Chapter 5: Preventing Life-Cycle Risks

The simple truth is, "first parts fail, then machines stop."[1] It follows that stopping parts from failing stops equipment failures. Broken machines are the end of a chain of causes and effects beginning with a failure trigger introduced at some point in the life cycle. It could be a defect built into a part or a bad event that occurred during the machine's service life. To get outstanding equipment reliability, you need to eliminate defects and stop failure-initiating events from happening to parts. Prevent the first cause of the final cause of a part's failure, and repeatedly do that for all machines in your operation, and you are guaranteed to create world-class plant and equipment reliability.

Equipment is designed using drawings, images, and words. Designers turn imagination into blueprints, specified materials, and written instructions. Parts are made and put together in working assemblies, and the assemblies brought together into machines and equipment. The designer expects a machine to be used as it was designed to be used: all parts stay within positional tolerance at operating conditions; lubricant is perfectly clean and in the required chemical composition; the stresses and strains in components stay a factor of safety below the capability of the selected materials of construction; and loads and forces act through the paths designed for them to follow. Few designers realize, unless they've worked for many years doing equipment maintenance, how such demands can turn their vision into an owner's nightmare.

From the designer's perspective, there is no reason that the equipment should fail unexpectedly because it was designed to work properly, with each part working within the physical limits of its materials of construction. Yet plant and equipment fail often. When they do, the failure can cause unbelievably huge business-wide losses—and even many deaths. To understand how defects in equipment arise, you need to know the activities involved in design, manufacture, storage, installation, operation, and maintenance. Figure 5.1 shows summary steps for each life-cycle process that affects equipment reliability.

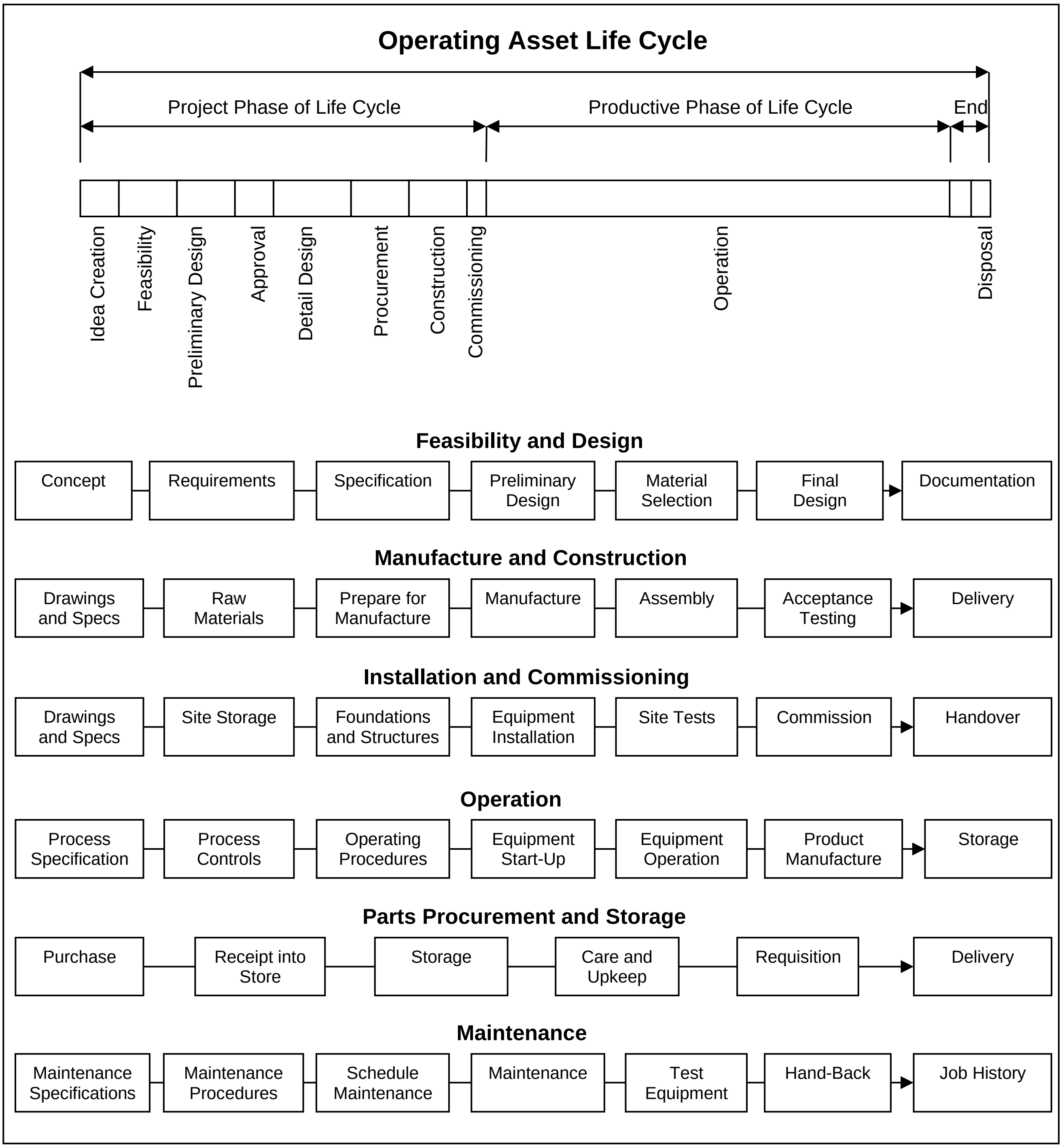

Figure 5.1—Life-Cycle Process Chains Are Complex

The simple flow diagrams hide the great complexity in each process. Each step has its own processes and subprocesses and an accompanying suite of procedures. There are hundreds and even thousands of opportunities for failure-causing variations to arise during the life cycle. Every step involves numerous activities and actions requiring many decisions and choices performed to varying degrees of uncertainty. Throughout the life cycle, there are many opportunities for small errors, misunderstandings, and inconsistencies. Randomness and variability introduce defects and failure causes. Faults and discrepancies accumulate, leading to microstructure loads and conditions outside the equipment's design parameters. Machine parts get stressed and strained, and at some point, an overly excessive load, or simply the accumulated fatigue from many loads (the proverbial straw that broke the camel's back), causes a part's failure. Each cause can be the start of a defect and all the future business problems and losses it brings. To stop plant breakdowns, you need to stop defects and failure causes by removing the variations that create them. If you want to have extraordinarily reliable equipment, you need extraordinary certainty that there will be no flaws in the life-cycle processes that impact your equipment's reliability.

Raising the "R"

To get reliability and maintenance excellence, three things ensure success.

1. Prevent stress, fatigue, and degradation of your critical parts' microstructure—your machines only stop when their parts fail.
2. Control work quality and task accuracy throughout the life cycle of your equipment parts to protect against human knowledge and skill errors introducing defects. Mistakes, misunderstandings, and ignorance during design, manufacture, selection, storage, installation, operation, and maintenance cause most plant availability and equipment reliability problems.

3. Build life-cycle asset management, supply chain, operation, maintenance, and reliability processes that deliver risk-prevention, defect-elimination and zero-failure strategies and practices to equipment parts.

Prevent part failures, and you will create highly reliable machines. The health of your equipment parts has a fatal impact on your chance for operational excellence. Minimizing the stresses that happen to the assemblies and parts in your equipment requires using Physics of Failure knowledge to eradicate the causes of failure. Stress in a part is minimized by preventing microstructure damage (e.g., bending, twisting, shearing, impact, excess pressure, etc.) and material removal (e.g., corrosion, chemical attack, abrasion, etc.). You can derive the minimal reliability excellence strategy by considering an individual part's Physics of Failure mechanisms.

