Narasi Sridhar *Editor*

Bayesian Network Modeling of Corrosion

Springer

Bayesian Network Modeling of Corrosion

Narasi Sridhar
Editor

Bayesian Network Modeling of Corrosion

Springer

Editor
Narasi Sridhar
Department of Materials Science
& Engineering
The Ohio State University
Columbus, OH, USA

ISBN 978-3-031-56127-6 ISBN 978-3-031-56128-3 (eBook)
https://doi.org/10.1007/978-3-031-56128-3

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

This book is dedicated to the memory of Peter Friis Hansen (1960–2023), who introduced me to Bayesian Networks and to Roger W. Staehle (1934–2017), who encouraged me to think broadly.

Preface

> Any man who sells his soul to synthesis will be a tragic target for a myriad merry darts of specialist critique. —Will Durant, The Story of Civilization

This book provides a synoptic view of our knowledge of corrosion through Bayesian networks. Bayesian Network (BN) is an artificial intelligence (AI) approach that provides a flexible way of modeling a system subject to a complex set of interactions. Unlike other AI approaches, such as neural networks, that seek to establish correlations between observations, BN can incorporate fundamental knowledge of a system and thus attempt to answer causal relationships. Such causal relationships are the key to predicting the performance of systems that can suffer a variety of corrosion-related failure processes. When the exact relationship between factors governing a phenomenon is known through an analytical or numerical model, then calculation of probabilities can be executed by propagating the uncertainties in the factors through the model. However, when the phenomenon is affected by factors that have complex interrelationships and when the models relating the factors to the desired end result are a mix of analytical, numerical, and expert-based relationships, the propagation of uncertainties from factors to the desired result is complex. Furthermore, multiscale models involving a variety of size and time scales may be difficult to handle because the handoffs between various models may be difficult. BN provides a convenient framework for these situations: (1) the exchange between various models is through conditional probabilities enabling independent development of models, (2) analytical, numerical, and statistical models can be included with complex interrelationships, and (3) inputs may be numerical, intervals, logical alternatives (true/false), or ordinal values (ranking). Thus, BN is a flexible tool that can be used in a variety of applications.

Although BN interfaces with our day-to-day lives in a variety of ways, including banking, phone calls, medical diagnosis, etc., its use for modeling an engineering discipline like corrosion is more limited. Although corrosion constitutes only a small number of overall BN publications, there has been a quadrupling of papers in BN's related to corrosion. There are several books on BN for medical, financial, and other

AI applications, but there is no book on the use of BN modeling in corroding systems. This book is aimed at practicing engineers, who wish to use BN to model corrosion processes. The book does not aim to provide a rigorous treatment of the mathematical underpinnings of BN, for which a number of other sources exist. A BN model is a living framework to encapsulate our evolving knowledge of corrosion processes.

The book does not aim to provide a recipe for BN of different systems, as this will be an impossible task. Instead, the focus is on how BN can be used to integrate our knowledge of corroding systems and make predictions of corrosion probability. Corrosion-related problems can be found in all engineering systems. The book provides examples from selected systems, with the hope that similar principles can be adopted for other systems. It is an assemblage of the experience of several people involved in developing and deploying BN for corrosion assessment. Therefore, the book provides a relatively broad perspective to the reader on the potential of BN as well as its limitations.

Chapter 1 introduces risk assessment to provide a context for the evaluation of the probability of corrosion. The chapter concludes with the use of risk assessment in society in terms of risk governance. Chapter 2 presents the principles of Bayesian Network models. The purpose of the chapter is to familiarize the reader with Bayesian networks, requirements to build a network, approaches to developing conditional probability tables, and presentation of results. The perspective is that of someone applying BN to a corrosion problem. Chapter 3 describes models used in corrosion life prediction (mechanistic, semi-empirical, etc.). The process for abstraction/simplification of models for probability assessment is discussed. Chapter 4 describes methods to propagate the distribution in input parameters using different sampling methods. It also describes the Markov modeling approach to propagate the probability of pitting corrosion over time using transition state probability. Chapters 5 through 10 describe the application of BN models in various industries from the perspective of corrosion. Chapter 11 sums up the current status of the use of BN in corrosion systems and possible future directions.

Columbus, OH, USA Narasi Sridhar

Acknowledgements

This book was born out of many years of collaboration with staff at DNV. I, the editor and primary author, specifically acknowledge the contributions of Francois Ayello, Arun Agarwal, John Beavers, Shan Guan, Swati Jain, Vinod Khare, Gerhardus Koch, Guanlan Liu, Andrea Sanchez Sours, Christopher Taylor, and Ramgopal Thodla to many aspects of Bayesian network development. I also acknowledge discussions with Aaron Stenta at Equity Engineering Group that enlightened different aspects of BN modeling, collaboration with Chenxi Liu (Wuhan University of Technology), and discussions with Mariano Kappes, National Atomic Energy Commission, Instituto Sabato (UNSAM-CNEA) on BN for oil and gas production systems. Input from Victoria Gelling and Ted Best (Sherwin Williams) on organic coatings is gratefully acknowledged. Finally, a great debt is owed to my wife, Virginia, for her continued support of my various projects.

