

AWA
19th Federal Convention

**Risk Based Availability Modelling for Asset Management &
Regulatory Purposes**

K J Anderson BD Dip TRP FIE Aust
R M Robinson BE BA FIE Aust



ACN 072 114 473
ABN 98 072 114 473

AWA 19th Federal Convention

Risk Based Availability Modelling for Asset Management & Regulatory Purposes

CONTENTS

1.0 SUMMARY

2.0 INTRODUCTION

Eight Paradigms

3.0 EXTENSION OF PARADIGM 6 -

A Water Industry Example

4.0 PROCESS AND DESCRIPTION

5.0 REFERENCES

AWA 19th Federal Convention

Risk Based Availability Modelling for Asset Management & Regulatory Purposes

1.0 SUMMARY

7 paradigms of risk support the base case Rule of Law as understood by Risk & Reliability Associates.

The benefits of the risk based availability modelling include:

- Greater understanding of the system,
- Optimisation of the system not the component parts,
- Better understanding of the system,
- The effect of all points and procedures and practices on end availability,
- The introduction of better practices needed to support the system model, and
- Greater availability of supply

2.0 INTRODUCTION

‘Risk’ means different things to most of us. If we knew what would happen next then there would be no ‘risk’.

In this context a paradigm is a universally recognised knowledge system that provides model problems and solutions. The paradigms are:

- o) The rule of law,
- i) Traditional risk management,
- ii) Asset based risk management,
- iii) Threat based risk management,
- iv) Market based risk management,
- v) Solution based ‘best practice’ risk management,
- vi) Systemic mutual feedback loop,
- vii) Risk culture concepts.

2.1 Paradigm 0 - The Rule of Law

- The rule of law is the base case
- The other paradigms represent methods of satisfying legal outcomes in the event of the risk occurring.
- As a consequence, asking lawyers which paradigm should be applied to ensure ‘due diligence’ generates a response, once they are explained, that all paradigms are necessary.

2.2 Paradigm 1 - Insurance

- Historically typified by the Lloyds insurance and the Factory Mutual Highly Protected Risk (HPR) approaches
- By looking at past incidents and losses and comparing these to existing plants and facilities, judgements can be made.
-

2.3 Paradigm 2 - Asset Management

- Typified by engineering based Failure Mode Effects and Criticality Analysis (FMECA), Hazard and Operability (HazOp) and Quantified Risk Analysis (QRA) 'bottom-up' approaches.
- Power of bottom up techniques lies in the closely coupled solutions to identified problems.
- Any proposed risk control solutions are particular, focussed and specific.
- Resulting risk management registers are powerful decision making tools.

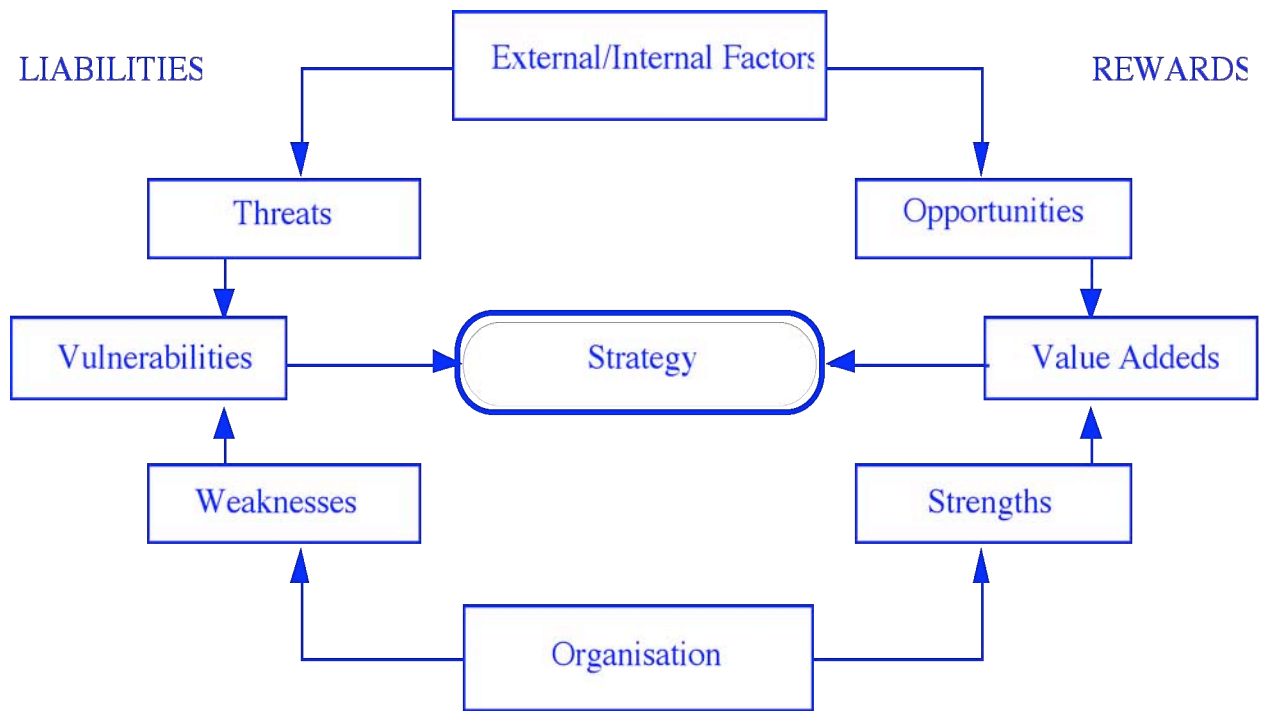
2.4 Paradigm 3 - Threats and Vulnerabilities