World-class reliability is not an accidental result; there is little luck involved in having an operation with outstanding equipment performance, low-cost production, and a healthy and safe workplace. You start the climb to world-class reliability by introducing the causes of reliability into your business processes. Then you teach your people how to do them expertly. Your company will get high equipment reliability when it uses the right processes, techniques, and methods that "raise the R"—reliability, the chance of success—of every step in every business process across the life cycle of your equipment. Your aim is to stop unwanted variation—the archenemy of reliability—so that only success remains. Figure 5.2 symbolizes intentionally raising the reliability of every process step, activity, and part. You move reliability from its current boxed-in performance and make it grow. You remove the risks in a step, activity, or part so that the chance to start a failure is reduced by orders of magnitude. Once the chance of failure is eliminated or greatly reduced, what is left is a vastly improved chance of success. The math behind this logic is seen in Formula 5.1—when success is certain failure cannot happen.

Formula 5.1

Chance of Failure = 1 – Chance of Success

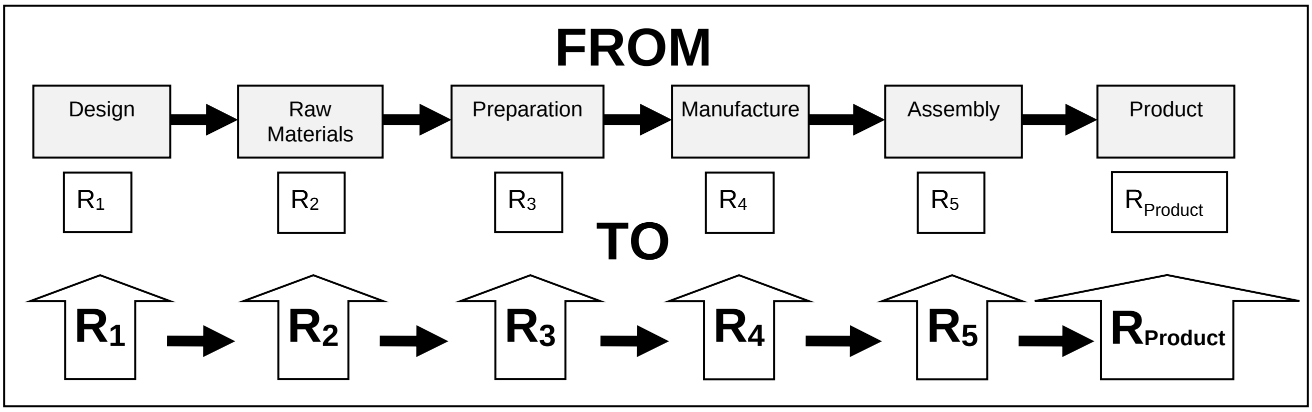

Figure 5.2—Raise the R with Higher Reliability in Every Process Step and Equipment Part

The Plant Wellness Way EAM Methodology

All that you have read so far needs to be put into a methodology for delivering the right project design, operating practices, and maintenance methods to produce lifetime reliability. World-class asset management, maintenance, and reliability need defect-eliminating processes, techniques, and methods used throughout the life cycle of plant and equipment. Operating plants and physical assets rely on us to get the working conditions right for them lifelong. The best strategies for improving reliability are those that extend the failure-free life of parts. When machine parts live and work in conditions that limit microstructure stresses to values that deliver long operating lives, they will return maximum reliability. You must kill all the “gremlins” in the life-cycle.

<u>Stress-to-Process Life-Cycle Asset Management Model</u>

The Plant Wellness Way is life-cycle asset management of parts and components, not plant and equipment. Its driving principle is the elimination of microstructure failure by reduction and prevention of stress in component materials of construction. It uses Physics of Failure knowledge to identify how each working component can suffer stress or degradation, after which you develop defect-eliminating activities and zero-breakdown strategies to use during the phases of the life cycle that prevent all the failure-initiating events from happening. The analysis is based on risk-elimination and reliability-creation principles that ensure you use the right answers to get operational and maintenance excellence.

The enterprise asset management, maintenance, and reliability methodology used in the Plant Wellness Way is called the Stress-to-Process Model. Figure 5.3 introduces the Stress-to-Process Model for asset management success. With it, you engineer and install world-class reliability in your company. The Stress-to-Process life-cycle management methodology lets you discover exactly how to produce world-class reliability and embeds the best solutions into your organization's processes. It is a scientifically based approach for designing and building the least cost, least manpower, and most successful enterprise asset management system. It gets you to build and use the life-cycle processes and practices that create healthy, long-lived parts and thereby create outstandingly reliable equipment. It turns a company into an Accuracy Controlled Enterprise (ACE) by making you "lock" the best solutions for outstanding equipment reliability into a life cycle long, company-wide quality assurance system that eliminates operating risks. Figure 5.4 is a more detailed view of the bottom-up Plant Wellness Way Stress-to-Process Model. From the causes of the causes of component stress, you design the business processes you use to reach the pinnacle of world-class plant and equipment reliability.