Contents

Chapter 1
Introduction: Risk Assessment

Narasi Sridhar

> *Risk and time are opposite sides of the same coin, for if there were no tomorrow there would be no risk.*
> *Peter L. Bernstein, Against the Gods, The Remarkable Story of Risk.*

Risk and Probability

Risk is defined by International Standards Organization (ISO) document on risk management principles [1] as the effect of uncertainty on objectives, the "effect" indicating any beneficial or adverse deviation from the expected. Generally, we associate risk with adverse consequences and reward with beneficial consequences. Indeed, one of the etymological origins of risk signifies 'heading into danger' or 'navigating between different dangers' [2]. All living beings make risk informed decisions, whether that is performed by genetic programming or deliberate analysis [3]. Some form of risk assessment existed even in ancient civilizations [4]. However, mathematical risk assessment methods evolved in the eighteenth century from games of chance. These formal risk assessment methods enabled systematic large scale investments in capital and trade and the growth of modern industrial civilization [2]. Risk is often defined as probability multiplied by consequence. However, this latter definition, while attractive in representing risk as a single value, does not convey the entirety of information needed to make decisions. For example, we often treat a low probability event leading to a high consequence (e.g., a large tsunami affecting a nuclear power plant) differently than a high probability event leading to a low consequence (e.g., an automobile fender bender). These two events may give rise to the same risk number, but are perceived differently. Therefore, a broader definition of risk involves asking three questions [5]: "what can go wrong?", "how

---

N. Sridhar (✉)
Department of Materials Science & Engineering, The Ohio State University,
Columbus, OH, USA
e-mail: nsridhar@mcconsultco.com

N. Sridhar (ed.), *Bayesian Network Modeling of Corrosion*,
https://doi.org/10.1007/978-3-031-56128-3_1

likely is it?", and "how does it affect us?". In mathematical terms, risk is properly defined as a set of triplets:

$$R = \{S_i, f_i, C_i\} \tag{1.1}$$

where, the risk, R, is defined as a function of a set of scenarios, S_i, (what can go wrong?), frequency or probability of occurrence, f_i, (how likely is it?), and consequence, C_i, (how does it affect us?). The scenarios are also referred to in different applications as features, events, and processes (FEP), threats, or hazards. For example, corrosion of a steel pipeline by groundwater causing a reduction in pipe wall thickness and leading to mechanical failure from internal pressure is a scenario. External corrosion of pipeline is considered to be a threat in ASME B31.8S standard [6], but is a part of this scenario. Adding to the confusion in terminology, literature on reliability analysis refer to a hazard rate as the ratio of probability distribution function at any time divided by the reliability up to that point in time. To avoid confusion, scenario is used in this book to refer to a sequence of events leading to an adverse consequence. The term, probability, goes beyond frequency and statistics. Probability is often defined statistically as the limit of the frequency for an infinitely large population of observations. However, probability can also be defined in terms of our confidence in an event, especially if repeated experiments cannot be done for that event to generate a frequency metric. This is the sense of probability used throughout this book.

The cumulative probability of an event is defined as the integral of the probability distribution function over time:

$$F(t) = \int_{x=-\infty}^{x=t} f(x)dx \tag{1.2}$$

Where, x is the value of a factor whose probability distribution function is given by $f(x)$. The reliability function (also called survival function) is defined as the probability of survival up to a certain time, t:

$$R(t) = \int_{x=t}^{x=\infty} f(x)dx = 1 - F(t) \tag{1.3}$$

A risk map can be created that places the different scenarios as illustrated in Fig. 1.1. In this figure, a series of scenarios are analyzed in terms of the probability of exceeding different consequence levels. For example, a scenario could be the external corrosion of a buried pipeline. There may be different consequences associated with such a scenario, such as environmental contamination, property damage, and fatalities. The probabilities of different levels of a consequence, such as environmental contamination, for the scenario of pipeline corrosion can be assembled in the form of a Complementary Cumulative Distribution Functions (CCDF), for example S_1 to S_4 in Fig. 1.1 and compared to regulatory requirements. The curve shows that high consequence events have a lower probability of

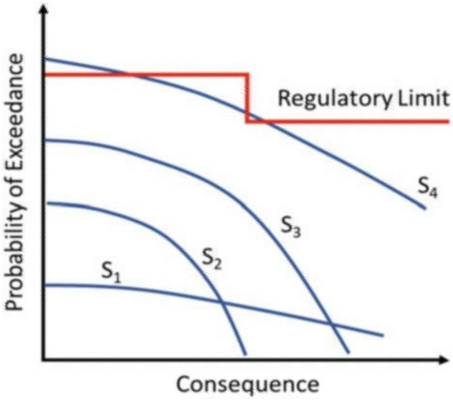

Fig. 1.1 Risk map based on evaluating various scenarios (given as S_1 to S_4) in terms of their probability of exceeding a given value and the consequence levels associated with each probability. Also shown is a risk limit imposed by regulations

exceedance than low consequence events. However, this does not have to be the case for all scenarios [5]. It is possible that the probability of high consequence event, such as damage from construction activity in a densely populated area, may be higher than the probability of a low consequence event of a construction damage at a remote area.

Although Fig. 1.1 depicts smooth curves for the different scenarios, they can also be discrete values represented by segmented lines. Once such scenarios and the associated probabilities and consequences are assembled, they can be compared to regulatory limits or other decision limits imposed by an organization to take mitigation actions.

Different dimensions of risk can be visualized (Fig. 1.2). The term, reliability, refers to the probability that a failure will not occur within a specified time frame. Mathematically, it is defined by Eq. 1.3. In reliability, the consequence is not explicitly considered. Figure 1.2a illustrates reliability by replacing “consequence” with “time”. In scenario RE_1, the system is highly reliable at short time periods, but its reliability decreases rapidly with time (e.g., a non-rechargeable battery). In Scenario $RE_{2,}$ the system has low reliability at short time periods (perhaps due to high initial defects), then stabilizes at a higher value as these defects are fixed, and then decreases at longer times due to aging and wear-out. This scenario is the typical bath-tub curve turned upside down (bath tub curves represent failure probabilities).

