

ENTERPRISE AVAILABILITY PROFILING

Robinson, R M & Procter, T A
r2a@r2a.com.au

Increasingly organisations are required to demonstrate due diligence for the management of assets. Traditionally this has been done "stair-wise" bottom up, and not in the context of the organisation's Enterprise Risk Framework. This tends to leave the senior decision makers with an uncertainty as to the precise meaning of the results. Enterprise Availability Profiling uses a combination of top down and bottom up risk techniques to ensure that the final availability model meets the needs and expectations of boards, customers and regulators. It is especially useful when acquiring (or disposing) of an asset to confirm its proper potential value.

Keywords: Risk Management, Asset Management, Reliability, Availability

1 INTRODUCTION

Improved financial performance and greater reliability of supply to customers can be achieved by the application of various risk management techniques. Enterprise (risk-based) availability profiling uses both top-down and bottom-up approaches to ensure transparent decision making at all levels of management.

The approach can provide benefits to a wide range of customer service industries, their customers and industry regulators, for example, gas, water, rail, marine, aviation and power. Customers will see the benefits in specification and performance reporting on the actual service received (quality and continuity of service and supply). Industry will be able to improve the efficiency of their methods used to deliver this service and demonstrate due diligence in the management of assets. The regulator will be able to better evaluate the price/service trade-off for industry.

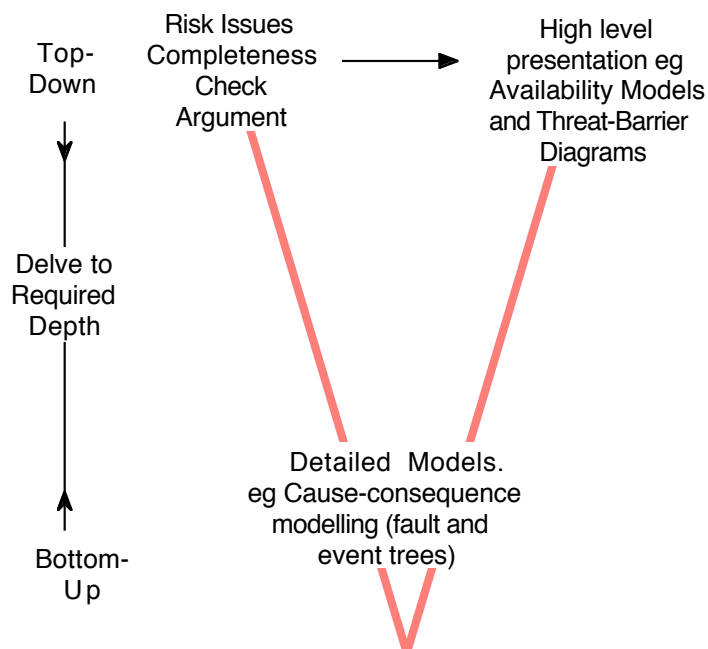


Figure I. Enterprise availability profiling risk context process

The R2A development process is shown above. Its primary strength is that the high level context is tightly defined so that the final availability profile meets the needs and expectation of boards, customers and regulators. That is, *enterprise* availability profiling really means *contextually tight* availability profiling. This contrasts with the more usual approach to availability, which is commonly done as a *stair* process from the bottom-up which, whilst not wrong, tends to leave the senior players with an uncertainty as to the precise meaning of the results. In a sense, this is risk engineers putting into the overall operating context the work of equipment reliability engineers.

2 METHOD

Three tasks are completed for Enterprise Availability Modelling and may be represented by the diagram below.

- i) A high level context (boundary) vulnerability analysis looking at the risk context. In the diagram below this is an examination of the credible boundary threats to the critical success factors of the plant or project.
- ii) A zonal assessment identifying the critical single point common mode or common cause failures such as issues associated with power supplies and the like. This can be done on a geographic and incident history basis. These are the typical common mode failures for which organisations currently purchase insurance, including for fire and explosions.
- iii) A high level functional availability analysis focussing on the identified critical elements.