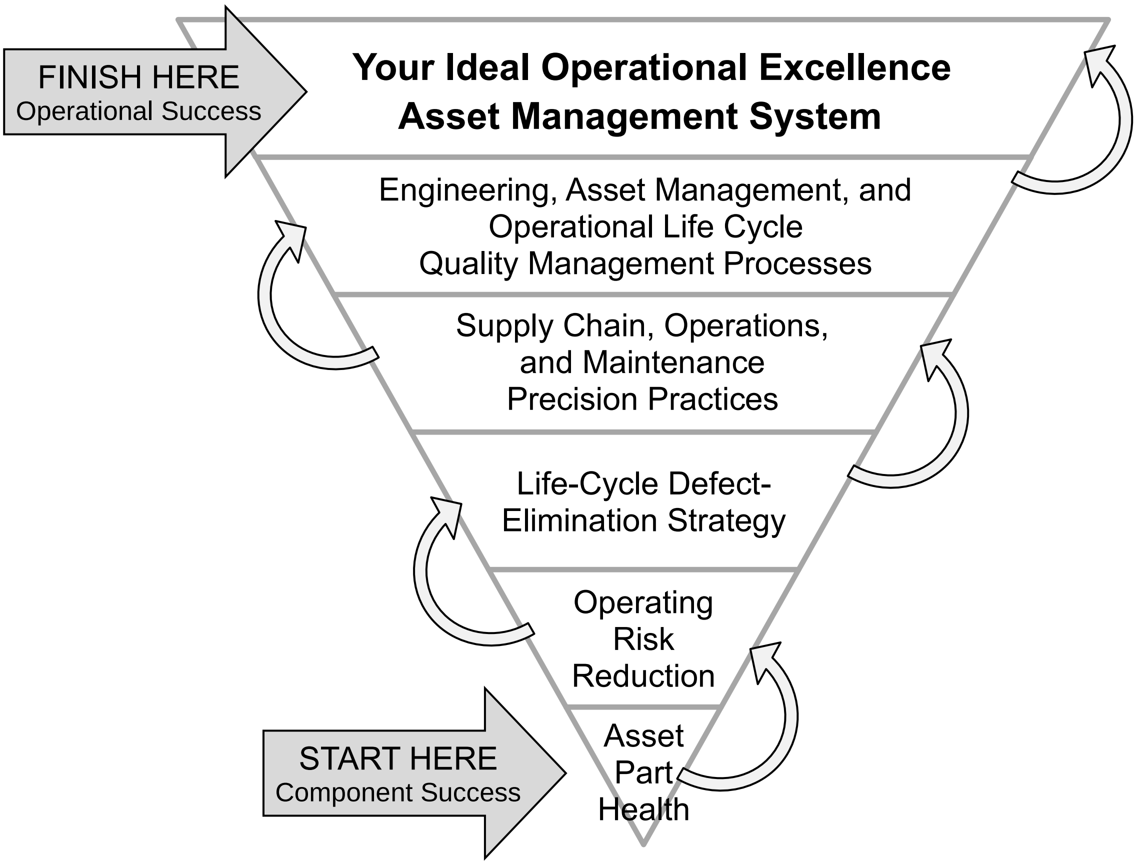

Figure 5.3—Atomic Stress to Business Process Asset Management Model

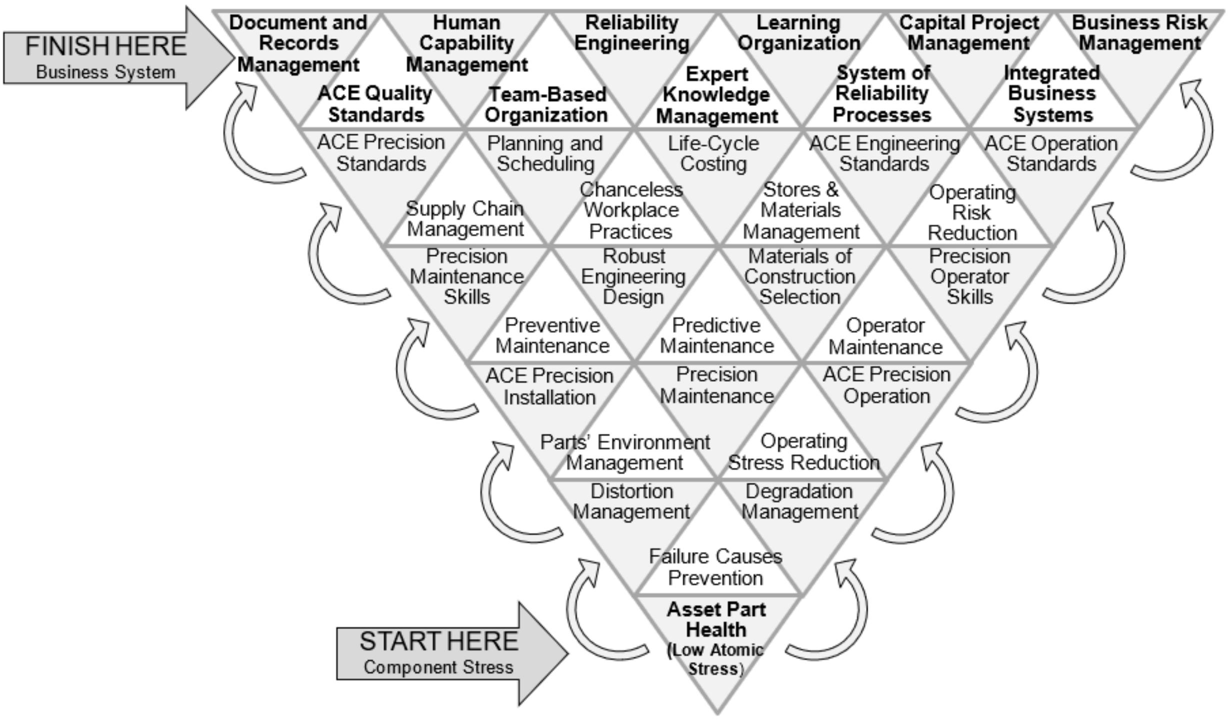

Figure 5.4—Plant Wellness Way: Up to the Top of World-Class Reliability]

Plant Wellness Way EAM System-of-Reliability

All physical asset failures can be grouped into one of two categories: microstructure distortion or atomic degradation. Distortion causes parts to suffer such high stress or fatigue that their microstructure fails. Whereas, when a part degrades, the material of construction is attacked by elements in the contacting environment. Physics of Failure methods let us analyse equipment for situations that cause a part's atomic structure to disintegrate and/or its microstructure to suffer excessive stress. You identify potential causes of microstructure distress and then institute the fewest life-cycle activities needed to keep each part at its highest reliability, so your operating plant and equipment reaches the highest availability.

Using the Stress-to-Process framework, you derive the activities to put into your financial management, project engineering, supply chain, warehousing, maintenance, and operational management processes to prevent the deformation and degradation of each part in your machines and equipment. You engineer a life-cycle asset management system—a system of reliability—to deliver parts with long, failure-free lives. With the right processes from bottom to top in your company, you naturally get the world-class asset maintenance and reliability results needed for operational excellence.

The five foundational business and reliability understandings used to improve equipment reliability the Plant Wellness Way are as follows:

1. The costs of defect and failure are directly connected to the number and size of risks carried by your business—the more risks tolerated, the greater the opportunity for errors and the greater the costs, losses, and waste that eventually accrue.
2. Failure events do not only have localized consequences; rather, failure costs surge company wide. Your business always pays every cent for all the costs of its failures.
3. All organizations, machines, and work are series processes, and the success of every series process depends on the success of each individual step.
4. There are natural physical limitations in the materials used to make your plant and equipment. Throughout their microstructure, the stresses from imposed loads must always stay well within the elastic deformation range of the materials of construction.
5. Variation away from the standard for best results produces defects that create failures. For world-class reliability, use only processes throughout a component's life cycle with natural variation within the outcomes that deliver excellence.

Figure 5.5 is an overview of the Plant Wellness Way methodology. It is the structured approach you will follow to arrive at the right design, operating, and maintenance strategies for maximizing equipment reliability. The methodology takes a life-cycle view of plant and equipment and recognizes that a lifetime of high equipment reliability depends on the reliability of the individual parts in a machine. It helps you develop the right engineering, project selection, plant construction, and operational and maintenance plans and practices for failure-free plant and equipment.

