hierarchical models allow the analyst to have the appropriate resolution of detail while still permitting abstraction.

RBDs depict paths that lead to success, while fault trees depict paths that lead to failure.

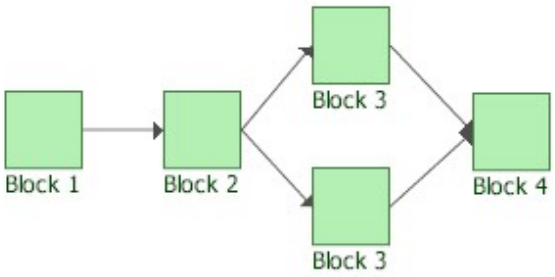

Figure 2. Simple Reliability Block Diagram. (SEBoK Original)

A **Failure Mode Effects Analysis** is a table that lists the possible failure modes for a system, their likelihood, and the effects of the failure. A **Failure Modes Effects Criticality Analysis** scores the effects by the magnitude of the product of the consequence and likelihood, allowing ranking of the severity of failure modes. (Kececioglu 1991)

System models require even more data to fit them well. “Garbage in, garbage out” (GIGO) particularly applies in the case of system models.

Tools

The specialized analyses required for RAM drive the need for specialized software. While general purpose statistical languages or spreadsheets can, with sufficient effort, be used for reliability analysis, almost every serious practitioner uses specialized software.

Minitab (versions 13 and later) includes functions for life data analysis. Win Smith is a specialized package that fits reliability models to life data and can be extended for reliability growth analysis and other analyses. Relex has an extensive historical database of component reliability data and is useful for estimating system reliability in the design phase.

There is also a suite of products from ReliaSoft (2007) that is useful in specialized analyses. Weibull++ fits life models to life data. ALTA fits accelerated life models to accelerated life test data. BlockSim models system reliability, given component data.

Discipline Specific Tool Families

Reliasoft and PTC Windchill Product Risk and Reliability produce a comprehensive family of tools for component reliability prediction, system reliability predictions (both reliability block diagrams and fault trees), reliability growth analysis, failure modes and effects analyses, FRACAS databases, and other specialized analyses. In addition to these comprehensive tool families, there are more narrowly scoped tools. Minitab (versions 13 and later) includes functions for life data analysis.

General Purpose Statistical Analysis Software with Reliability Support

Some general-purpose statistical analysis software includes functions for reliability data analysis. Minitab has a module for reliability and survival analysis. SuperSmith is a more specialized package that fits reliability models to life data and can be extended for reliability growth analysis and other analyses.

R is a widely used open source and well-supported general purpose statistical language with specialized packages that can be used for fitting reliability models, Bayesian analysis, and Markov modeling.

Special Purpose Analysis Tools

Fault tree generation and analysis tools include CAFTA from the Electric Power Research Institute and OpenFTA , an open source software tool originally developed by Auvation Software.

PRISM is an open source probabilistic model checker

that can be used for Markov modeling (both continuous and discrete time) as well as for more elaborate analyses of system (more specifically, "timed automata") behaviors such as communication protocols with uncertainty.

References

Works Cited

American Society for Quality (ASQ). 2022. *Glossary: Reliability.* Accessed on May 9, 2022. Available at http://asq.org/glossary/r.html.

American Society for Quality (ASQ). 2016. *Reliability Engineering Certification – CRE*. Accessed May 9, 2022. Available at http://asq.org/cert/reliability-engineer.

DoD. 2005. *DOD Guide for Achieving Reliability, Availability, and Maintainability*. Arlington, VA, USA: U.S. Department of Defense (DoD). Accessed on May 9, 2022. Available at https://www.acqnotes.com/Attachments/DoD%20Reliability%20Availability%20and%20Maintainability%20(RAM)%20Guide.pdf

Ebeling, C.E., 2010. *An Introduction to Reliability and Maintainability Engineering*. Long Grove Illinois, U.S.A: Waveland Press.

GEIA. 2008. *Reliability Program Standard for Systems Design, Development, and Manufacturing*. Warrendale, PA, USA: Society of Automotive Engineers (SAE), SAE-GEIA-STD-0009.

IEEE. 2008. *IEEE Recommended Practice on Software Reliability*. New York, NY, USA: Institute of Electrical and Electronic Engineers (IEEE). IEEE Std 1633-2008.

Kececioglu, D. 1991. *Reliability Engineering Handbook*, Volume 2. Upper Saddle River, NJ, USA: Prentice Hall.

Laprie, J.C., A. Avizienis, and B. Randell. 1992. *Dependability: Basic Concepts and Terminology*. Vienna, Austria: Springer-Verlag.

Meeker, W., Escobar, L., and Pascual, F. 2022 *Statistical Methods for Reliability Data.* 2nd ed. Hoboken, NJ: Wiley.

Nelson, W. 1990. *Accelerated Testing: Statistical Models, Test Plans, and Data Analysis*. New York, NY,

USA: Wiley and Sons.