A very simple example of a Threat and Vulnerability analysis follows.

THREATS	CRITICAL SUCCESS FACTORS		
	Reputation	Operability	Staff
Technical	xx	xx	xx
Community	-	-	xx
Political	x	x	x
Financial	xxx	xxx	x
Natural Events	x	xxx	x
Y2K	x	xx	x

Sample Vulnerability Matrix

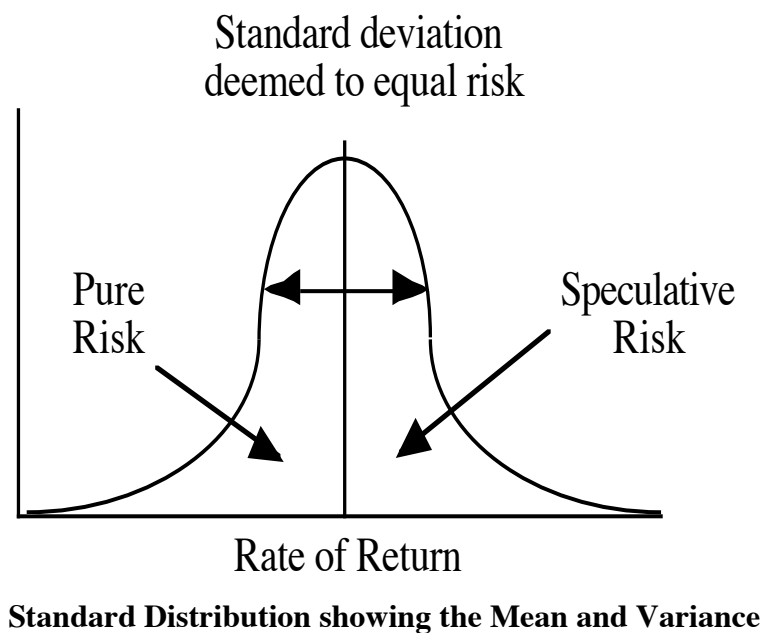
- Intersections of a threat with a "critical success factor" or "asset" are termed vulnerabilities.
- The SWOT analysis provides insight into the risk of loss (vulnerabilities) and the risk of gain (value added).