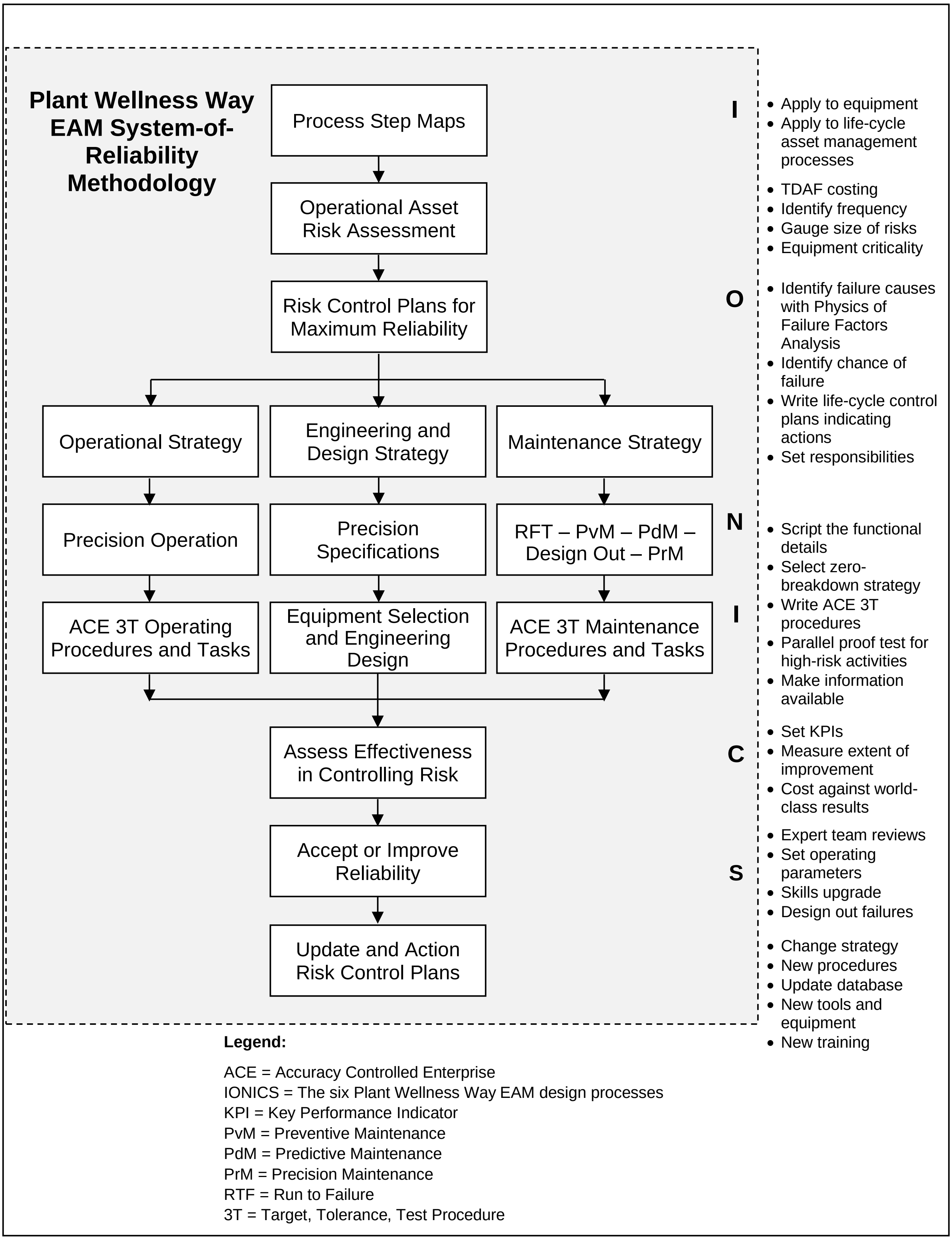

Figure 5.5—Remove Operating Risks with the Plant Wellness Way Methodology]

You are always trying to get the longest life out of your parts. If the parts do not fail, the equipment cannot fail. You improve your equipment reliability by eradicating, reducing, and controlling the risks to parts throughout their lifetimes. With fewer risks to parts, there will be fewer failures. This driving philosophy makes you continually reduce the chance of defects in critical working parts. These are the parts that stop your machines if they fail. By relentlessly reducing the likelihood of things going wrong in working parts, equipment reliability naturally improves because the parts carry lower and lower chances of failure. The methodology forces you to work out how to prevent risks to operating components arising in the first place anywhere in the life cycle. It then requires you to implement risk elimination and prevention by embedding the solutions wherever in the life cycle they are most effective, including project feasibility, engineering design, plant construction, supply and procurement, and operations and maintenance.

From a Plant Wellness Way perspective, if you must repair your equipment, then the business processes used to deliver equipment health and well-being have failed. Your machines are not well if you must continually correct problems and fix random failures. In the Plant Wellness Way, you do not maintain and repair your equipment in the traditional way. Instead, you create the right conditions for your operating plant and machines to stay well throughout their life cycles and permanently sustain those conditions. You produce lasting equipment health by causing components to have high reliability and removing the life cycle causes of their failures. You instigate and forever continue the ideal health and wellness requirements and practices that your plant and equipment parts need for failure-free operation.

Plant and equipment wellness is not possible if your maintenance is failure focused. Companies using preventive (PvM), predictive (PdM), and run-to-failure (RTF) maintenance strategies easily default to being failure focused. To achieve “wellness,” you must create and endlessly sustain component health. Successful reliability creation solutions and methods that cause equipment parts to be healthy must be designed, installed, and continually practiced in all business processes and activities. In this way, world-class reliability performance becomes a natural business habit and the organization's culture.

Asset Management Strategy from Physics of Failure Factors Analysis

You derive the minimal reliability excellence strategy for a machine by considering each part's Physics of Failure mechanisms. First the causes that can destroy a part's microstructure are established, and then the types of events causing those factors are identified. Once the causes of the causes are found, you determine the most suitable and effective solutions to eliminate or prevent each one and install them in appropriate procedures used during the part's life cycle.

The microstructure of metals and plastics are failed in the ways listed in Table 5.1. These principal factors of materials breakdown are called the Physics of Failure Factors. There are not that many ways to physically destroy atomic bonds and cause solids to come apart. Occasionally, unique peculiarities exist that are specific to the atomic structure of a group of solids. When you encounter such a unique factor, add it to the POF Factor table for that group of materials.

Physics of Failure Factors for Solid Materials		
No.	**Metals**	**Plastics**
1	Compressive force crushes the microstructure until it collapses	Compressive force crushes the microstructure until it collapses
2	Tensile force stretches the microstructure until it separates	Tensile force stretches the microstructure until it separates
3	Shear force tears the microstructure until it rips	Shear force tears the microstructure until it rips
4	Cyclic stress fatigue from compressive, tensile, and/or shear forces	Cyclic stress fatigue from compressive, tensile, and/or shear forces
5	Melt or overheat the microstructure	Melt or overheat the microstructure
6	Separation of microstructure (e.g., dislocation)	Separation of the microstructure
7	Material missing from microstructure (e.g., cavities)	Material missing from microstructure (e.g., cavities)

8	Material mechanically ripped from the microstructure	Material mechanically ripped from the microstructure
9	Foreign inclusion in the microstructure	Foreign inclusion in the microstructure
10	Electromagnetic radiation destroys atomic bonds	Electromagnetic radiation destroys atomic bonds
11	Chemical reaction destroys atomic bonds	Chemical reaction destroys atomic bonds
12	Crystal lattice attack of microstructure grain boundaries	Depolymerization decomposition

Table 5.1—POF Factors That Fail the Microstructures of Solids

There are, however, numerous causes that can produce the mechanisms that fail microstructures. Table 5.2 lists a range of causes for three types of microstructure failure. Each principal microstructure failure factor has multiple failure-causing mechanisms that can arise to produce circumstances in which the atomic structure of the item is destroyed. Parts will fail any time their structure is not strong enough for the stresses inside them. The events that can produce those stresses number in the hundreds and even thousands of opportunities during a part's lifetime.

Mechanisms Causing Microstructure Failure			
No.	**Forces or energy cause microstructure damage**	**Microstructure mechanically damaged or destroyed**	**Chemical reaction destroys atomic bonds**
1	Pressure	Overloaded	Foreign inclusion in material of construction
2	Overloaded	Punch (impact load on small area)	Corrosion (pitting, galvanic, crevice, etc.)
3	Pressure hammer	Hammer impact, dent	Acidic atmosphere
4	Expansion	Gouge	Product ingress/egress
5	Unbalance	Abrasion (wear material away)	Chemical reaction
6	Gouge	Solid object impact (e.g., vehicle, lifting chains)	Oxidisation
7	Hydraulic shock (water hammer)	Impingement (jet of fluid)	Dissimilar materials
8	Physical abuse	Detach-debond-delaminate	Hygromechanical (moisture absorption)
9	Acts of God/acts of Nature	Physical abuse	Inclusions in contacting process
10		Friction	Crystal lattice attack
11	Electrical discharge	Physically deformed (bend, twist, squash)	Solar radiation: UV and thermal effects
12		Erosion	Hydrogen attack/embrittlement
13			Stress corrosion cracking
14			Chemical attack
15			Electrical discharge

Table 5.2—Wide Range of Cause Mechanisms that Fail Microstructures

For example, free water in oil will lead to roller bearing failure by thinning the lubricant film between the raceway and rolling elements until there is metal-to-metal contact. Once moving metal parts hit against each other, their surfaces are ripped away, or they crack. But free water can only be present in oil if it gets into the lubricant. Prevent water ingress and there is no cause for the bearing to fail from watery oil or grease. When you look across the life cycle of lubricating oil, there are dozens of ways for water to get into a machine's lubricant. Water can get into oil if it is put in by the oil manufacturer; if the equipment maker puts water in the machine during cleaning or testing; if rain gets inside the equipment during storage; if rain or sea water gets inside the equipment during shipping or road transport; if it is flushed into the machine during commissioning or maintenance; or if it leaks into the sump from inside the equipment. Water could also come from rain falling on unsealed oil drums; from capillary action down the threads of bungs on sealed drums when water pools on the lid; by hosing down equipment and water pressure pops open a shaft seal; from condensing humidity drawn through a breather; from leaking cooling system pipework; and by many other unintended events that can happen over an equipment's lifetime. When you adopt the Plant Wellness Way, the answers that prevent each of those risks become the reliability creation strategy you put into place throughout your business, along your supply chains, and across the life cycle.

