PREDICTIVE RISK-BASED STRATEGIES TO MANAGE SAFETY

Dr. Willem Sprong

D.Ing GIBB (PTY) Ltd

SUMMARY

Predicting failure will reduce the risk to railway safety, if risk is understood and implemented correctly. Traditional strategies were compliance based, but recent developments tend to use risk based strategies. This can also be referred to as conformance versus performance based strategies. This paper explains the differences between the two strategies. It discusses the advantages and disadvantages of each. Implementation and how it should be approached is a focus towards the end of the paper. Throughout the paper, the definition for reliability will be detailed and reference to the difference between availability and reliability will be used to explain the new understanding required to implement a risk based strategy.

A quote from an article written by Sandy Dunn (2005) [1] called, Condition Monitoring in the 21st Century - "Predicting the future is fraught with danger. Many wiser heads than mine have made bold predictions of the future, only to be proved hopelessly wrong." – Maybe why the art of predicting maintenance requirements never evolved. According to her the field of condition monitoring was only established with any significance during the last quarter of the last century.

Richard Price (2012) summarised the principle of risk-based regulation in his paper, Risk-based health and safety regulations, by concluding that an unsafe industry cannot be an efficient industry. [2] It is very important that safety never be used as an excuse against change.

INTRODUCTION

The railway industry is characterised through major incidents that influence operators, clients and the environment. For the rail industry to improve its efficiency, progress and grow, it needs a regulatory framework which gives the public assurance that the railways are safe, reliable and efficient.

According to Wolter J. Fabrycky reliability as described in his book, Systems Engineering And Analysis, can be defined simply as the probability that a system or product will perform in a satisfactory manner for a given period of time when used under specific operating conditions. This definition stresses the elements of probability, satisfactory performance, time and specified operating conditions. [3]

An improvement in reliability will improve the safety of the railway system. This can be achieved through management and leadership. A base must be established with the management of regulations. But excellence will be achieved through leadership. Essentially this is the difference between compliance-based and risk-based systems.

RELIABILITY

The basic rule still remains that more must be done with less. It is not good practice to spend lots of money on maintenance only and not to use the opportunity to improve the overall condition of the assets. There must be a change in the thinking and method of working towards a more effective and efficient result. Simply going in the same direction year after year will result in the available money not being spent in the best way.[4]

The essential elements of the reliability definition described above are probability, satisfactory performance, time and specified operating conditions.

Probability

Probability, the first element in the reliability definition, is usually stated as a quantitative expression representing a fraction or a percent specifying the number of times that an event can be expected to occur in a total number of trials. For example, if the probability of survival of an item for 80 hours is 0.75 (or 75%), it indicates that the item can be expected to function properly for at least 80 hours 75 times out of a hundred.

Johannesburg, 4-9 October 2015

When there are a number of supposedly identical items operating under similar conditions, it can be expected that failure will occur at different points in time. Failures are therefore described as probabilistic. For example, the 3kV DC system consists out of many substations that are feeding into it. These substations have similar equipment inside which operate under similar conditions. Failure of the equipment will not occur at the same time. The fundamental definition of reliability is heavily dependent on the concepts derived from probability theory.

Satisfactory performance

The second element in the reliability definition is satisfactory performance, indicating that specific criteria must be established, which describe what is considered to be satisfactory. It can also be described as the required function of the item in the system. A combination of qualitative and quantitative factors defining the functions that the system or product are to accomplish, usually presented in the context of the system specification, are required. For the 3kV DC traction substation the basic requirement is to provide a regulated supply of 3000V DC to the traction system [4].

The satisfactory performance of any piece of equipment or component can, therefore, be described as achieving the delivery requirement that it was designed for. In other words, the system delivers what is expected from it.

Time

The third element, time, is one of the most important because it represents a measure against which the degree of system performance can be related. The time parameter must be known in order to assess the probability of the system to complete a task or given function as scheduled. Of particular interest is the ability to predict the probability of an item or system operating without failure for a designated period of time.

Reliability can also be defined in terms of mean time between failure (MTBF) or mean time to failure (MTTF), making time critical in reliability measurement [5]. MTBF is the average time between failures and MTTF is the average time until the first failure.

If the time is not properly defined in a study of this nature, it will create confusion on the perception of reliability. It is important to remember that reliability was defined earlier as the ability of the equipment to perform according to expectation. If the equipment performs as expected, the operator would perceive it as being reliable.