Reliability refers to a system’s ability to function as intended over a desired time. The term, safety, on the other hand, refers only to the personal bodily consequence (injury or fatality) arising from the failure of a system, and not its functionality (Fig. 1.2b). A system can be reliable (i.e., perform its intended function), but not safe (the intended function can cause injury even if operated properly). Conversely, a system can be safe, but not reliable. For example, hexavalent chromium containing coating pre-treatment system is reliable, but not safe from a health perspective. Alternative coatings may be safer, but not as reliable. Sustainability (Fig. 1.2c) is the ability of a system to function today without causing harm to future generations or the environment. For example, reinforced concrete can be designed to perform reliably and safely today, but may create severe environmental consequences at a future time due to CO_2 emissions in its manufacturing or safety consequence due to corrosion of reinforcing steel bars. Alternate cement formulations with much lower

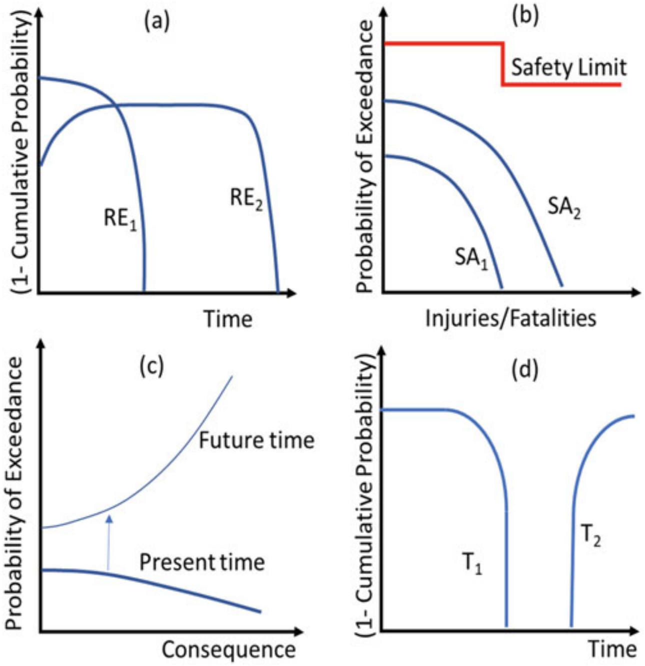

Fig. 1.2 Different dimensions of risk. (**a**) reliability (RE); (**b**) safety (SA); (**c**) sustainability; and (**d**) resilience (T)

CO_2 emissions have been put forward, but have not proven to have the same strength characteristics as Portland cement. Thus, sustainability combines reliability, safety, and environmental consequences. Resilience (Fig. 1.2d) is a term used to describe the ability of a system to recover or survive from a man-made or natural accident. Thus, resilience refers to the conditional probability of a system to function as intended after an adverse event. For example, a flooding event may reduce the functionality of a bridge structure severely (i.e., its reliability decreases as shown by T_1), but it may recover its usage after the floodwater recedes if it is designed to retain its strength after it is exposed to floodwater (T_2).

Corrodible Systems

Why should there be a book dedicated to risk assessment of corrodible systems? After all, there are many books on risk and reliability analyses. The main reason for a book dedicated to corrosion risk management is that the books on risk or reliability assessment, generally, deal with corrosion in a superficial manner or not at all. In many cases, risk is focused essentially on consequences of failure and the probability of failure is assigned a number based on the experience with a certain population of equipment without regard to the actual service environment. In some cases, corrosion is considered as a factor and given an index or a failure probability based on service experience. Another approach, typically used in structural reliability analysis, is the assumption of a continuous corrosion process—for example continuous decrease in the thickness of a structural member or the growth of a defect. The fundamental assumption in the conventional reliability approach is that the corrosion mode does not change with time (corrosion rate may change). However, corrosion can shift dramatically from one mode to another, like a low-grade fever morphing into raging pneumonia, with seemingly small changes in environmental or other factors. The likelihood of new failure modes of structures and systems due to corrosion are increasing with the age of the assets, lack of resources for maintenance, accumulation of contaminants, and external events such as climate change.

Corrosion adversely affects the reliability, safety, sustainability, and resilience of systems. Many international studies have indicated that the cost of corrosion ranges from 1.5% to 5.2% of the Gross Domestic Product (GDP) or Gross National Product (GNP) [7–11] and a significant part (ranging from about 15% to 35%) of this cost can be avoided through proper corrosion management. More importantly, corrosion adversely affects the sustainability and safety of society. For example, a study by Milford et al. [12] showed that CO_2 emission targets for the steel industry can only be met by extending the use of materials and reducing the tonnage of materials used through improved designs. Both these approaches require careful consideration of corrosion.

Risk assessment must be coupled with a deeper understanding of corrosion processes, especially if proper mitigation is desired. The need to develop fundamental, predictive models should, however, be balanced against data and computational needs. No modeling, however sophisticated, can predict the behavior of complex systems, so testing and monitoring are essential. The coupling of sensors to real-time risk assessment is an emerging field that has significant implications on how we select corrosion models. Finally, regardless of how quantitative one gets, risk involves human judgements and actions. Thus, combining the “hard sciences” with “soft” data, such as human-machine interfaces, training, etc. is necessary to develop a comprehensive understanding of corrosion risks.

A risk-informed approach is necessary because as systems age, the degradation of the various components increases the probability of failure and introduces new failure modes. The uncertainty about our knowledge to estimate the failure probabilities also increases with time. An examination of the corrosion literature suggests that many failures were not anticipated when they occurred:

- Stress corrosion cracking of coated and cathodically protected carbon steel pipelines in soil environments was not known prior to a major failure in 1965.
- Stress corrosion cracking of nickel base alloys in high temperature, high purity water was not acknowledged despite research conducted in the 1950’s until many failures in steam generators occurred.