The technique used to discover the causes of the causes of microstructure damage is called Physics of Failure Factors Analysis. It is the starting point in the Stress-to-Process Model to discover the ideal life-cycle reliability strategy for each part. You work from the parts' microstructure properties up to the correct business processes needed to sustain outstanding component longevity. By finding all ways that a component's microstructure can fail, you can proactively select the correct life-cycle strategies to eliminate the risk every time it might arise. You use degradation and deformation prevention practices to keep every part healthy, well, and safe throughout its life. You apply high-reliability methods and work quality assurance to install, maintain, and operate the part. You train people in the right reliability techniques and solutions. You stipulate the supply chain risk controls that your vendors must use to protect your physical assets' lives. Thus, you intentionally design outstanding and lasting plant and equipment reliability into your business.

Plant and Equipment Risk Identification

Because machines fail after their critical working parts fail, the Plant Wellness Way requires you identify the parts in a machine that will stop it from operating when they break. These parts are investigated using Physics of Failure Factors Analysis to find all their life-cycle risks. Unacceptable risks are eliminated, and when that is not possible, the risks are controlled and managed with the least number of suitable engineering, operating, and maintenance strategies. Your intention is to reduce the chance of equipment failure to less than once in a span of three times the service life of the equipment in the operation. For example, for equipment expected to be in production for 20 years, the likelihood of a failure incident is to be less than a 1-in-60-year event. For an asset that is expected to be in operation for just 5 years, the target is no more than a 1-in-15-year event. Every critical component in the equipment must therefore have a far lower chance of failure for their combined odds to produce the required equipment likelihood of failure.

In all cases, the decision to apply component risk-elimination or risk-control strategies are decided by the economic value of their adoption and use. The total expense of providing risk mitigations to reduce equipment failure frequencies to once in three times the service life may be too costly to justify. Nonetheless, the philosophy of drastically reducing component risk to get outstanding equipment reliability is sound and sensible asset management.

A risk matrix is used to show risk level and is derived by using Formula 5.2:

Formula 5.2

Risk ($/yr) = Consequence ($/event) x Likelihood (events/yr)

On the risk matrix the intersection of the "consequence" and "likelihood" values ranks the risk. The consequence is the severity of an event, and the likelihood is the probability that it will occur. Table 5.3 is a common 5 x 6 risk matrix used to gauge the risks in a business. It has five consequence columns and six likelihood rows. A 5 x 5 matrix is also often used in occupational health and safety systems to assess job risks.

RISK MANAGEMENT PHILOSOPHY		**Business-Wide Consequence**					
E – Extreme risk: Detailed action plan approved by CEO **H – High risk: Specify responsibility to senior manager** **M – Medium risk: Specify responsibility to department manager** **L – Low risk: Manage by routine procedures** **Extreme** or **high** risk must be reported to senior management and requires detailed treatment plans to reduce the risk to **low** or **medium**		**People**	Injuries or ailments not requiring medical treatment	Minor injury or first aid treatment case	Serious injury causing hospitalization or multiple medical treatment cases	Life-threatening injury or multiple serious injuries causing hospitalization	Death or multiple life-threatening injuries
		Reputation	Internal review	Scrutiny required by internal committees or internal audit to prevent escalation	Scrutiny required by clients or third parties, etc.	Intense public, political, and media scrutiny (e.g., front-page headlines, TV, etc.)	Legal action or commission of inquiry or adverse national media
		Business Process & Systems	Minor errors in systems or processes requiring corrective action or minor delay without impact on overall schedule	Policy procedural rule occasionally not met, or services do not fully meet needs	One or more key accountability requirements not met; inconvenient but not client welfare threatening	Strategies not consistent with business objectives; trends show service is degraded	Critical system failure, bad policy advice, or ongoing noncompliance; business severely affected
		Financial	**$500**	**$5K**	**$50K**	**$500K**	**$5,000K**
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Historical Likelihood			**1**	**2**	**3**	**4**	**5**
Event occurs at this site annually or more often	**6**	**Certain**	**M**	**H**	**H**	**E**	**E**

Event regularly occurs at this site	5	**Likely**	**M**	**M**	**H**	**H**	**E**
Event is expected to occur on this site	4	**Possible**	**L**	**M**	**M**	**H**	**E**
Event occurs from time to time on this site	3	**Unlikely**	**L**	**M**	**M**	**H**	**H**
Event occurs in the industry, and could on this site, but doubtful	2	**Rare**	**L**	**L**	**M**	**M**	**H**
Event hardly heard of in the industry. May occur but in exceptional circumstances	1	**Very Rare**	**L**	**L**	**L**	**M**	**H**

Table 5.3—5 x 6 Risk Matrix for Determining the Risk Level

Such risk matrices are developed using the recommendations of international risk management standards. The business-wide consequences for people, reputation, business processes and systems, and finance are explained and scaled to reflect the organization using the matrix. The methods and principles to apply in addressing risk can be advised in the "Risk Management Philosophy" box shown at the top-left side of the matrix. The risk matrix is used to gauge whether an item or situation has an acceptable, low, medium, high, or extreme level of risk. As a general intent, risk mitigations need to drive risk levels lower by two levels or more. Extreme and high risks are reduced to medium and low, respectively, and a medium-level risk is reduced to low or less. Unknown to most managers this is this yet another "Crosshair Game" practice because there is no certainty of result. In the Plant Wellness Way risk is driven down to levels that create the required reliability.

It is important to retain mathematical accuracy when developing a risk matrix. The design of the matrix corresponds to the use of log to the base-10 ($\log_{10}$) math. The numbers used in the consequence and likelihood scales are $\log_{10}$ values. For example, the $\log_{10}$ of 100 is 2; the $\log_{10}$ of 1,000 is 3; the $\log_{10}$ of 10,000 is 4; the $\log_{10}$ of 1,000,000,000 is 9; and so on. By using $\log_{10}$ values, we can keep the matrix small. If we used linear scales, this would require a huge piece of paper to show the graduation mark for a value of 1,000,000,000 because it would be far, far to the right on the scale. But by using $\log_{10}$ scales, we can shrink the matrix to one page. Because the risk scales are $\log_{10}$, we add the indices. For example, 100 x 1,000 = 100,000 is $10^2 \times 10^3 = 10^5$; as a $\log_{10}$ calculation, it becomes 2 + 3 = 5. That is how the numbers in the cells of the sample risk matrix accompanying this book are determined.

The various business reputation, occupational health safety, and business system consequences in a column need to correspond to the financial value of the column. Similarly, for likelihood, each row is representative of the intervals at which the risk happens. The $\log_{10}$ numbers corresponding to each level of likelihood and consequence can be added together to provide a numerical indicator of the risk. This is often useful for comparing dissimilar risks in order to set priorities, or when a simple means, not involving quantitative risk calculations, is needed to give each risk a representative value. By ensuring mathematical and financial accuracy, the use of a matrix is defendable as sound and reasonable when making decisions.

The TDAF costs are used to establish the risk boundary that an organization is willing to accept. Figure 5.6 shows the risk boundary concept of investment to prevent failures. This company will not accept annualized TDAF costs of more than $20,000, and it is willing to invest money to reduce greater risks. If the risk is acceptable, nothing is done to stop it except to ensure that it does not change. Should the event happen, the business knowingly pays for its rectification. But if the cost of failure is unacceptable, then mitigations are put into place to sufficiently reduce the risk. The mitigations to prevent the risk are seen as a better investment than paying to fix the consequences later.