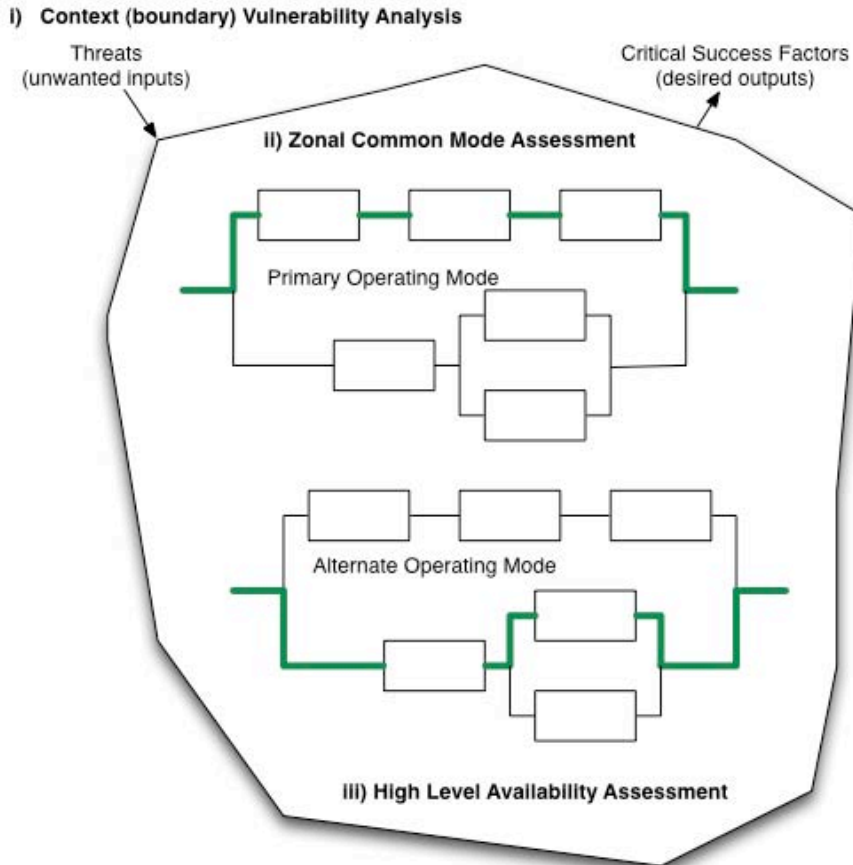


Figure II. Context of the three assessments

The central portion of the diagram shows the alternate operating modes in the event that the process under consideration has high level redundancy.

3 CONTEXT (BOUNDARY) VULNERABILITY ASSESSMENT

This context (boundary) vulnerability assessment involves a boundary being drawn around the system in question, with required inputs and outputs identified and located. High level system or process flow diagrams are often useful in this respect, as the boundary defined is often close to the physical boundary of the system. Such diagrams may be developed in a workshop.

It is usually completed as a half-day workshop with key stakeholders. This technique identifies the critical success factors and credible threats. A criticality assessment is then completed to identify overarching issues.

A vulnerability assessment is a high level military intelligence technique used to determine if there are any overarching issues that could prevent a mission from being successful. It simply asks two questions. "What are we trying to achieve?" (that is, required outcomes that need protection) and "What are the credible threats to these aims?" (unwanted inputs that might affect these aims). This usually results in a vulnerability matrix such as that shown below.