Augmented SWOT Process

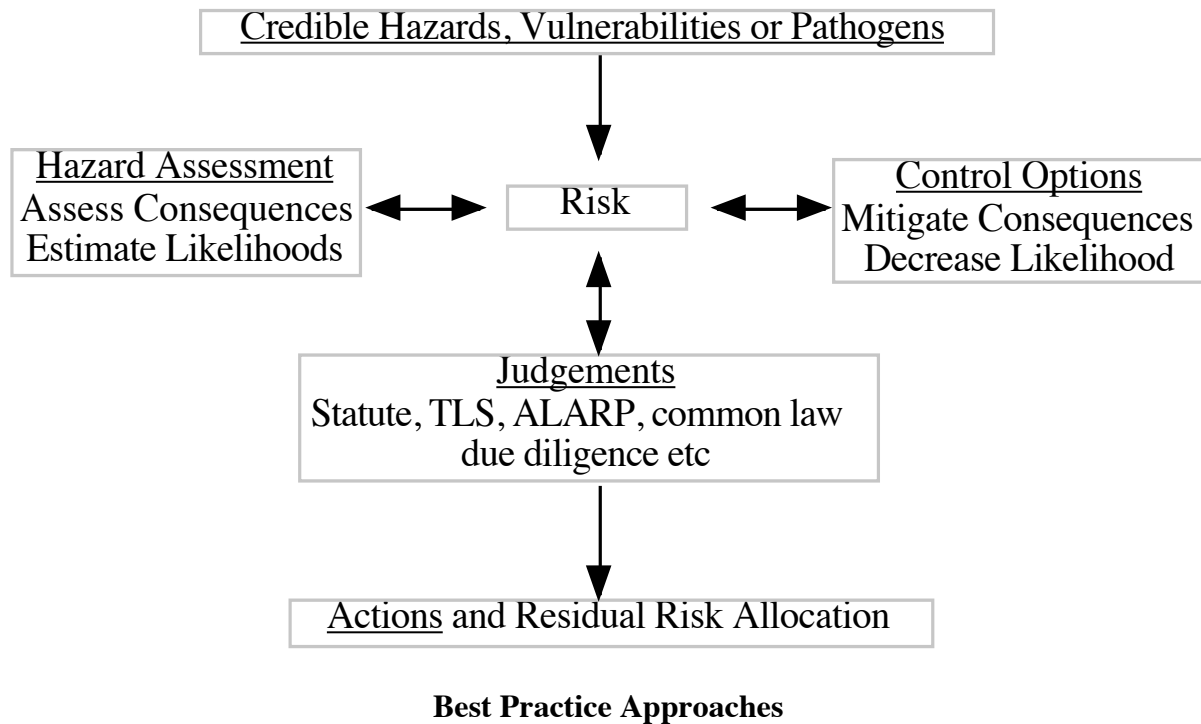
2.5 Paradigm 4 - Risk as Variance

The comparatively recent market based risk management, based on the notion of the risk being equal to variance with an equivalent risk of gain as well as loss.



2.6 Paradigm 5 - Best Practice

- This is solution based ‘best practice’ risk management rather than hazard based risk management.
- Look at all the good ideas other people in an industry use



2.7 Paradigm 6 - Biological/Computer Simulation Paradigms

- The most practical manifestation of the biological paradigms
- Modelling a complex system in a virtual reality environment and playing endless “what if” scenarios.

Suppose every vessel in the plant ‘knows’ what over temperature or overpressure it can withstand before rupture, and after having ruptured under such conditions can ‘project’ and ‘communicate’ its thermal and pressure energies to adjacent vessels which then respond accordingly.

Obviously, this requires fearsome computer power and an extensive interpretation of nature. And, a belief that hyper-reality can come close to reality.

2.8 Paradigm 7 - Risk Culture

James Reason (1997) develops a cultural paradigm model in several ways. He notes three types of risk culture.

Pathological Culture

- Don't want to know
- Messengers are 'shot'
- Responsibility is shirked
- Failure is punished or concealed
- New ideas actively discouraged

Bureaucratic Culture

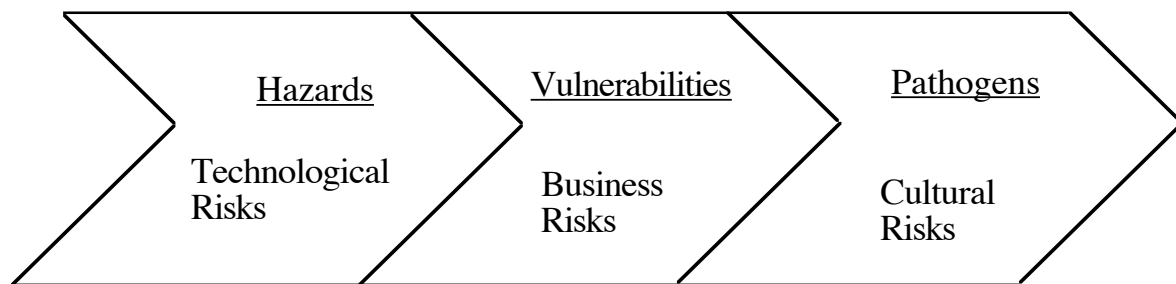
- May not find out
- Messengers are listened to if they arrive
- Responsibility is compartmentalised
- Failures lead to local repairs
- New ideas often present new problems

Generative Culture

- Actively seek it
- Messengers are trained and rewarded
- Responsibility is shared
- Failures lead to far reaching reforms
- New ideas are welcomed

Three Risk Cultures after Reason (1997)

Culture is now being identified as central to effective risk management suggesting a new focus.