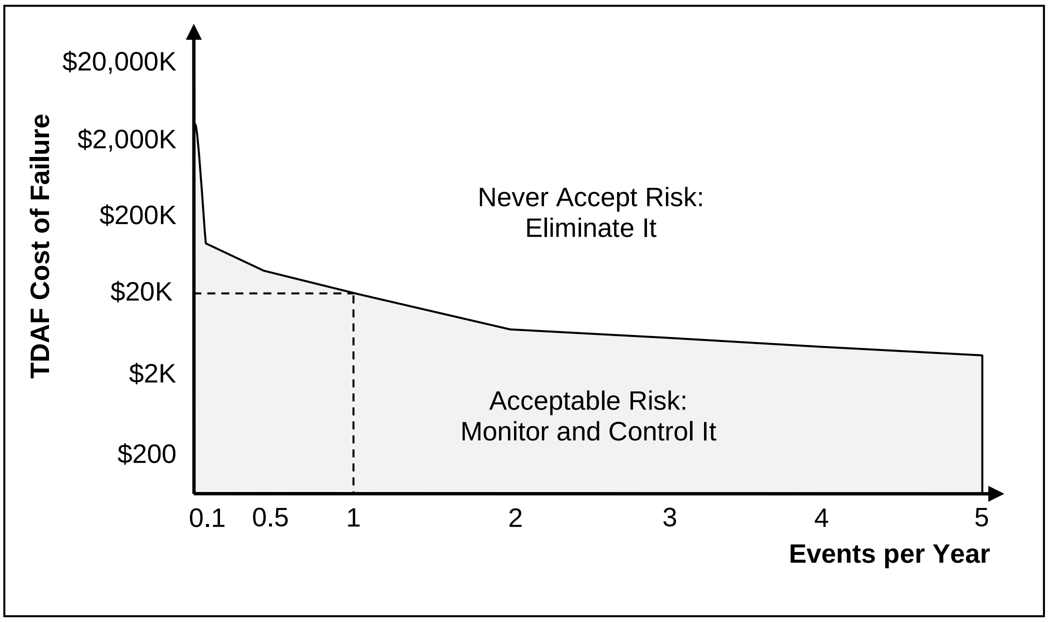

Figure 5.6—The Risk Boundary Concept

Your risk matrix needs to be calibrated so that the bottom of the low risk level represents your business risk boundary. Calibrating a risk matrix means adjusting the consequences to match your company's circumstances. A risk that is significant to a small organization may be insignificant to a much larger business. The financial value of each consequence column on the risk matrix is set by the amount that your company senior management considers an insignificant cost. Each subsequent column then follows log to the base-10 rules to set its value higher by an order of magnitude.

Because the standard 5 x 6 risk matrix causes the cells furthest to the right in the table to represent large amounts of money, it is necessary to alter the matrix to a finer scale for use in the Plant Wellness Way. A 16 x 13 risk matrix like the one in Table 5.4 is used. It is the previous 5 x 6 matrix with each column and row halved to create more cells covering smaller ranges. The table is also extended to lesser values to include small problems that happen often. This allows you to show smaller changes in risk on the 16 x 13 matrix that would not be noticeable on the 5 x 6 matrix. Even finer scales can be introduced if necessary.

Only financial values of consequences are used in the Plant Wellness Way. The business reputation, occupational health safety, and business system consequences are not shown. Every situation's severity must be converted to the money lost by your business when it happens. This is a financial truth of doing business—in the end, everything bad that happens in your organization causes a financial loss. It is vital to know how much money is in jeopardy with every risk carried.

Likelihood of Equipment Failure Event per Year				TDAF Cost per Event		$30	$100	$300	$1,000	$3,000	$10,000	$30,000	$100,000	$300,000	$1,000,000	$3,000,000	$10,000,000	$30,000,000	$100,000,000	$300,000,000	$1,000,000,000
Event Count per Year	Time Scale	Descriptor Scale	Historic Description			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
						1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
100	Twice per week	Certain		L13	2	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5	11
30	Once per fortnight	Certain		L12	1.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5
10	Once per month	Certain		L11	1	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
3	Once per quarter	Certain		L10	0.5				3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5
1	Once per year	Almost Certain	Event will occur on an annual basis	L9	0					3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
0.3	Once every 3 years	Likely	Event has occurred several times or more in a lifetime career	L8	-0.5						3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5
0.1	Once per 10 years	Possible	Event might occur once in a lifetime career	L7	-1							3.5	4	4.5	5	5.5	6	6.5	7	7.5	8
0.03	Once per 30 years	Unlikely	Event does occur somewhere from time to time	L6	-1.5								3.5	4	4.5	5	5.5	6	6.5	7	7.5
0.01	Once per 100 years	Rare	Heard of something like it occurring elsewhere	L5	-2									3.5	4	4.5	5	5.5	6	6.5	7
0.003	Once every 300 years			L4	-2.5										3.5	4	4.5	5	5.5	6	6.5
0.001	Once every 1,000 years	Very Rare	Never heard of this happening	L3	-3											3.5	4	4.5	5	5.5	6
0.0003	Once every 3,000 years			L2	-3.5												3.5	4	4.5	5	5.5
0.0001	Once every 10,000 years	Almost Incredible	Theoretically possible but not expected to occur	L1	-4													3.5	4	4.5	5

Table 5.4—Calibrated 16 x 13 Risk Matrix to Observe Changing Risks

Color-coding in the matrix is used to indicate each risk level. Below the boundary, risks are acceptable but need to be monitored to ensure they do not change. Above the boundary, risks are acted on using strategies and actions that reduce the risk to below the low-risk boundary and, ideally, to that point that an equipment failure occurs less than once in three times the service life. By implication, risks less than low are the risks you live with. That does not mean you do nothing to mitigate the risk. For example, the risk of a planet-shattering meteorite hitting the Earth is extremely small, but it is not impossible. We monitor outer space looking for dangerous meteorites even though we can do nothing to prevent them from hitting the planet. In your business, you will have risks that are so small as to be unlikely to arise, but you still must watch out that situations do not change in ways that let those risks become potential realities. You cannot use the excuse that a risk is negligible on the risk matrix to not bother preventing it from happening.

The risk matrix in Figure 5.7 shows a low-risk boundary set at an annualized cost of $10,000 per event. The business will accept the equivalent of one failure per year if it costs less than $10,000, but it will act to reduce those situations in which failure events produce accumulated costs of more than $10,000 annually. Note this means the operation will accept $100,000 loss events every 10 years and will do nothing else to prevent them beyond ensuring that an event happens no more than once every 10 years. If you can’t afford even one $100,000 failure, it would be shrewd to get an appropriate insurance policy that moves the risk to the insurance company, while you pay only the premium.