CRITICAL SUCCESS FACTORS >>> (Desired outputs)	Safe & healthy people (staff, contractors, etc.)	Product ontime delivery	Product quality & quantity	Safe & healthy community	Sound physical environment	Reliable equipment & assets	Compliance	Shareholder satisfaction
THREATS (Unwanted inputs)								
Alcohol / drugs	xxx	-	-	-	-	-	xxx	xxx
Bushfire	x	-	-	x	x	xx	-	xx
Change of ownership	x	-	-	-	-	-	-	x
Critical equipment failure	xxx	xxx	xxx	xx	xxx	xxx	xxx	xxx
Discrimination	x	-	-	x	-	-	x	x
Distribution failure	-	-	-	-	-	-	-	xxx
Extreme weather event	xx	-	-	-	-	x	-	xx
Fire / explosion	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx
Fraud	x	-	-	xx	-	-	-	xxx
Global warming	xx	xx	xx	xx	x	xxx	xx	xxx
Industrial action	xxx	xxx	xxx	xx	-	-	-	xxx
IT threat - business management system	x	-	-	-	-	-	-	x
Maintenance outsourcing	x	-	-	-	-	x	-	-
Noise / odour / dust	xx	-	-	x	x	-	xx	xx
Non availability of skills	x	x	-	-	-	xx	-	xx
Offsite utilities supply failure (water, gas, electricity, etc.)	x	xxx	xxx	x	x	-	x	xxx
Process control failure (IT)	xxx	x	xxx	xx	xxx	xxx	xxx	xxx
Raw materials supply failure	-	xxx	xxx	-	-	-	-	xxx
Raw product contamination	-	x	xx	-	-	x	-	xx
Regulatory regime change	-	-	-	-	-	xx	xxx	xxx
Sabotage / terrorism	xxx	xxx	xxx	xx	x	xxx	-	xxx

Figure III. High level boundary vulnerability assessment

Vulnerabilities are typically characterised as minor, moderate or critical using the following criteria:

- xxx** Critical vulnerability that must be (seen to be) addressed
- xx** Moderate vulnerability
- x** Minor vulnerability
- No detectable change
- v/a** Possible value adding

Figure IV. Vulnerability table key

Provided the list of assets is complete (those things that make the project, site or process successful) and the list of credible threats is complete then a strategic completeness check of potential vulnerabilities is achieved. Credible critical vulnerabilities (those assessed as ‘xxx’) are the priority for further risk assessment and characterisation. Note that in the table above likelihood is not considered beyond deciding whether or not a threat is credible.

An organisation's existing risk framework may be used for consequence and risk characterisation. In general, the vulnerability characterisation is as shown in Figure V below.

		-	x	x	xx	xxx	
LIKELIHOOD	Almost Certain	A	M	H	H	VH	VH
	Likely	B	M	M	H	H	VH
	Some chance	C	L	M	M	H	H
	Unlikely	D	L	L	M	M	H
	Rare	E	L	L	M	M	H
			1	2	3	4	5
			Noticable	Minor	Moderate	Major	Catastrophic
			CONSEQUENCE				

Figure V. 5 x 5 Risk characterisation matrix

(after Table 6.6 of HB 436:2004), showing “xxx” Criticality Consequence Values

4 ZONAL CRITICAL COMMON MODE FAILURES

The zonal assessment is designed to identify critical common mode (single point) failures on a geographic and incident history basis. This is to focus the availability and reliability modelling on the critical elements. This is usually done using incident history to date which is then tested against an experienced group of operators in a half-day workshop environment. Such a

process is consistent with the ideas in ARP 4761, the US Civil Airborne Safety Code. It might also be completed with insurance engineers since this is typically of primary interest to underwriters.

This step identifies failure modes which may fall outside silos of the organisation. Historically, large organisations have managed risk in organisational silos. Risk monitoring is often carried out by individual risk functions that measure and report their specific risks in different methodologies and formats. Consequently, senior management and the board receive pieces of the puzzle, but not within a unified framework. A view has emerged that such a fragmented approach simply doesn't work, because some risks are highly interdependent and cannot be segmented and managed entirely by independent units. In addition, some risks can fall outside the silos and might not be identified without some sort of formal overall completeness check. The enterprise risk framework diagram in Figure VI describes one understanding. When activities are undertaken bottom-up, each specialist group comes to an internalised understanding of what is important to the organisation.