Specified operating conditions

The specified operating conditions under which a system or product is expected to function constitute the fourth significant element of the reliability definition. These conditions will include environmental factors, such as the geographical location where the system is expected to operate, the operational profile, temperature cycles, humidity, vibration, shock, and so on. The input from the operator is one of the factors influencing the condition as mentioned. The expectation should not be to operate a system out of the

The reliability function

The reliability function is derived by Blanchard and Fabrycky, System Engineering and Analysis, 1990 [3].

The reliability function is determined from the probability that a system will be successful at least for some specified time t. The reliability function, R(t), is defined as

$$R(t) = 1 - F(t) \qquad (1)$$

where F(t) is the probability that the system will fail by time t. F(t) is basically the failure distribution function or unreliability function. If the random variable t has a density function of f(t), the expression for reliability is

$$R(t) = 1 - F(t) = \int_t^\infty f(t)\, dt \qquad (2)$$

If the time to failure is described by an exponential density function, then

$$f(t) = 1/\theta\ e^{-t/\theta} \qquad (3)$$

where θ is the mean life and t the period of interest. The reliability at time t is

$$R(t) = \int_t^\infty 1/\theta\ e^{-t/\theta}\, dt = e^{-t/\theta} \qquad (4)$$

Mean life (θ) is the arithmetic average of the lifetimes of all items considered, which for the exponential function is MTBF. Thus

$$R(t) = e^{-t/M} = e^{-\gamma\lambda t} \qquad (5)$$

where γ is the instantaneous failure rate and M the MTBF.

If a component has a constant failure rate, the reliability of that item at its mean life is approximately 0.37. Thus, there is a 37% probability that the system will survive its mean life without failure. Mean life and failure rate are related as

$$\gamma = 1/\theta \qquad (6)$$

Figure 1 illustrates the exponential reliability function, where time is given in units of t/M. The illustration focuses on the reliability function for the exponential distribution, which is commonly used in many applications.

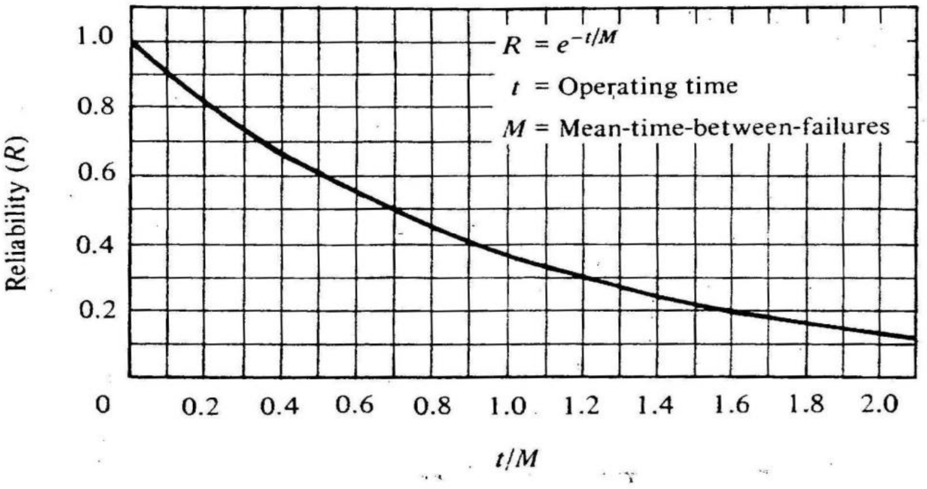

Figure 1: Reliability curve for the exponential distribution. [3]

The failure rate is the rate at which failures occur in a specified time interval. The failure rate per month is expressed as

λ = *Number of failures / total operating months (7)*

The failure rate may be expressed in terms of failures per month, percent failures per 12 months or failures per million hours. In the case of a 3kV DC traction substation the failure rate was best expressed as failures per month. For the analysis in this chapter, the rate was taken as the number of months during which events take place.

The relationship between the failure rate and the MTBF is

$$MTBF = 1/\lambda \qquad (8)$$

The failure rate is important when determining corrective maintenance actions. All system failures must be addressed to include failures due to primary defects, failures due to manufacturing defects, failures due to operator defects, and so on (Blanchard, 1990) [3].

PREDICTING FAILURE

The quote from Sandy Dunn [1],“Predicting the future is fraught with danger. Many wiser heads than mine have made bold predictions of the future, only to be proved hopelessly wrong.” This quote should not prevent the implementation of a predictive approach to risk management. It is impossible, according to the mathematical laws of statistics, to reduce the probability of risk to zero. It is also true that it will never be one hundred precent.