- Extremely high corrosion rate of carbon steel pressure vessel due to boric acid in control rod drive nozzles in nuclear power plants was not known until the Davis-Bessy nuclear power plant inspection revealed such a problem.
- Stress corrosion cracking of steel in methanol and fuel grade ethanol was not known prior to the 1980's and 1990's, respectively.
- Stress corrosion cracking of martensitic stainless steel in high temperature methanol was not known until about 2021.

Even when certain failure modes are anticipated, such as the hydrogen embrittlement of high strength steel bolts, the pertinent information may not have been available, uncertain, or used to assess the risks and take mitigation actions. This has occurred in the case of sub-sea bolts [13] as well as bridges [14]. An aging system loses its resilience because any adverse event, such as an earthquake or flooding, can cripple an already deteriorated system.

There are several qualitative and quantitative approaches to assessing the risks of corrodible systems [15]. There is no one universal approach to risk assessment. The techniques used for risk assessment often depend on the complexity of the system, the specific needs of the stakeholders, regulatory requirements, and resources available. Often, more than one approach is used, starting with a simple, qualitative assessment. Rigorous mathematical methods are not always better than qualitative approaches in providing risk insights, nor are they free of subjectivity. However, quantitative methods do allow one to test the system and assess the effect of assumptions in a consistent manner.

Risk Assessment Approaches

A brief description of the techniques for risk assessment are listed in Table 1.1.

Qualitative Approaches

Qualitative risk analysis methods include check lists, structured interviews, Hazard and Operability (HAZOP) analyses, Failure Modes and Effects Analysis (FMEA), Risk Matrices, and Barrier—Block (Bow-ties). The qualitative approaches are useful in providing an overview of the risk factors related to a system and developing risk mitigation actions. They can be used as a first step in identifying the risk factors. Risk rating systems are used by many organizations to understand and communicate risks to the stakeholders.

Although qualitative methods are good at gaining initial insights into risk factors and as communication tools, they suffer from many serious deficiencies, especially in systems that can suffer from corrosion:

Table 1.1 Risk assessment techniques—description

Risk assessment technique	Description
Job Hazard Analysis (JHA)	A procedure that systematically identifies: (1) job steps, (2) specific hazards associated with each job step, and 3) safe job procedures associated with each step to minimize accident potential. It is also called job safety analysis. (Process Safety Glossary n.d.)
Management of Change (MOC)	Written procedures to manage changes (except for "replacements in kind") to process chemicals, technology, equipment, and procedures, and change to facilities that affect a covered process, must be established and implemented. (Process Safety Glossary n.d.)
Pre-Start-up Safety Review (PSSR)	A safety review that takes place before any highly hazardous chemical is introduced into a process to confirm if design meets specifications, employee training is adequate, operating, maintenance and emergency procedures are in place to name a few[a]
HAZOP (Hazard and Operability Studies)	It is a method recommended for identifying hazards and problems that prevent efficient operation. A standard series of guidewords is used to carry out this exercise[b]
Hazard identification (HAZID)	Hazard Identification is a collective term that encompasses all activities involved in identifying hazards and evaluating risk at facilities, throughout their life cycle, to make certain that risks to employees, the public, or the environment are consistently controlled within the organization's risk tolerance
Bow tie analysis	Bow ties are a simple and effective tool for communicating risk assessment results to employees at all levels. The analysis clearly displays the links between the potential causes, preventative and mitigative controls and consequences of a major incident. Bow tie exercises may be integrated with other HAZID or other semi-quantitative analysis techniques such as Layers of Protections Analysis (LOPA) depending on the level of complexity required
Risk Matrix	A tabular approach for presenting risk tolerance criteria, typically involving graduated scales of incident likelihood on the Y-axis and incident consequences on the X-Axis. Each cell in the table (at intersecting values of incident likelihood and incident consequences) represents a level of risk[c]
Layer of Protection Analysis (LOPA)	Layer of protection analysis (LOPA) is a simplified method of risk assessment that provides the much-needed middle ground between a qualitative process hazard analysis and a traditional, expensive quantitative risk analysis. Beginning with an

(continued)

Table 1.1 (continued)

Risk assessment technique	Description
	identified accident scenario, LOPA uses simplifying rules to evaluate initiating event frequency, independent layers of protection, and consequences to provide an order-of-magnitude estimate of risk
Safety Integrity Level (SIL)	It is the Discrete level (one out of four) allocated to a safety instrumented function for specifying the safety integrity requirements to be achieved by the safety instrumented system
JITF risk model	This is recently developed semi-quantitative risk analysis model by the Joint Industry Task Force (JITF)[d]
Fault Tree Analysis (FTA) and Bayesian Network (BN) Analyses	A method used to analyze graphically the failure logic of a given event, to identify various failure scenarios (called cut-sets), and to support the probabilistic estimation of the frequency of the event. The Fault Tree analysis is a subset of the more general Bayesian Network analysis. The BN analysis links various causative events through conditional probabilities
Failure Modes Effects Analysis (FMEA)	This method tabulates a list of equipment in the process along with all possible failure modes for each item. The effect of a failure is considered with respect to the process[e]
Event Tree Analysis (ETA)	A method used for modelling the propagation of an initiating event through the sequence of possible incident outcomes. The event is represented graphically by a tree with branches from the initiating cause through the success or failure of independent protection layers
Quantitative Risk Analysis (QRA)	A QRA is a formal and systematic approach to estimating the likelihood and consequences of hazardous events, and expressing the results quantitatively as risk to people, the environment or a business
Performance Assessment (PA) or Total System Performance Assessment (TSPA)	Performance Assessment techniques link a variety of process models in a logical sequence of events leading to an ultimate consequent event. The linked models are then run through a probabilistic driver, with each run, called a realization, involving variations of parameters of the models. The resultant CCDF lines are then compared to performance requirements
Bayesian Network (BN) or Bayesian Belief Network (BBN)	This involves first developing a full understanding of the factors and events leading to system performance, creating a graphical description of the cause-effect relationships between these factors in the form of a network of nodes and lines/edges connecting these nodes, and quantifying these relationships (lines/edges) in the form of