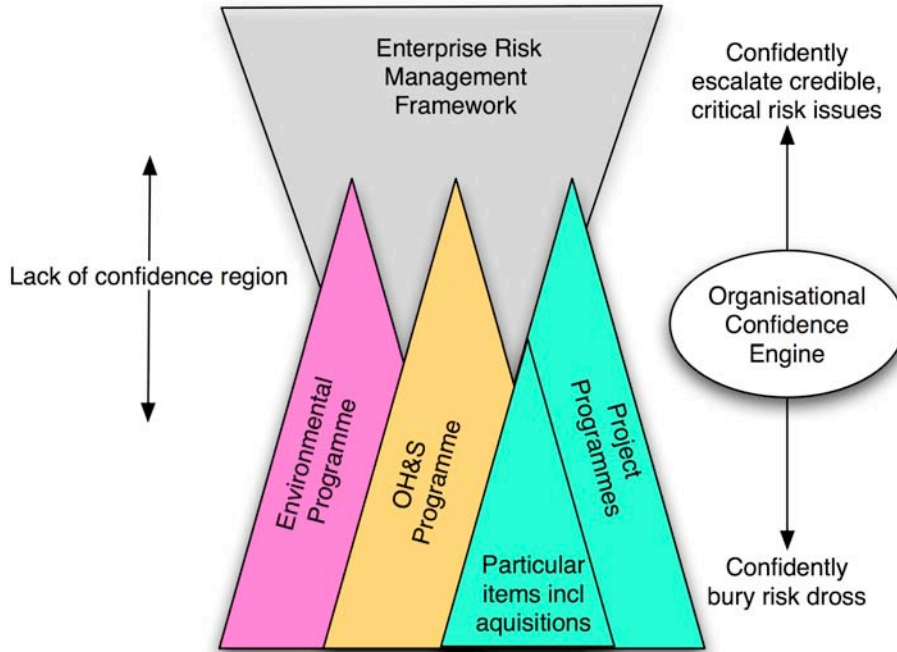


Figure VI. Enterprise risk framework

By focussing on failure modes which affect multiple sections of the plant or process, or which don't fit into the silos defined by the organisation, risks are fitted into the context defined in the boundary vulnerability analysis. This leads naturally on to the preliminary segmentation of the plant or process into functional sections affected by different common mode failures, rather than accepting without testing the organisational silos defined prior to the availability study.

5 FUNCTIONAL AVAILABILITY MODELLING

Risk-based availability modelling using system operating mode diagrams is the primary technique here. The key concept is to divide the system or process under consideration into sub-systems that are independent of each other and that all the interested parties can picture and agree represents the system as a whole.

Block diagrams are a simple way of representing complex systems diagrammatically, and can be used for both risk and availability studies. It is absolutely critical that as many interested parties as possible contribute, as any modelling done is on the basis that the block diagram is an accurate representation of reality for each particular study. All interested parties should sign off on the block diagram.

Subsystems may be in a series configuration (where failure of any subsystem results in failure of the overall system), or in parallel, where both subsystems must fail for an overall system failure.

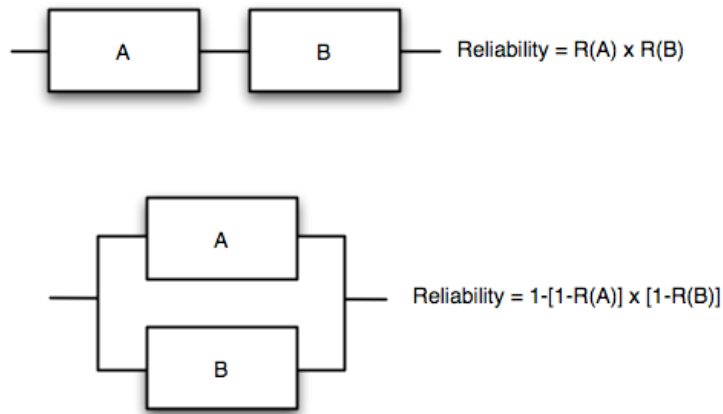


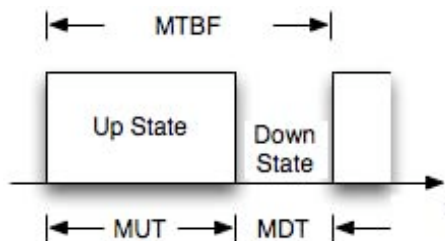
Figure VII. Basic blocks

Block diagrams can be drawn either based on reliability or availability.