If risk cannot be reduced to zero, the effect of the failure must be mitigated to an acceptable level. The approach of predicting failure rests heavily on the ability to analyse trends and not to focus on individual events. In the rail safety environment it is important to understand which occurrences must be investigated to achieve an improvement in safety.

Not all investigation will lead to improved safety. Risk based investigations and analysis must be efficient and effective.

"A risk-based approach to regulation explicitly acknowledges that the government cannot regulate to remove all risks and that regulatory action, when taken, should be proportionate, targeted and based on an assessment of the nature and the magnitude of the risks and of the likelihood that regulation will be successful in achieving its aims." (Paul & Huber, 2015) [5]

Efficient

Resources are extremely limited. Not only financial resources but human and material resources as well. To be efficient means that you are achieving maximum productivity with minimum wasted effort or expense. In other words, efforts must be affordable. The drive for risk-based regulation targets efficiency gains.

Effective

Effort must be targeted at the most riskiest events. To be effective, the efforts must work. Risk analysis must focus on the product of the impact and the probability of an even occurring. Regulators must align their priorities and regulatory activity with the highest risk and potential for improvement.

RAILWAY SAFETY

Safety is a key quality requirement expected by the railway transport customers, passengers and freight companies and society. The public has a vested interest in the railway industry and require that it be operated and maintained responsibly. The minimum requirement is to at least maintain the existing level of safety. This is done through compliance-based management with an increase expected when reasonable practical.

It must be preferred to achieve outcomes by providing support and collaboration on risk-based safety improvement initiatives, to encourage industry to build the capacity to improve its performance voluntarily and collectively. Risk-based regulatory activities are more about providing leadership instead of management.

Improving safety

Safety can be improved through the support of the following focus area.

- Influence industry to work together to identify and manage railway risks as an industry
- Support the creation of industry generated standards to reduce risk
- Support the adoption of endorsed industry generated standards by rail transport operators
- Supplement industry with Approved Codes of Practice or recommended changes to legislation
- Provide advance notice to rail transport operators of the areas of greatest national or local risk so that opportunity for reasonably practicable improvements can be made

The risk-based approach combines checking legal compliance with proactively pushing for excellence in management. The one cannot be implemented without the other; the two strategies are complimentary to each other.

A push is required for excellence in management by businesses, because excellent management improves the likelihood of safety compliance every day, and also the likelihood of effective risk control. Excellence in management is so important because managers control risks and it is known that managers' performance varies over time.

If managers and the businesses in which they operate are already high performing, then there is a greater likelihood that their dips in performance will still be above the legal minimum and risks will be adequately controlled. But if they are only poorly performing, then there is a greater likelihood that their normal performance will be below the legal minimum, leaving risks are uncontrolled. Determining risk should start with an evaluation of the capability of managers to control risks.

Information intelligence is required to determine risk. The intelligence can be obtained from own inspections, investigations and enforcement activities over a long period. It allows for the analysis of trends and not just current conditions. It is my belief that those responsible for regulating safety should form part of the inquiries of the operators as well. Valuable information can be obtained in this regard. It must be understood as a supporting function to the operators.

Risk-based regulatory activities

From the discussion above, it is clear that risk-based and compliance-based regulatory activities cannot stand separate. Compliance-based, also referred to as conformance-based, must provide the base for at least maintaining the current safety status. Risk-based, or sometimes also referred to as performance-based activities, will enable the achievement of excellence. That will provide the vehicle to improve safety.

What is risk-based regulatory activities then? Prof. Julia Black described is as follows during a presentation that was done at the London School for economics and politics in 2008.[7]

She explained that it is systematised decision making frameworks and procedures to prioritise regulatory activities and deploy resources, principally relating to inspection and enforcement, based on an assessment of the risks that regulated firms pose to the regulator’s objectives.

Some key elements form part of this definition. A risk tolerance must be set to enable an agreement between the parties on the acceptable risk. Most process will focus on the risk assessment, but identifying the risk before such assessment is crucial. The statistical analysis required to determine the probability opf such risk occurring requires various assumptions to be made. Assigning scores and weighting to each risk therefor is vital.

Linking resources to the identified risk and the response to the score calculated makes the risk-based activities efficient and effective.

To identify and assess risk, I used the process called FMECA. Failure Mode, Effect and Criticality Analysis is a logical process that can be followed to calculate the scores and identify mitigating activiets to reduce the impact of occurrences happening.

To perform an effective FMECA, a thorough knowledge of the system is needed. The first step therefore is to obtain all information available on the system. An FMECA can be performed from different viewpoints, such as safety, mission, success, availability, repair cost, failure mode, etc

The required outcome must be considered when deciding how to approach the FMECA. Which components failed frequently, what is the effort required to repair and what influence does such a failure have on the safety.