(continued)

Table 1.1 (continued)

Risk assessment technique	Description
	conditional probability tables. There are parent nodes that affect subsequent nodes, called child nodes. The BN is a generalized form of fault-tree/event tree approach

[a] U.S. Department of Labor, Occupational Safety and Health Administration, "Process Safety Management" OSHA 3132, 2000

[b] Trevor. A. Kletz, Hazop & Hazan: Identifying and assessing process industry hazards: CRC Press, 2018

[c] CCPS Process Safety Glossary, Center for Chemical Process Safety. https://www.aiche.org/ccps/resources/glossary

[d] API, 2017, Underground Natural Gas Storage: Risk Assessment and Treatment—Natural Gas Storage Well Methodology Guidance for Underground Natural Gas Storage Operators, Prepared by The American Petroleum Institute, The American Gas Association, The Interstate Natural Gas Association of America, 2017

[e] Crowl, D.A., Louvar, J.F., 2002. Chemical Process Safety, Fundamentals with Applications, second ed. Prentice Hall International Series in the Physical and Chemical Engineering Sciences, ISBN 0-13-018176-5

- Qualitative methods do not help us prioritize our actions in an objective fashion;
- It is difficult to judge the importance and sensitivity of different factors and thus evaluate the cost/benefit of mitigation measures;
- It is difficult to make time-based assessments and corrosion is a time-based phenomenon;
- It is difficult to assess failures that occur through a new mechanism. Experts before 1960 would have never assessed the risk of external SCC on pipelines as there was no mechanistic basis for expecting it.

Semi-quantitative Methods

These methods provide a risk score or index, but are essentially qualitative and subjective in developing the risk scores. The overall risk is treated as a sum of weighted values of various factors. Each factor is assigned a weight (positive or negative) and a value. The weights and values may be based on expert input or industry experience, and may be tuned to a specific application. Although the risk scoring approach provides a number for ranking of relative risks, the numbers do not truly follow the laws of probability and they lack predictive value. For example, adding the risk indices essentially assumes that the factors are independent of one another and do not occur together. There is no conditional dependence between different factors.

Quantitative Methods

Component Level Statistical Analysis Methods

Statical treatment of past performance are typically called Quantitative Risk Assessment or QRA, but they are far from the only quantitative method, or even the most useful from a corrosion perspective. This is because the traditional QRA relies on component-level failure statistics (e.g., frequency of valve failures) and cannot assess the effect of process, material, or environmental changes on future failures. However, such aggregated statistics may be useful as a first cut to assessing the probability of failure of a complex system. They can also be used to validate other probabilistic analysis methods.

Reliability and Performance Assessment Methods

The traditional reliability analysis methods compute the probability of a limit state function approaching a defined criterion. The limit state function is defined in structural reliability as a function representing the "Resistance (R)" and "Load (L)". For example, R, also called fragility, may be the tensile strength or fracture toughness and L may be the applied or residual stress on a load bearing member. However, this concept can be broadened to other factors defining the performance of a system (e.g., corrosion potential (E_{corr}) representing the "load" and repassivation potential (E_{rp}) representing the resistance to localized corrosion [16]. A simple limit state for failure may be $\boldsymbol{R - L \leq 0}$, where R and L are regarded as independent of each other. In such a case, if R and L are regarded as random parameters defined in terms of normal distributions, then exact analytical solution for the probability of failure can be attained [17] (Eq 1.4):

$$\boldsymbol{p_f = Normal\left[-\frac{(\mu_R - \mu_L)}{\left(\sigma_L^2 + \sigma_R^2\right)^{0.5}}\right]} \tag{1.4}$$

Note that in Eq. 1.4, L and R can be defined as functions of time, thus yielding the p_f as a function of time. However, in the most general case, the limit state is a complicated function of R and L. Further, R and L may not be independent of each other. For example, in SCC, the resistance, defined as either a crack growth rate or a threshold stress intensity factor, is dependent on loading conditions, such as load mode, strain rate, etc. Finally, both R and L may be complex functions of time. Solutions for such complicated situations may require a variety of simplifications [17–19]. Reliability, which is 1- F(t), where F(t) is the cumulative probability of failure, is not concerned about the consequences of failure. Performance assessment is a term used for assessing the risk of systems, where the probability of failure is coupled to possible consequences [20]. The reliability and performance assessment methods can be generally depicted as shown in Fig. 1.3.

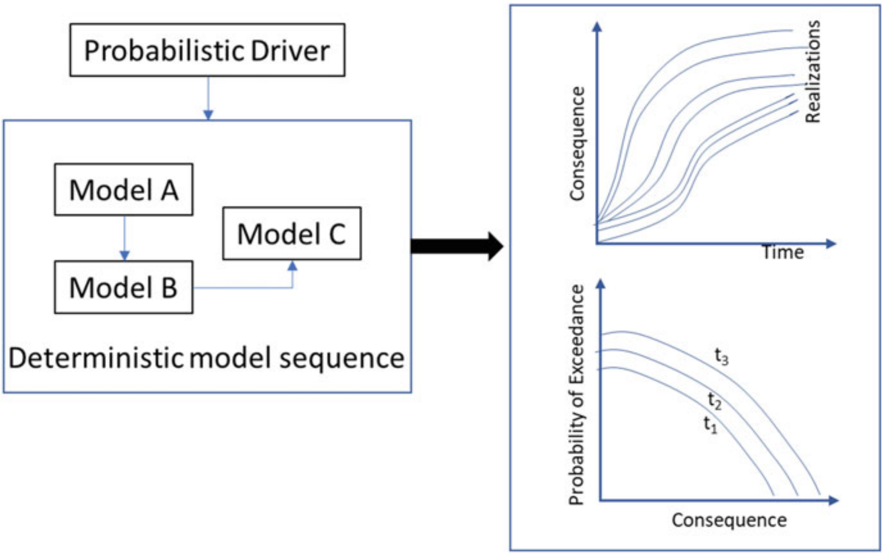

Fig. 1.3 Schematic representation of performance assessment method and resultant predictions