In general, R2A Enterprise Availability Studies deal with systems rather than components. It is assumed that:

- i) systems operate continuously (including any possible scheduled breaks);
- ii) systems are repairable;
- iii) system availability has reached steady state, that is, enough time has passed from commissioning for the wearing in period to have negligible affect on system availability; and
- iv) systems have a constant failure rate (ie. random failures).

In this case, the availability of a system (or subsystem) is defined by the mean uptime (MUT) and the mean downtime (MDT). MUT is simply the length of time the component operates. MDT is the sum of scheduled and unscheduled maintenance and repair to the component, but does not include time when the component is idle due to lack of demand. If maintenance or repair are carried out in idle time they does not contribute to the MDT. For instance, if a component is required for 330 days/year and does not operate for 5 days due to mechanical faults, the availability is $325/330=0.9849$, rather than $325/365=0.8904$. MDT+MUT may also be referred to as the mean time between failures (MTBF).



$$\text{Availability} = \frac{\text{MUT}}{\text{MUT} + \text{MDT}}$$

Figure VIII. Mean uptime and mean downtime

If the availability of a component is required, R2A generally treat each component as part of a continuous system. That is, the average lifespan of the component is analogous to the MUT, and the average time taken to replace a component (following failure or scheduled maintenance) is analogous to the MDT. This is shown in Figure IX below.

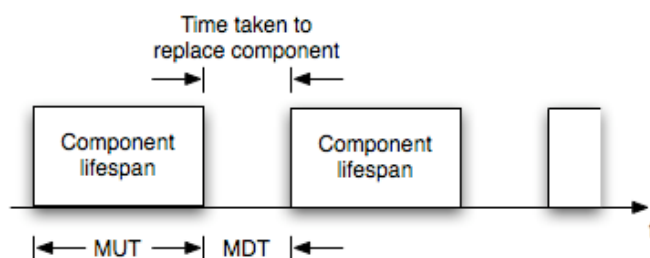


Figure IX. MUT and MDT analogies for components

Care must be taken when constructing models, as physical layout may not represent the functional arrangement. For instance, if two power feeds are physically in parallel but, alone, neither can supply enough power for the process, they are functionally in series. Critical process components show up as bottlenecks in the block diagram, as do any common mode failures identified in the previous step.

The representation will depend on the definition of success or failure adopted for the system. If there are multiple definitions (usually associated with alternate operating modes) separate diagrams may be required for each.

For example, the diagram below represents a simple service delivery system accompanied by its availability block diagram. Customer service depends on the availability of the upstream delivery system. There are different operating modes depending for example on reservoir maintenance requirements, reducing anticipated overall availability. This is in addition to unexpected plant outages and other vulnerabilities manifesting.