The FMECA must include the following information:

- Item identification – Identify each significant system component that is likely to fail.
- Description of failure modes – Define the most probable modes of failure for each identified item. Failure modes are related to the operational modes that the system experiences through the performance of its designed function.
- Cause of failure – The anticipated cause of failure should be described for each instance.
- Possible effects of failure – Describe the most probable effects as a result of each failure. Effects may range from complete system destruction to partial system operation.
- Probability of occurrence – Through statistical means, estimate the probability of failure occurrence. Probabilities of occurrence may initially evolve from experience factors or through reliability allocation and will be based on reliability prediction data as more date is captured as the system progresses.
- Criticality of failure – Failures may be classified in terms of criticality in any one of four categories, depending on the defined failure effects as follows.

Minor failure – Any failure that does not degrade the overall performance and effectiveness of the system beyond acceptable limits.

Major failure – Any failure that will degrade the system performance and effectiveness beyond acceptable limits but van be controlled.

Critical failure – Any failure that will degrade the system beyond acceptable limits and could create a safety hazard if immediate corrective action is not taken.

Catastrophic failure – Any failure that could result in significant system damage, such as to preclude functional accomplishment, and could cause deaths and personnel injuries.

- Possible corrective action or preventive measures – Describe the action than can be initiated to reduce the probability of failure occurrence or to minimize the effect of failure, (Benjamin S. Blanchard, Systems Engineering and Analysis, 1981).[3]

Some very important observations can be made from the FMECA that will help to identify areas of concern. Each of the items identified can be broken down into smaller components and a FMECA can be done in greater detail. The detail depends on the risk tolerance that was agreed upon.

Challenges in implementation

Some of the challenges to implement a risk-based regime are:

- Combining simplicity with complexity
- Knowledge and data –getting the right data, and making better use of the knowledge the agency has
- Structure and operation of internal risk governance processes –how to balance the need for organisational structures to ensure the accuracy and consistency of assessments with speed and responsiveness.
- Changing the culture to embed the risk based approach across the whole organization
- Ensuring internal compliance with the risk based regime
- Ensuring that assessments of firms are forward looking
- Going beyond the individual firm in assessing risk
- Managing blame
- Making resources follow risks
- Managing political risk

Lessons from current experiences

Similar approaches were implemented during the study, and some lessons that were learnt are:

Starting out

- Start with risks, not rules
- Ensure the organisation has sufficient powers to implement the approach
- Beware of other regulatory or governmental policies which may contradict or hinder the adoption of a risk based approach
- Ensure you know what your goals are - it is worth doing, but don’t do it for the wrong reasons

Dealing with transition

- Designing and implementing a risk based framework will take time
- Organisational challenges are significant and should not be underestimated
- Think beyond the risk assessment to how the organisation will respond Challenges of maintenance
- Keep the framework simple to use and be prepared for the need to make continual adjustments
- Think in terms of achievability

Need for communication internally and externally

Need to recognise that risk based processes require regulators, and politicians, to take risks.

CONCLUSION

The idea of risk-based regulation that should replace compliance-based regulation is incorrect. Conformance to standards and regulations are required to maintain the current safety status. This must as least be a minimum acceptable level.

Risk-based regulatory activities compliment compliance-based activities. The regulations stay the same, but the management of the activities change. Through a process, such as the FMECA, risk identification and assessment will assist in the re-deployment of resources. The focus will be on the risks that can be addressed and will make a difference in the reliable operation of railways. Not all risk can be averted, but should be mitigated to an acceptable tolerance.

REFERENCES

[1] DUN, S. Condition Monitoring in the 21st Century. The Plant Maintenance Resource Centre (Internet). April 2005.

[2] PRICE, R. Risk-based health and safety regulations. International Rail Safety Conference. October 2012

[3] BLANCHARD, BS & FABRYCKY, WJ. Systems engineering and analysis. 2nd Edition. Prentice Hall, Englewood Cliffs. New Jersey. 1990. ISBN 0-13-880758-2. 721p.

[4] SPRONG, W. Applying the Predictable maintenance approach to 3kV DC Traction Substations. Dissertation in fulfilment of requirements for D.Ing, University of Johannesburg. 2007.

[5] RAO B.K.N. Handbook on condition monitoring. First edition, Elsevier Advanced Technology, 1996.

[6] PAUL, R & HUBER, M. Risk-based Regulation in Continental Europe?. October 2015

[7] BLACK, J. Risk based regulation. Presentation to the OECD. December 2008