The limit state (Model C) for failure is modeled either through a single or multiple, interconnected models (A and B), resulting a deterministic output. The adjective "deterministic" in this context can be defined as a single output based on single input parameter. Determinism does not imply a physics-based model—deterministic outputs can be obtained from empirical correlations. The whole sequence of models is then computed repeatedly using randomly generated input parameters for the various models, each computational run being called a "realization". The ensemble of realization results are then depicted either as a probability—consequence diagram (sometimes referred to as a spaghetti diagram) or as a cumulative complementary distribution function (CCDF) describing the probability of exceedance versus time. The probability of failure is a sub-part of the performance assessment process and results in a probability of failure versus time plot.

Bayesian Networks

The Bayesian Network (BN) approach also uses a sequence of events/processes. Unlike the case of performance assessment methods, where the whole sequence of processes is run through a probabilistic driver, these processes are represented as probability distributions and they are linked through conditional probability tables (CPT). This allows BN models to be more flexible because probability distributions of individual processes can be computed outside the main BN. Additionally, the approach allows easier insertion or editing of processes at a system level. The BN modeling approach is described in greater detail in the next chapter.

Consequence Analyses

Environmental, health, safety, and financial consequences are parts of risk assessment. Although all consequences can be monetized, one or more types of consequences are given priority in different industrial applications. For example, in radioactive waste disposal, the radiological exposure and health consequence dominates risk assessment. On the other hand, in nuclear power production, all four consequences are evaluated, but health and safety consequences dominate in public consciousness. In liquid hydrocarbon pipelines, environmental and financial consequences are given greater weight, whereas in natural gas pipelines, safety and financial consequences are given greater weight. In some cases, one type of consequence is converted into another. Thus, number of fatalities (a safety consequence) may be monetized in terms of average value of a life in certain situations, e.g., dealing with emissions regulations. The evaluation methods differ in terms of levels of sophistication. Typically, environmental consequences are evaluated using sophisticated plume modeling. On the other hand, safety consequences are described in simpler terms, such as fatalities or injuries. This book does not address consequence analysis.

Risk Governance, Acceptability, and Decision Making

Although this book is about probabilistic calculations, it is important to recognize the context in which probabilistic analyses are performed. Probability analyses are performed to improve decision making under uncertainty and to meet regulatory criteria. These two processes are obviously intertwined.

The regulatory regimes in different countries and industries span the gamut of completely prescriptive to fully risk-based approaches. In a prescriptive regulatory approach, the processes, procedures, designs, and materials are all fully specified. The advantage of this approach is that there is less ambiguity in the requirements—the stakeholders know exactly what standards to meet. However, there are several major disadvantages to a prescriptive approach: the prescriptive approach does not guarantee that system-wide risks are mitigated. Even if specific parts of the system meet prescribed requirements, their interactions may lead to unplanned consequences. Prescriptive approaches discourage innovation and diminish the desire by the industry to do its utmost to reduce risks. It encourages the "check-the-box" mentality, wherein actions are taken to satisfy a regulatory requirement and not necessarily to mitigate risks (a failing even with risk-based approaches). An alternative to the prescriptive regulation is a risk-based regulation. In the risk-based regulations, the overall risk limits are prescribed, but the technology developer and operators are given the freedom to meet these risk criteria using appropriate methods. The methods used to meet the risk criteria must be defensible. The risk-based approaches encourage innovation and place the burden on the technology developer and operator to mitigate risks. However, it is recognized that risk-based approaches involve considerable uncertainties in risk limits, knowledge, and data. Therefore, such regulations also require that the technology developers and operators make the maximum effort to reduce risks beyond the risk calculations. This principle is called As Low as Reasonably Practical (ALARP) or As Low as Reasonably Achievable (ALARA). The ALARP requirement involves performing cost/benefit analyses and determining whether the cost of reducing risks far exceeds the benefit derived from such actions. The ALARA requirement, which arose in the nuclear power industry, requires that actions be taken to reduce the radiation dose rates to individuals as low as possible, even if risk assessment indicates that the dose criteria are met. ALARP and ALARA are fuzzy numerical requirements, but ensure that considerations beyond risk assessments are brought into the discussion of overall system risk. A modification of the risk-based approach is the risk-informed performance-based approach that is espoused by the U.S. Nuclear Regulatory Commission. In this approach, a combination of risk criteria as well as specific system/sub-system prescriptive requirements are imposed. This approach tries to capture the advantages of both prescriptive and risk-based approaches.

Proper risk governance is necessary for a risk-based approach. Governance, as opposed to government, refers to the coordinated actions of the governmental and non-governmental organizations (including industry, standardization bodies, local communities, and other non-profit organizations) in regulating activities of societal interest. More and more, this coordinated, collective action is regarded by economists and policy makers as more effective than governmental organizations alone using the traditional regulatory and legal approaches. Risk governance refers to such a collective decision-making activity performed under uncertainties. Renn [21] states that risk is a human construct—a mental model of the world around us. It is not a real phenomenon, but the anticipation of a real phenomenon. It is linked to a real phenomenon that can cause real harm. Since risk is not a real phenomenon, it cannot be proven or verified like a physical phenomenon. It also depends on societal values—what is perceived as risk by one society may be a natural occurrence or fate by another. Risk governance may consist of many interlocking steps (Fig. 1.4).