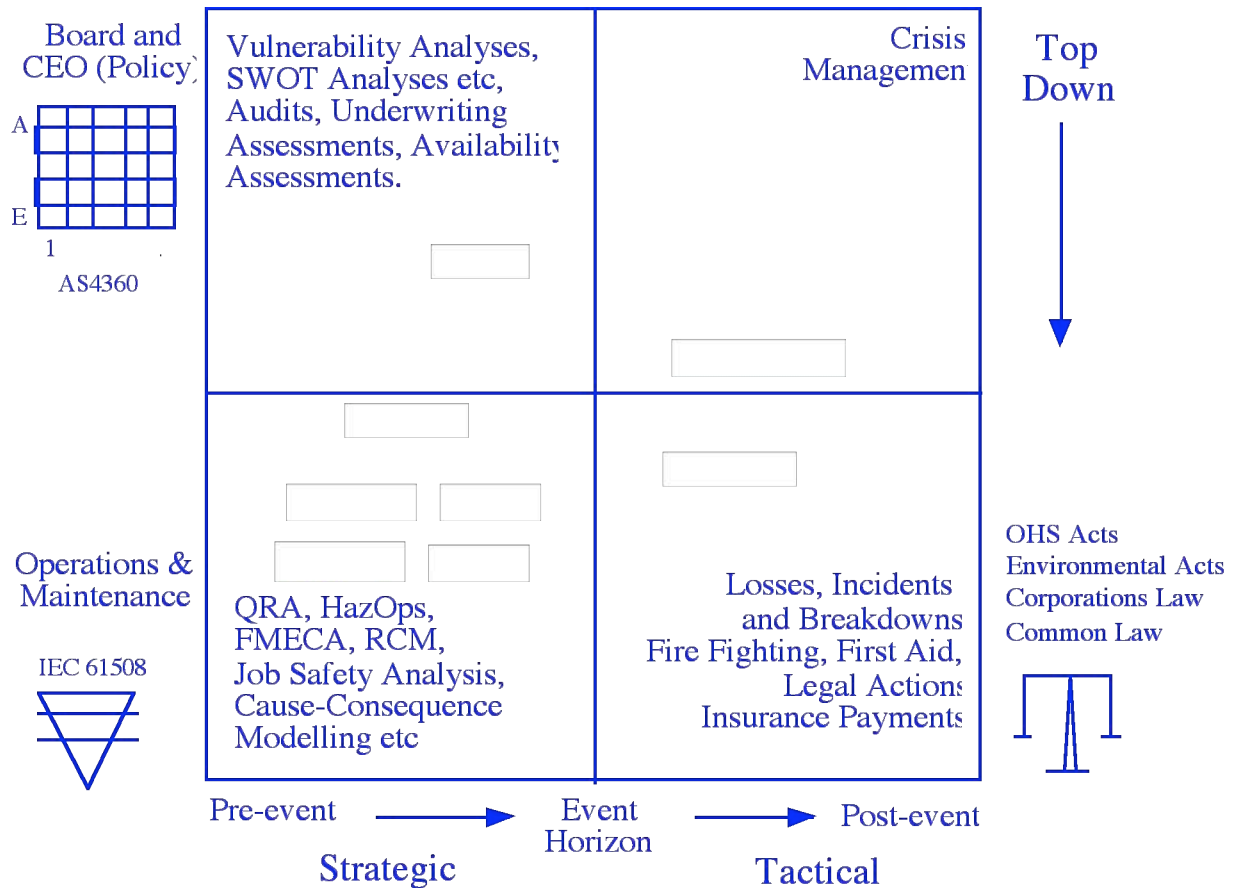


Technological to Business to Cultural Risk

The concept of a Safety Case is one interesting development.

2.9 Paradigm Integration

The figure below illustrates how and at what level the different paradigms are applied within a large organisation.



An Integrated Risk Paradigm Framework

3.0 Extension of Paradigm 6 - A water industry example

- The idea of focussing on service delivery to regulate water businesses.
- Customer service can be provided by integrated operation of all components in the delivery chain.

The process has the following key steps:

- Define key customers,
- Define availability requirements with key customers,
- Develop high level reliability block diagrams of service assets that provide the availability,
- Identify key hazards or vulnerabilities to service assets,
- Apply hazards to reliability block diagrams of service assets,

-
- f) Establish the reliability of each of the service assets in the chain,
 - g) Analyse effects of hazards on service availability to key customer groups, and
 - h) Establish the most efficient way to achieve required availability for key customers.

3.1 The Study

R2A undertook a study to develop a risk based approach to service availability modelling for the Victorian water industry last year under the auspices of the Department of Natural Resources and Environment and in association with Binnie Black & Veatch of the UK.

The purpose was to develop the concept of risk based availability modelling and prove the concept in an industry environment.