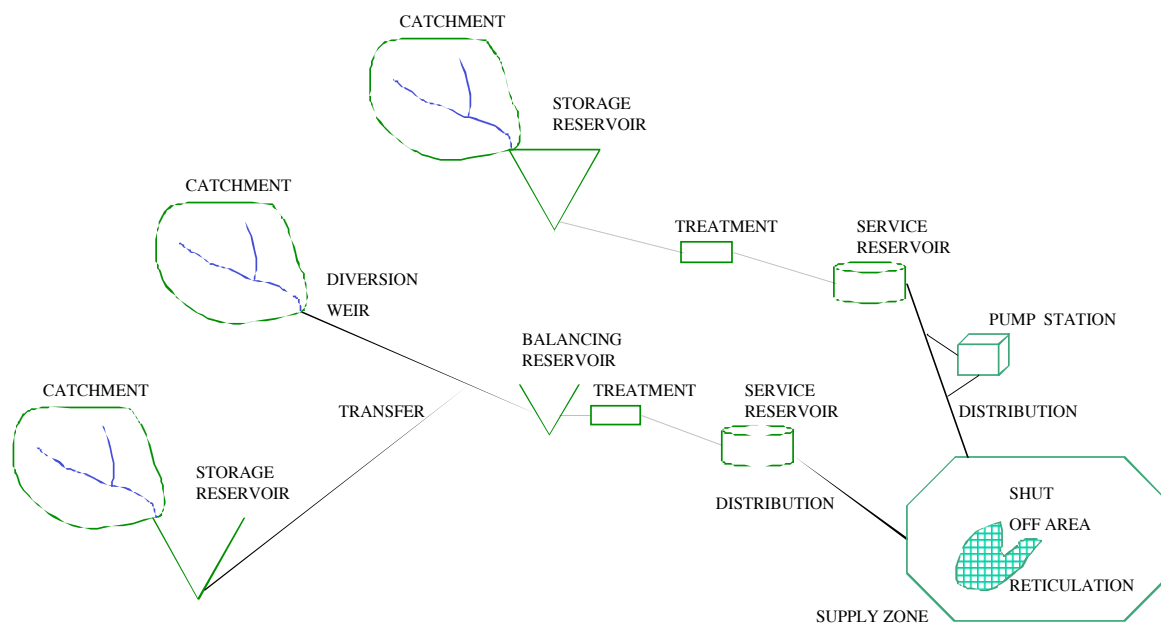


Figure X. Schematic Layout of a Water Supply Network

If the primary operating modes, the time in each mode and the availability of each mode is known then the annual expected customer supply can be projected. Critical vulnerabilities in achieving this cumulative target can be identified and explored. These can also be further risk assessed and characterised within existing organisational risk frameworks. This work is consistent with IEC 61508 and EN 50126. These high level system operating mode block diagrams are normally constructed in Microsoft Excel.

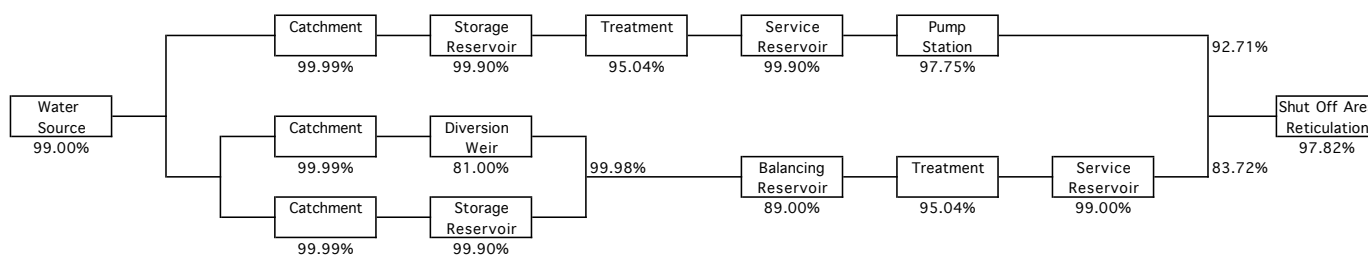


Figure XI. Availability block diagram

In the example above the two systems in series have a lower availability, 92.71% and 83.72% than the overall system in parallel, 97.82%, thereby demonstrating the benefit of having duplicated supply. Also worth noting is that despite all the individual components in the top system having an availability of >95%, the overall availability of the system is only 92.71% since they are in series. In the lower system, if the availability of the balancing reservoir were to increase from 89% to 98% then the lower system availability would become 92.19% instead of 83.72%.

Unless the experienced operators at the workshop advise otherwise, the model will be based on random failure rates over a peak period mission time and a mean downtime (MDT) for the alternate operating modes. This substantially simplifies the modelling as described below.