NRC. 2015. *Reliability Growth: Enhancing Defense System Reliability.* Washington, DC: National Academy Press. Access May 25, 2023. Available at https://nap.nationalacademies.org/catalog/18987/reliability-growth-enhancing-defense-system-reliability.

O'Connor, D.T., and A. Kleyner. 2012. *Practical Reliability Engineering*, 5th Edition. Chichester, UK: J. Wiley & Sons, Ltd.

ReliaSoft. 2007. *Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA).* Accessed May 9, 2022. Available at http://www.weibull.com/basics/fmea.htm.

Shooman, Martin. 2002. *Reliability of Computer Systems and Networks*. New York, NY, USA: John Wiley & Sons.

Primary References

Blischke, W.R. and D.N. Prabhakar Murthy. 2000. *Reliability Modeling, Prediction, and Optimization.* New York, NY, USA: Wiley and Sons.

Dezfuli, H, D. Kelly, C. Smith, K. Vedros, and W. Galyean. 2009. "Bayesian Inference for NASA Risk and Reliability Analysis", National Aeronautics and Space Administration, NASA/SP-2009-569. Accessed on May 25, 2023. Available at https://ntrs.nasa.gov/citations/20090023159.

DoD. 2005. *DOD Guide for Achieving Reliability, Availability, and Maintainability.* Arlington, VA, USA: U.S. Department of Defense (DoD). Accessed September 11, 2011. Available at http://www.acq.osd.mil/se/docs/RAM_Guide_080305.pdf.

Kececioglu, D. 1991. *Reliability Engineering Handbook*, Volume 2. Upper Saddle River, NJ, USA: Prentice Hall.

Lawless, J.F. 1982. *Statistical Models and Methods for Lifetime Data.* New York, NY, USA: Wiley and Sons.

Lyu, M. 1996. ''Software Reliability Engineering''. New York, NY: IEEE-Wiley Press. Accessed May 9, 2022. Available at http://www.cse.cuhk.edu.hk/~lyu/book/reliability/index.html.

Martz, H.F. and R.A. Waller. 1991. *Bayesian Reliability Analysis.* Malabar, FL, USA: Kreiger.

Meeker, W., Escobar, L., and Pascual, F. 2022 *Statistical Methods for Reliability Data.* 2nd ed. Hoboken, NJ: Wiley.

NRC. 2015. Reliability Growth: Enhancing Defense System Reliability. Washington, DC: National Academy Press.

DoD. 2011. ''MIL-HDBK-189C, Department of Defense Handbook: Reliability Growth Management (14 JUN 2011).'' Arlington, VA, USA: U.S. Department of Defense (DoD). Accessed May 9, 2022. Available at http://everyspec.com/MIL-HDBK/MIL-HDBK-0099-0199/MIL-HDBK-189C_34842.

DOD. 1998. ''MIL-HDBK-338B, Electronic Reliability Design Handbook'' U.S. Department of Defense Air Force Research Laboratory IFTB. Accessed May 9, 2022.Available at http://www.weibull.com/mil_std/mil_hdbk_338b.pdf.

U.S. Naval Surface Weapons Center Carderock Division, NSWC-11. ''Handbook of Reliability Prediction Procedures for Mechanical Equipment.'' Accessed May 9, 2022. Available at http://everyspec.com/USN/NSWC/download.php?spec=NSWC-10_RELIABILITY_HDBK_JAN2010.045818.pdf.

Additional References

IEEE. 2013. *IEEE Recommended Practice for Collecting Data for Use in Reliability, Availability, and Maintainability Assessments of Industrial and Commercial Power Systems*, IEEE Std 3006.9-2013. New York, NY, USA: IEEE.

NIST/SEMATECH Engineering Statistics Handbook 2013. Accessed May 9, 2022. Available at http://www.itl.nist.gov/div898/handbook/.

Olwell, D.H. 2001. "Reliability Leadership." *Proceedings of the 2001 IEEE Reliability and Maintainability Symposium.* Philadelphia, PA, USA: IEEE. Accessed May 9, 2022. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=902431.

Reliability Analytics Toolkit. n.d. web page containing 31 reliability and statistical analyses calculation aids. Seymour Morris, Reliability Analytics. Accessed May 9, 2022. A.vailable at http://reliabilityanalyticstoolkit.appspot.com/

ReliaSoft. 2007. "Availability." Accessed May 9, 2022. Available at http://reliawiki.com/index.php/Introduction_to_Repairable_Systems#Availability.

SAE. 2000a. *Aerospace Recommended Practice ARP5580: Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications.* Warrendale, PA, USA: Society of Automotive Engineers (SAE) International.

SAE. 2000b. *Surface Vehicle Recommended Practice J1739: (R) Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery (Machinery FMEA).* Warrendale, PA, USA: Society of Automotive Engineers (SAE) International.

Relevant Videos

- Availability
- Reliability, Availability

< Previous Article | Parent Article | Next Article >
SEBoK v. 2.10, released 06 May 2024