Likelihood of Equipment Failure Event per Year				TDAF Cost per Event		$30	$100	$300	$1,000	$3,000	$10,000	$30,000	$100,000	$300,000	$1,000,000	$3,000,000	$10,000,000	$30,000,000	$100,000,000	$300,000,000	$1,000,000,000
Event Count per Year	Time Scale	Descriptor Scale	Historic Description			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
						1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
100	Twice per week	Certain		L13	2	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5	11
30	Once per fortnight	Certain		L12	1.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5
10	Once per month	Certain		L11	1	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
3	Once per quarter	Certain		L10	0.5				3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5
1	Once per year	Almost Certain	Event will occur on an annual basis	L9	0					3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
0.3	Once every 3 years	Likely	Event has occurred several times or more in a lifetime career	L8	-0.5						3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5
0.1	Once per 10 years	Possible	Event might occur once in a lifetime career	L7	-1							3.5	4	4.5	5	5.5	6	6.5	7	7.5	8
0.03	Once per 30 years	Unlikely	Event does occur somewhere from time to time	L6	-1.5								3.5	4	4.5	5	5.5	6	6.5	7	7.5
0.01	Once per 100 years	Rare	Heard of something like it occurring elsewhere	L5	-2									3.5	4	4.5	5	5.5	6	6.5	7
0.003	Once every 300 years			L4	-2.5										3.5	4	4.5	5	5.5	6	6.5
0.001	Once every 1,000 years	Very Rare	Never heard of this happening	L3	-3											3.5	4	4.5	5	5.5	6
0.0003	Once every 3,000 years			L2	-3.5												3.5	4	4.5	5	5.5
0.0001	Once every 10,000 years	Almost Incredible	Theoretically possible but not expected to occur	L1	-4													3.5	4	4.5	5

$10,000 event every year
A Risk Envelope
$100,000 event every two years
Risk Boundary

Figure 5.7— Risk Matrix Showing the Level of Business Risk

The risk levels intentionally skew at the top left of the matrix. Frequent small, low-cost risks cannot be allowed to remain in your business, for two reasons. The first is that every small event takes resources and time to address. That time and effort could be better used to do far more valuable work. Small problems have massive opportunity costs, and so all small problems must be eliminated. Second, negligible risks can turn into large operational risks such as breakdowns, waste, losses, and unhappy customers. All small hazards become the doorways to large safety risks, such as injury, dismemberment, or death. Living with frequent small problems requires frequent intervention, which puts operators and maintainers at risk of harm many times. When you do not stop frequent small problems, it is only a matter of time before someone gets hurt or you have a serious production disruption and suffer another "missed-the-budget month." It is vital that small repetitive risks are escalated to a higher concern and importance, so you justify getting rid of them before they become your future injuries and disastrous TDAF cost losses.

Your risk matrix is a financial model of your business. The consequential value you lose when a risk event happens is real money lost to your company. The likelihood of events comes from your own equipment failure history. Your risk matrix shows what happens in your business, it exactly reflects the outcomes of the way your organization behaves.

Using the risk matrix lets you see the scale of a loss event and immediately spot the savings you would get if the risk were reduced to an acceptable level. The savings made from lowering a risk so that a failure event does not occur become new operating profits. When the potential profits are large, you have a strong business case for new expenditure to reduce the risk. For example, the $100,000 failure event occurring every two years represented in Figure 5.7 rates as a high risk. The annual risk calculated with the risk formula is $50,000 per year. If the likelihood of the event could be reduced to once every 10 years with suitable mitigating actions costing $10,000 annually, the business would get an additional $40,000 operational profit each year. The money to pay for the risk mitigations to gain the resulting profit becomes available when the risk goes down. With the risk reduced to a low-level occurrence of once a decade for a cost of $10,000 per year, the average annual operating profit rise is a recurring 400% annual return on investment. A project having a 400% annual return on investment presents a very strong business case to do it urgently.

Business Risk Impact Review

The business risk from operating equipment is identified by gauging the combined severity of a part's failure on the operation, safety, environment, and company reputation. You begin by asking the following economic questions for each asset to identify the business-wide impact from its worst failure events.

1. Are the total business-wide consequences of any failure of the equipment acceptable?
2. Where failure is acceptable, how frequently can it occur before it becomes unacceptable?

Events that can cause human death are treated differently from those that only destroy or ruin operating assets. When people can die from an incident, you must include it in the consideration of business risk. Modern SFAIRP[2] safety philosophy dictates you need to do all that is possible to prevent a fatality so that the likelihood of death-causing events is incredibly low.

Where an event's consequence and frequency plot on the company risk matrix determines whether the risk analysis is taken further. The operations group will know whether failure of an equipment item will cause a production stoppage that has adverse business impact. If the combined severity of equipment failure is economically acceptable, it is allowed to fail, and the analysis goes no further for that item. The default maintenance and operating strategy for such equipment is "run to failure": no maintenance activity is performed on it, and no spare parts are carried in store for it. When the equipment breaks, the decision is made to rectify it or address the failure in an appropriate way. Corrective actions are instigated after failure, and the accompanying costs and time delays are accepted without concern because a failure of the equipment does not matter to business success.

When an equipment failure is considered financially unacceptable or minor failures are too frequent, the business-wide economic impact of a part's failure is determined using TDAF costing. The estimate needs to be acceptably accurate to be believed by managers and defendable when challenged by others. Aim to be better than ±20% of true business costs, losses, and waste in your TDAF cost estimates. The consequence is the worst TDAF cost should a critical part fail in service. The likelihood is the historical annual frequency for the failure event in the business (or the frequency from other comparable, similarly operated businesses if the imagined failure has not yet occurred). The business risk from each part is marked on a calibrated business risk matrix. This component risk assessment process is repeated for each critical part in the equipment. The greatest risk is the component failure event with the highest annualized cost. In this way, you quantify the worst business risks and make them visible to everyone. When component risks are above the risk boundary, action must be taken to reduce those risks to an acceptable level. Such components are then individually analysed in a Physics of Failure Factors Analysis to identify useful risk mitigations.

The risk to your operation varies with the equipment component concerned, the type of failure it suffers, and the risk mitigations your company has in place for each failure. This produces a spread of risk values. If you plot a point for every risk from the critical parts in an item of equipment onto your company risk matrix, there will be an area on the matrix covered in dots. The range of risks will have a shape. That patch is the risk envelope for the equipment. Figure 5.7 shows a risk envelope within which are all the points representing one equipment's range of risks for the operation using it.

Risk-Reduction Decisions

When the business impact of an equipment failure is greater than what the organization will tolerate, you put into place appropriate actions that reduce risk below the acceptable boundary and keep it there. The mitigation methods and actions chosen must be effective in reducing the risk by either lowering the consequential business-wide impact of the event (its TDAF cost) or lowering the likelihood of the event occurring (its degree of uncertainty).

You check the effectiveness of your chosen mitigations by plotting the risk before and after on a risk matrix to ensure the proposed risk controls can bring the desired results. You and your management must be convinced that what is done to reduce risk will work and that the risk will remain under the low level. If a mitigation action does not clearly deliver substantially reduced consequence and/or lower frequency, it is a waste of resources, and it is discarded, and a better mitigation chosen. Figure 5.8 shows how the effectiveness of mitigations is checked and tested for their potential economic value. In the example, the consequence of the $100,000 failure event is unchanged, but the likelihood has been substantially reduced from annually to once a decade because of the new mitigations used. This reduction in risk saves nine failures during the decade totalling $900,000. There is great financial benefit to be gained by having highly reliable plant and equipment.

Likelihood of Equipment Failure Event per Year				TDAF Cost per Event		$30	$100	$300	$1,000	$3,000	$10,000	$30,000	$100,000	$300,000	$1,000,000	$3,000,000	$10,000,000	$30,000,000	$100,000,000	$300,000,000	$1,000,000,000
Event Count per Year	Time Scale	Descriptor Scale	Historic Description			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
						1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
100	Twice per week	Certain		L13	2	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5	11
30	Once per fortnight	Certain		L12	1.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5
10	Once per month	Certain		L11	1	2.5	3	3.5	4	4.5	5	5.5	6	[illegible]	7	7.5	8	8.5	9	9.5	10
3	Once per quarter	Certain		L10	0.5				3.5	4	4.5	5	[illegible]	[illegible]	[illegible]	[illegible]	7.5	8	8.5	9	9.5
1	Once per year	Almost Certain	Event will occur on an annual basis	L9	0					3.5	4	4.5	[illegible]	[illegible]	6	[illegible]	7	7.5	8	8.5	9
0.3	Once every 3 years	Likely	Event has occurred several times or more in a lifetime career	L8	-0.5						3.5	4	[illegible]	[illegible]	[illegible]	[illegible]	6.5	7	7.5	8	8.5
0.1	Once per 10 years	Possible	Event might occur once in a lifetime career	L7	-1							3.5	4	[illegible]	[illegible]	5.5	6	6.5	7	7.5	8
0.03	Once per 30 years	Unlikely	Event does occur somewhere from time to time	L6	-1.5								3.5	[illegible]	[illegible]	5	5.5	6	6.5	7	7.5
0.01	Once per 100 years	Rare	Heard of something like it occurring elsewhere	L5	-2									3.5	4	4.5	5	5.5	6	6.5	7
0.003	Once every 300 years			L4	-2.5										3.5	4	4.5	5	5.5	6	6.5
0.001	Once every 1,000 years	Very Rare	Never heard of this happening	L3	-3											3.5	4	4.5	5	5.5	6
0.0003	Once every 3,000 years			L2	-3.5												3.5	4	4.5	5	5.5
0.0001	Once every 10,000 years	Almost Incredible	Theoretically possible but not expected to occur	L1	-4													3.5	4	4.5	5