The approach has the following objectives:

3.1.1 Customer Service Focus

- Improved identification of customer service objectives
- Customer notification of service delivery

3.1.2 Increased System Efficiency at Better Cost

- Elimination of over-capitalising of plant
- Avoidance of system “gold-plating”
- Identification of system requirements
- Focused reporting on performance in provision of service to customers

3.1.3 Improved Relationships

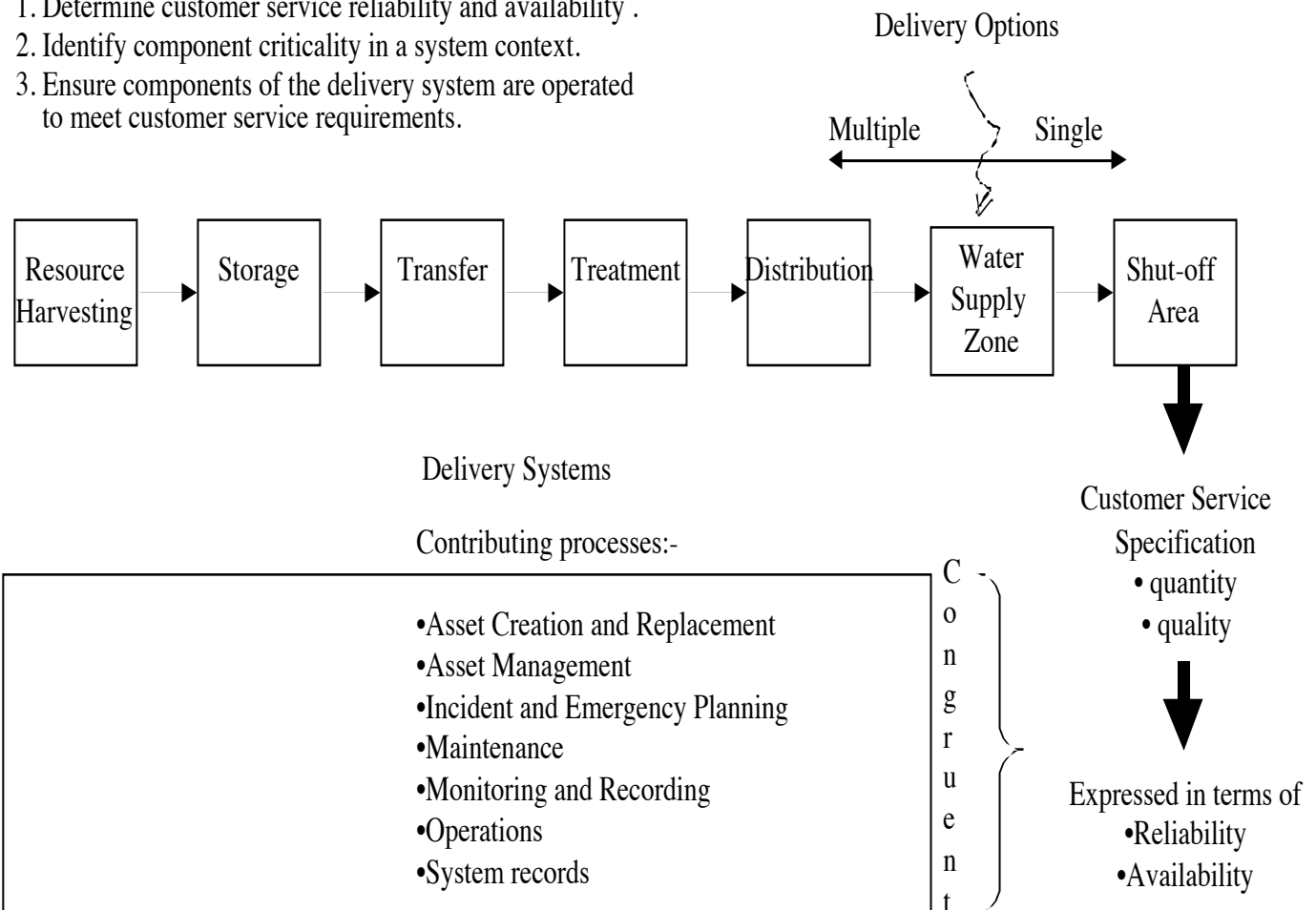
- Clarification - Regulator’s role in monitoring outcomes
- Clarification - service provider role - managing processes
- Improved harmony and efficiency of the relationships between all parties

3.1.4 Regulator ‘s Focus

- Output focus on service provided to the customer
- Confirmation of corporate performance
- Clearer expression of assets

Objectives

1. Determine customer service reliability and availability .
2. Identify component criticality in a system context.
3. Ensure components of the delivery system are operated to meet customer service requirements.