1. Pre-estimation: This step brings together the various societal stakeholders in selecting what risks are worth managing. This step frames the risk discussion. For example, certain parts of a society may want to avoid a particular risk by not employing a specific technology (e.g., nuclear power). They may consider the consequences to be too large and reducing the probability of occurrence of adverse events too costly or difficult. Others may believe that a technology has merit (e.g., nuclear power may reduce global warming relative to fossil power) and wish to discuss the pros and cons of managing the technology. The pre-estimation step is a broad discussion of whether we wish to undertake a specific activity.
2. Interdisciplinary Risk Assessment: Risk assessment is a technical activity in which various technical disciplines are brought to model the scenarios, probabilities, and consequences of a set of activities as discussed in previous sections and the rest of this book. Lindoe et al. [22] argue that the interdisciplinary risk

Fig. 1.4 Risk governance framework [21]

estimation consists of two major activities: risk assessment and concern assessment. The former is the technical assessment of risk with respect to corrosion or other adverse phenomena. The concern assessment is the psychological and sociological consequence assessment. It can be further characterized by ubiquity, persistence, reversibility, delay effect, potential for mobilization, perception of familiarity and experience with the hazard, intergenerational equity, perception of fear/dread, perception of personal or institutional control, and confidence in the risk management organizations.

3. Risk Acceptability: This is a highly controversial task that deals with evaluating the tolerability of risk (ToR). Although, the tolerability of risks can be quantitatively defined in terms of number of fatalities, radiation or chemical dose, etc., how these are demarcated in terms of whether a mitigation action should be taken and how to apportion them among different populations for those risks that are not localized are issues that can be debated.

4. Risk management: If the risks are tolerable, no further action needs to be taken other than continued monitoring. If the risks are intolerable, risk avoidance may be followed (but avoiding a technology may carry its own risks). If the risks fall between these two endpoints, risk mitigation measures must be taken.
5. Risk Monitoring and Control: Risk evaluation, at least as a technical discipline, tends to be model oriented as different scenarios are developed and the probabilities and consequences are calculated. However, models are partial representations of reality and no matter how rigorous and comprehensive a model is, there are aspects of reality that cannot be captured or may not be known. In terms of psycho-sociological aspects, risk evaluation is even more difficult and ambiguous. Therefore, continued monitoring of the systems and actions is essential to update our risk evaluation. Such monitoring can be using physical means (sensors, etc.) or social means (survey, etc.). Control measures must be in place to manage risks if monitoring indicates potential risk elevation due to unforeseen circumstances.
6. Communication: Open communication is key to all the previous steps. Communication increases the confidence in the risk governance activities. Communication enables better risk evaluation by incorporating inputs from all knowledge holders in the risk assessments. Finally, communication raises the awareness of risks and helps in the monitoring and control of risks.

Acceptability of Risk

We accept many risks subconsciously in our lives because to evaluate every potential hazard consciously would paralyze us as individuals and as a society. However, our sub-conscious acceptance of a hazard is rooted in sociological and cultural circumstances. For example, in advanced countries, we do not think consciously about the hazards of getting in a car and driving, whereas we do think consciously about the risks of hiking in a wild place. In contrast, someone in a primitive society may have misgivings about getting in a car, but not about walking in a wild place. We may think consciously about the hazards of air travel despite the statistical evidence that car travel kills more people than air travel. This is due to the psychological phenomenon of giving a lower risk tolerability of multiple deaths in a single accident than the same number of total deaths in separate individual accidents. It may also be due to our feeling of greater control over our cars than an aircraft controlled by third parties. Acceptability or tolerability of risk is a value judgement placed by individuals, companies, and societies. Despite the great sophistication in the quantitative assessment of risks, the acceptance of that risk is subject to many unquantifiable factors.

An approach that is broadly used to classify risks by society is shown in Fig. 1.5 [23]. In the U.K. HSE, a risk of fatality to individuals of 10^{-6} per year is considered acceptable for both workers and the public. It must be noted that this number is essentially the probability of fatality. This risk is considered to be far below the

Fig. 1.5 Overall framework for risk acceptability as described by the U.K. Health and Safety Executive

typical risk the public undertakes in its everyday activities. On the other hand, a risk of fatality of 10^{-3} per year to an individual worker is considered unacceptable and forms the upper boundary of tolerable risk. To account for the societal aversion of multiple fatalities from a single accident, the HSE sets the tolerability limit for risk involving more than 50 fatalities to 2×10^{-4} per year. For the general public, on whom a risk is imposed, the limit of tolerability of risk is set at 10^{-4} per year.

However, HSE does not limit the definition of risk tolerability to fatalities alone, but considers other consequences, such as environmental damage, in evaluating total risk to an activity. In this book, risk governance and tolerability will not be discussed in detail. However, the concepts outlined above provide the framework in which corrosion risk assessment should be conducted.

Summary

The concept of probability is an essential element of evaluating risk. Probability is defined in this book as our confidence in an outcome and can be evaluated using a variety of qualitative and quantitative methods, depending on the objective of the evaluation. The book will elaborate the quantitative assessment of corrosion probability using a Bayesian network approach. Once risk is evaluated, the acceptability of risk and how it is managed is a dictated by societal decisions. The acceptability of the probability of an adverse event, such as fatality, is defined in some risk governance documents and regulations.