Risk = $100,000 / yr event
Likelihood Reduction
Consequence Reductio
Money Saved by Mitigations
Risk = $100,000 / 10 yr event

Figure 5.8—Business Risk Matrix Showing the Effectiveness of Risk Mitigations

When several risk mitigations are required to operate collectively to achieve the required risk reduction, it may be necessary to accept a less than optimal individual mitigation choice because it is an integral part of the total risk-reduction solution. A common example is to carry critical spares in your warehouse and pay all the ongoing costs to keep them reliable and available even if the parts in service rarely fail. The spares are integral to your operating risk-reduction solution, and all of them must be on site, even if they are dead money. It is only because the spares are handy as part of a larger strategy that your operation can operate at a very low risk of disaster. Another seeming wasteful risk mitigation is to limit the number of times routable assemblies are rebuilt before being replaced with totally new units. Although a routable, by definition, is to be refurbished, its frequency of failure rises as the unchanged components age and fail. At some point, the rising failure rate of the rebuilt routable will cause high corrective maintenance costs from its frequent replacement. Even though the cost of a new unit will be more than the cost to rebuild the routable again, you would be wise to pay for the new unit. You will substantially reduce the operating risk to your plant by using new equipment with long times between failures rather than paying a lesser amount to fix old, tired assemblies that will not last for very long.

A business makes money if a risk can be prevented for less than the risk's equivalent annualized cost. The greatest opportunity for a company to manage risk for much less cost is to identify those methods, systems, and practices that reduce the chance of a risk arising and then implement them with great energy and vigour across the organization. Maintenance is one of the methodologies available to reduce the risk of equipment failure, but if used wrongly it becomes a consequence reduction strategy done after failure has started. In the Plant Wellness Way maintenance is used for proactive failure prevention. It combines with cost-effective engineering and operational choices to deliver chance-reduction strategies that stop all failures from starting during the equipment lifetime.

Any risk mitigation or combination of risk controls you choose will have to meet the criteria of substantially reducing the original risk with much lower event frequency and/or a large reduction in consequences. The word "substantial" is defined in the *Collins English Dictionary* as "worthwhile; important; of telling effect." In the context of risk management, any improvement you select must clearly deliver better outcomes by a proportion that is indisputably valuable to the organization. On the risk matrix, you want to see a big distance between the original risk point and the final risk.

There are three decision rules used in the Plant Wellness Way for deciding when you should accept a risk mitigation for a physical asset.

- A solution that reduces <u>opportunity</u> for failure is acceptable if it significantly extends the time between situations when component failure is possible. It is satisfied by mitigations that reduce the frequency of microstructure stress excursions and/or of contact environmental degradation events. Examples are engineering solutions that lessen the frequency of causes of failure factor mechanisms, and the application of world-class practices, such as precision maintenance and precision operation, throughout service life.

- A solution that reduces the <u>chance</u> of failure or increases <u>reliability</u> must significantly reduce the stress in a part. It is satisfied by solutions that indisputably lower the size of component microstructure stress or improves the microstructure's capability to comfortably handle all imposed stresses. Examples include de-rating the service duty, reengineering the component by using parts made of greatly stronger materials or with quality properties that mitigate the effect of stress, changing part shape to reduce microstructure stresses, and practicing precision maintenance and operation all the time so stresses are always minimized.

- A solution that reduces consequence is acceptable if it significantly reduces the TDAF cost. It is achieved by using mitigations that prevent large financial losses if a failure initiation event happens.

Opportunity Cost of Run-to-Failure Decisions

If the business-wide risk of a failure is already below the risk boundary, do not spend time conducting an analysis. You will get greater value from your time by preventing higher-risk situations. For example, if a small 5-kilowatt conveyor gear box drive fails, it will cost $1,500 to $2,500 for a new one, depending on the gearbox model. It will take about four hours to change out the unit at a direct maintenance labour and services cost of about $1,000. Provided a new unit can be sourced within an hour after a breakdown, the business-wide impact of costs, waste, and losses in a continuous process operation could reach $35,000. If a breakdown happens no more than every five years, the annualized risk is $7,000. This risk is well below the $10,000 per year risk boundary of our imaginary manufacturer, and thus our maintenance strategy defaults to accepting that failure. However, if the same gearbox fails every two years and each failure costs $35,000, you will have to address the reasons for the failure, as the annualized cost of $17,500 is now above the $10,000 per year risk boundary. In this case, you cannot accept a run-to-failure strategy and need to develop mitigations to reduce the frequency of failure.

A trap you fall into with a run-to-failure decision is that, by default, you design into your operation regular breakdowns of unimportant machines and equipment. These require you to use maintenance time and budget repairing equipment of minor importance. The value of the opportunities lost because limited maintenance resources are used to fix inconsequential equipment when they could be doing far more valuable work must be considered in selecting a maintenance strategy. That time and money could be better spent creating plant reliability or eradicating larger risks rather than repairing broken things of trivial importance. Run to failure might seem to be an acceptable risk-reduction strategy, but not if it costs you opportunities to get far greater successes.

You remove the opportunity trap from the run-to-failure strategy by proactively replacing unimportant equipment shortly before it is likely to fail. In the case of the $2,500 gearbox in the continuous process plant, we originally devised a strategy to replace it new upon breakdown about once every five years, for a TDAF cost of $35,000. But when fixing a breakdown imposes such high cost, you need to check the value of doing an old-for-new replacement during a planned outage. The gearbox will cost $2,500 to buy regardless of whether it's a breakdown or a scheduled production shutdown. The time needed to swap the old gearbox with a new one during a shutdown will be less because the plant is already handed over for maintenance. The same job done in a shutdown will have a total business-wide cost of about $5,000. It is clearly more economical to install a new gearbox as planned preventive maintenance for $5,000 than to have a TDAF cost breakdown of $35,000. The best strategy for this gearbox is not the default run-to-failure strategy but a zero-breakdown preventive maintenance strategy to replace it brand-new every four years in a planned shutdown and never let the equipment age so long that you risk failure in service. In fact, you could fit a new gearbox every two years so that failures are impossible, and it would still be far less costly than having a breakdown after five years. The above zero failures strategy will bring you modern, new equipment, lower maintenance costs, lower risk, and higher operating profits.

This simple maintenance strategy selection case study has an important message for you—when making maintenance decisions, you can only determine the best choice after you do economic modelling. Maintenance is an economic decision. Companies who are not doing economic models of all their maintenance choices are sure to be wasting great amounts of money. The right maintenance strategy to adopt is the one that brings the most money to the company—the least life-cycle cost choice is always the one to take. Only do the maintenance that brings the most operating profit over the lifetime of the asset. The best financial choice for your company is also the best maintenance choice for your company. In the Plant Wellness Way, you can see on the risk matrix which maintenance strategy will bring you most operating profit.

FOOTNOTES

1. First heard from retired professor David Sherwin in his three-day "Introduction to Reliability Engineering" course, Perth, Western Australia, June 2007.

2. So Far As Is Reasonably Practicable (SFAIRP) is a risk management framework used for industrial situations.