Focus on Customer Service Objectives

4.0 PROCESS AND DESCRIPTION

4.1 Define Key Customers

4.2 Define Availability Requirements for Key Customers

Possible options include:

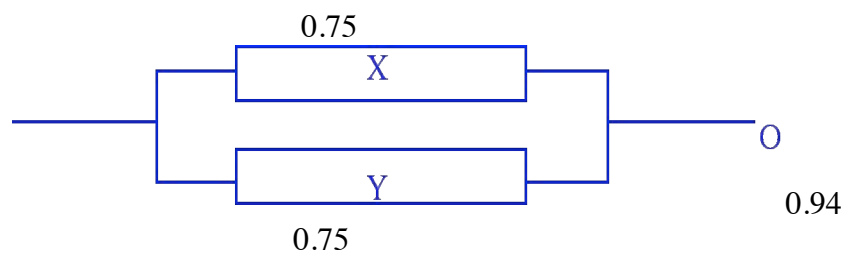
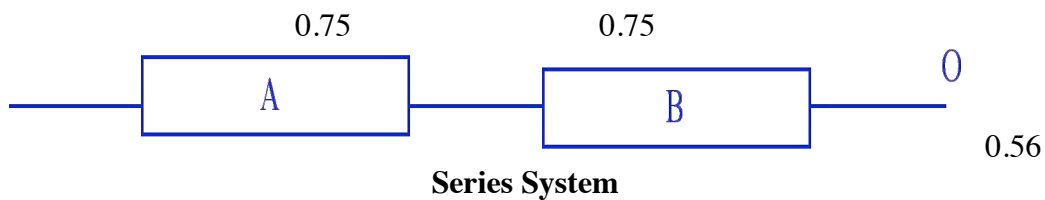
Event	Example Measure
Number of outages for shutoff area	5 per year
Average unavailability for shutoff area	4 hrs per outage

$$\begin{aligned}
 \text{Reliability} &= \frac{8760 - 20}{8760} \\
 &= 99.77\%
 \end{aligned}$$

Reliability	Unavailability (hrs)	Unavailability (days)
90%	876	36
95%	438	18
99%	87.6	3.5
99.5%	43.8	1.8
99.9%	8.76	
99.99%	0.876	

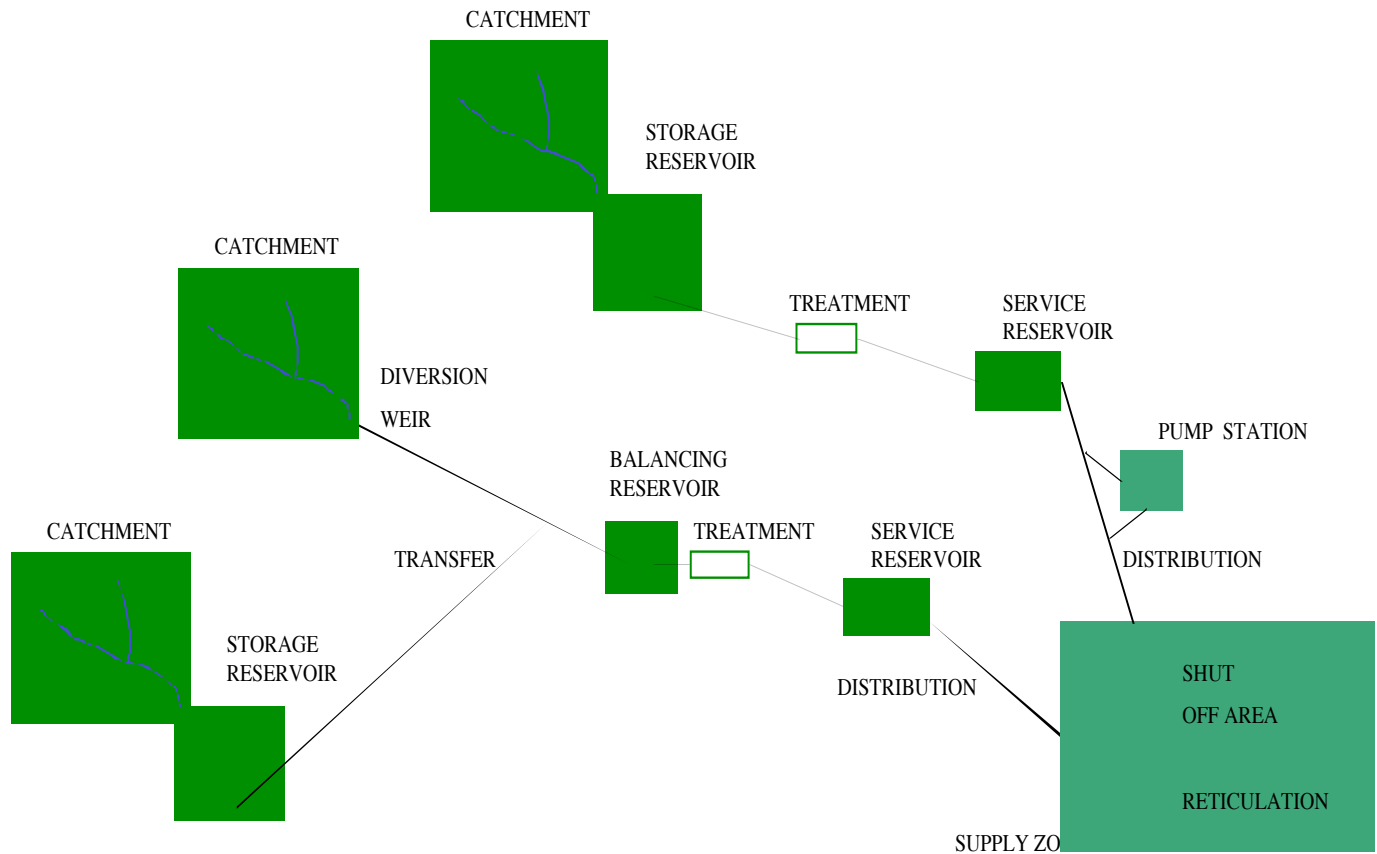
4.3 Develop High Level Reliability Block Diagrams of Service Assets