References

1. XXX31000, I, *International Standards Organisation, Risk Management – Principles and Guidelines* (ISO, Geneva, 2009)
2. L. Bernstein Peter, *Against the Gods: The Remarkable Story of Risk* (Wiley, New York, 1996)
3. D. Kahneman, *Thinking, Fast and Slow* (Macmillan, 2011)
4. V.T. Covello, J. Mumpower, Risk analysis and risk management: An historical perspective. Risk Anal. **5**(2), 18–120 (1985)
5. S. Kaplan, B.J. Garrick, On the quantitative definition of risk. Risk Anal. **1**(1), 11–27 (1981)
6. B31.8S-2004, A, *Managing System Integrity of Gas Pipelines, ASME Code for Pressure Piping, B31, Supplement to ASME B31.8* (The American Society of Mechanical Engineers, New York, 2004)
7. G. Koch, J. Varney, N. Thompson, O. Moghissi, M. Gould, J. Payer, *International Measures of Prevention, Application, and Economics of Corrosion Technologies Study* (NACE International, Houston, 2016)
8. G.H. Koch, M.P.H. Brongers, N.G. Thompson, Y.P. Virmani, J.H. Payer, *Corrosion Cost and Preventive Strategies in the United States* (Federal Highway Administration, 2001), p. 773
9. R. Bhaskaran, N. Palaniswamy, N.S. Rengaswamy, M. Jayachandran, A review of differing approaches used to estimate the cost of corrosion (and their relevance in the development of modern corrosion prevention and control strategies). Anti-Corros. Methods Mater. **52**(1), 29–41 (2005)
10. R. Bhaskaran, N. Palaniswamy, N.S. Rengaswamy, M. Jayachandran, Global cost of corrosion – A historical review, in *Corrosion: Materials*, ed. by S.D. Cramer, B.S. Covino Jr., (ASM International, 2005)
11. B. Hou, X. Li, X. Ma, C. Du, D. Zhang, M. Zheng, et al., The cost of corrosion in China. npj Mater. Degrad. **1**(1), 4 (2017)
12. R.L. Milford, S. Pauliuk, J.M. Allwood, D.B. Müller, The roles of energy and material efficiency in meeting steel industry CO2 targets. Environ. Sci. Technol. **47**(7), 3455–3462 (2013)
13. Bureau of Safety and Environmental Enforcement, O.o.O.R.P., *QC-FIT Evaluation of Connector and Bolt Failures Summary of Findings, QC-FIT Report# 2014–01* (2014)
14. H. Townsend, K. Frank, B. Brignano, C. Choi, Hydrogen embrittlement testing and results of full-size ASTM A354 grade BD rods in the SFOBB. Bridge Struct. **11**(4), 117–130 (2015)
15. 31010, I.I, *International Electrotechnical Commission, Risk Management – Risk Assessment Techniques* (Geneva, 2009)
16. O. Pensado, R. Pabalan, Probabilistic methodology to estimate environmental conditions for localized corrosion and stress corrosion cracking of Alloy 22 in a high-level radioactive waste repository setting. J. Nucl. Mater. **381**(3), 231–241 (2008)
17. R.E. Melchers, A.T. Beck, *Structural Reliability Analysis and Prediction* (Wiley, 2018)
18. O. Ditlevsen, H.O. Madsen, *Structural Reliability Methods*, Internet Edition 2.2.5 edn. (Wiley, 2005)
19. B.H. Thacker, D.S. Riha, S.H.K. Fitch, L.J. Huyse, J.B. Pleming, Probabilistic engineering analysis using the NESSUS software. Struct. Saf. **28**(1–2), 83–107 (2006)
20. S. Mohanty, R. Codell, J.M. Menchaca, R. Janetzke, M. Smith, P. LaPlante, et al., *System-Level Performance Assessment of the Proposed Repository at Yucca Mountain Using the TPA Version 4.1 Code* (Center for Nuclear Waste Regulatory Analyses, San Antonio, 2002), p. 130
21. O. Renn (ed.), *Risk Governance – Coping with Uncertainty in a Complex World* (Earthscan Risk in Society Series, R.E. Lofstedt, Earthscan, London, 2008)
22. P.H. Lindoe, M. Baram, O. Renn (eds.), *Risk Governance of Offshore Oil and Gas Operations* (Cambridge University Press, 2014)
23. F. Bouder, D. Slavin, *The Tolerability of Risk: A New Framework for Risk Management* (Taylor & Francis, 2013)

Chapter 2
Bayesian Network Basics

Narasi Sridhar

> *Causal questions can never be answered by data alone. They require us to generate a model of the process that generates the data.*
> *– Judea Pearl and Dana Mackenzie, The Book of Why*

Introduction

Scientists and engineers are trained in the use of statistical techniques to understand the significance of their findings and correlate the results to factors they controlled in their experiments or observed in the field. The basis for statistical techniques is that there is an inherent variability in the measured results superposed on possible causative factors. The inherent variability in the measured values itself is a result of myriad causative factors that cannot be easily quantified. For example, a coin toss provides variability in the results that is considered random or stochastic, but it is not truly random. The result is caused by variations in tossing mechanics, atmospheric parameters, differences in the weight of the coin faces, etc. When these causes become numerous and hard to quantify, they can all be combined into a random variability. Such randomness is called aleatory uncertainty, derived from the Greek word *alea* for a dice. The variability arising from our lack of knowledge of the fundamental forces shaping a phenomenon is called epistemic uncertainty. Indeed, one can argue that, except for quantum mechanical phenomena, there is no true aleatory variability. Aleatory uncertainty is just the result of epistemic uncertainty. This relationship between aleatory and epistemic variability is illustrated in a highly readable book on the game of roulette by Bass [1]. The chances of winning in roulette wheel can be increased by implementing the physics of the ball movement. Thus, stochastic reasoning may sweep much under the rug.

N. Sridhar (✉)
Department of Materials Science & Engineering, The Ohio State University,
Columbus, OH, USA
e-mail: nsridhar@mcconsultco.com

N. Sridhar (ed.), *Bayesian Network Modeling of Corrosion*,
https://doi.org/10.1007/978-3-031-56128-3_2