There are four basic configurations (BS 5760: Part 2:1994) namely; series, parallel (active redundant), m out of n units and cold standby. Models for the series and parallel configurations are shown below:

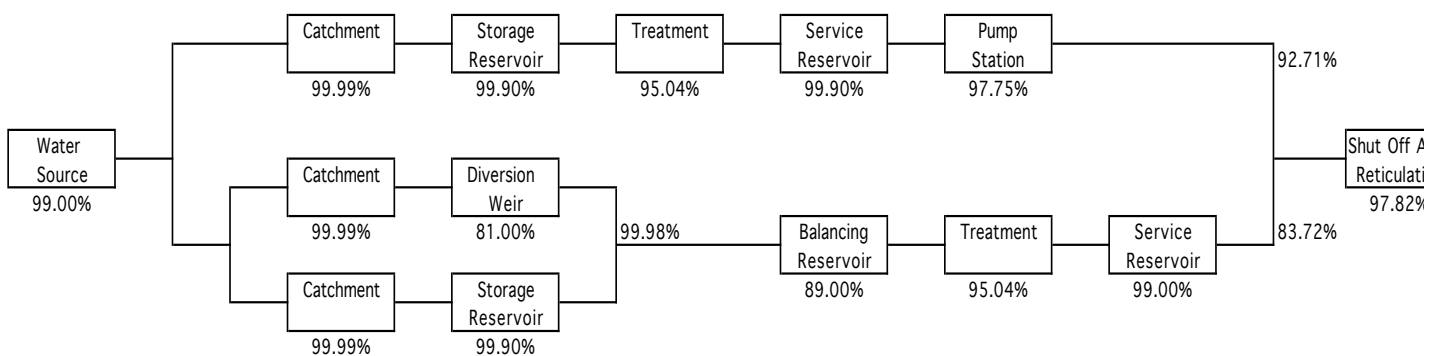


High reliability is achieved by low cost redundant systems rather than “gold plated” single systems.

The diagram below represents a service delivery system accompanied by its reliability block diagram.

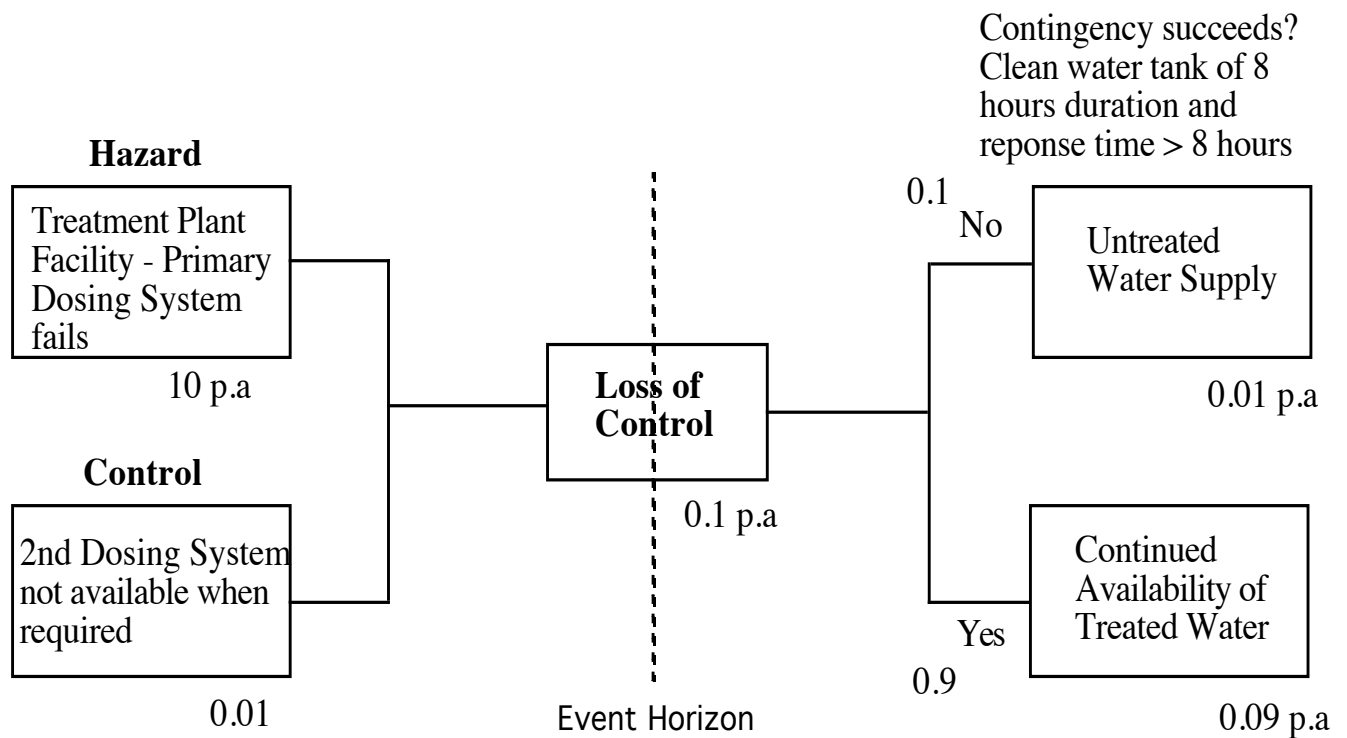


Customer service delivery depends on the reliability and availability of the upstream delivery system



Example reliability block diagram for the above service delivery system

Each block can be further reduced to other block diagrams, or alternatively, other tools, such as cause-consequence models can be used. For example the following is a cause consequence model for the failure of a dosing system at a water treatment plant facility.



Cause-Consequence Diagram for Water Treatment

If the untreated water supply outcome of 1 in 100 years is unacceptable then 3 options arise:

- Improve the reliability of the primary dosing system
- Improve the availability of the second dosing system
- If the dosing system fault detection and response time is greater than 8 hours then either the capacity of the clean water tank needs to be increased or an alternative consequence system is required.

That is, there are different control options each capable of improving the reliability of treated supply.

4.4 Identify and Characterise Key Hazards or Vulnerabilities to Service Assets

In this case, the hazards or vulnerabilities represent those things that have not yet gone wrong but perhaps could.

HAZARDS
VULNERABILITIES

OR

INCIDENTS AND
OCCURRENCES

	Like- lihood	Sev- erity	Risk
H1	0.1	2	0.2
H2	0.2	3	0.6
H3	0.05	50	2.5
H4	0.3	2	0.6
H5	0.65	13	8.45
H6	0.025	260	6.5
H7	0.001	1500	1.5
H8	0.45	0.5	0.23
H9	0.01	6	0.06
H10	0.5	60	30
H11	0.005	100	0.5
⋮			
Hi	0.003	1	0
ΣHi			51.1

	Like- lihood	Sev- erity	Risk
'I1'	0	2	0
I2	1	3	3
'I3'	0	50	0
I4	2	2	4
'I5'	0	13	0
'I6'	0	260	0
'I7'	0	1500	0
'I8'	0	0.5	0
'I9'	0	6	0
I10	1	45	45
'I11'	0	100	0
⋮			
'Ij'	0	0	0
ΣIj			52

<<< Pre-Event Control / Post-event Management

Concept Hazard (or Vulnerability) Registers

A table of sample likelihood and an example measure is given below:

Event	Example Measure
Likelihood of shutoff for >1 hour duration	10% per year
Likelihood of shutoff for >4 hour duration	1% per year
Likelihood of shutoff for >1 day duration	0.1% per year
Likelihood of shutoff for >1 week duration	0.01% per year

4.4.1 Hazard and Vulnerability Identification

Existing hazard and vulnerability identification processes would be used in the first instance. These would include HazOp (Hazard and Operability Study) and FMECA (Fault Modes, Effects and Criticality Analysis (the basis of RCM (Reliability Centred Maintenance) and well as historical records of maintenance works.

4.4.2 Risk Characterisation

This could be achieved in a number of ways but a calibrated risk matrix process would probably be effective for hazards or vulnerabilities that have not been manifest. Otherwise reference to comparative industry figures would probably be the simplest approach.

4.5 Apply Hazards to Reliability Block Diagrams of Service Assets

4.6 Establish Most Efficient Way to Achieve Required Availability for Key Customers