Each block can be further reduced to other block diagrams, or alternatively, other tools, such as cause-consequence models can be used (1 - success = failure). For example the following is a cause consequence model for the failure of a dosing system at a water treatment plant facility.

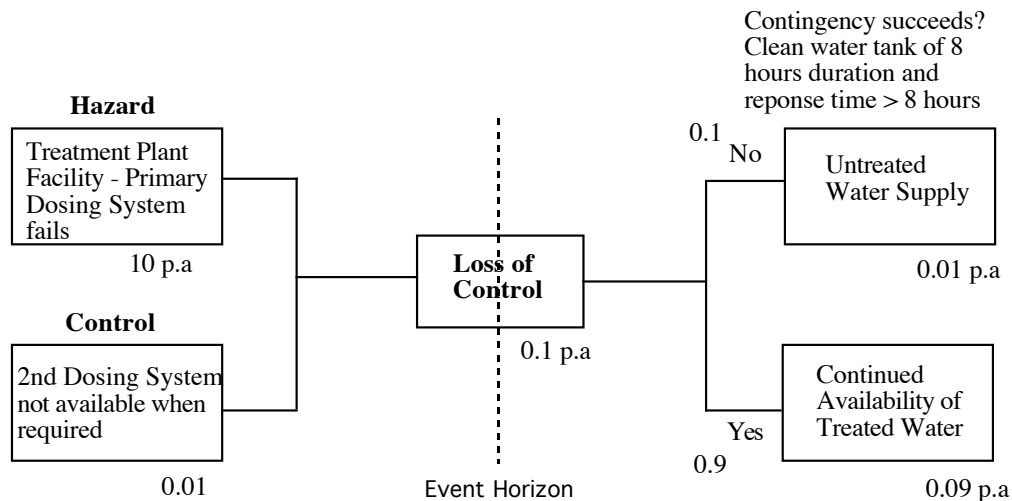


Figure XII. Cause-Consequence Diagram for Water Treatment

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

- i) Improve the reliability of the primary dosing system
- ii) Improve the availability of the second dosing system
- iii) 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 contingency plan is required.

That is, there are different control options each capable of improving the reliability of treated supply. One is probably more cost effective than the others.

6 GENERATIVE INTERVIEWS

In order to test the preliminary models and the results of the zonal assessment and context vulnerability assessment, a series of generative interviews should be conducted with representative key stakeholders. This is a worthwhile reality check in most situations and provides the most useful feedback to the proponent organisation.

7 CONCLUSIONS

In these times of "due diligence" the need to explain "everything" in ways that senior decision makers understand has become paramount. Enterprise Risk Profiling addresses this concern by placing reliability of systems into the downside risk context of major enterprises. This requires the convergence of existing risk and reliability skills described in this paper.

8 BIBLIOGRAPHY

1. British Standards Institution, *Reliability of Systems, Equipment and Components, Part 2: Guide to the Assessment of Reliability*, BS 5760:1994.
2. Institute of Electrical and Electronics Engineers Inc., *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, IEEE Std 493-1980.
3. Robinson, R M et al., *Risk & Reliability – An Introductory Text 6th Ed.*, R2A Pty Ltd, 2006.
4. Robinson, R M, *Risk Based Availability Modelling for Asset Management and Regulatory Purposes*, briefing paper for Systems Engineering Society, Engineers Australia, July 2000.
5. Rome Laboratory and Reliability Analysis Centre, *Reliability Toolkit: Commercial Practice Edition*, Rome, New York.
6. Sherwin, D J and Bossche, A, *The Reliability, Availability and Productiveness of Systems*, Chapman & Hall, London, 1993.
7. Smith, A M, *Reliability-Centred Maintenance*, McGraw-Hill, New York, 1993.
8. Smith, D J, *Reliability, Maintainability and Risk. Practical Methods for Engineers 4th Ed.*, Butterworth-Heinemann, Oxford, 1993.
9. Society of Automotive Engineers International, *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment*, ARP 4761, December 1996.
10. Standards Australia & Standards New Zealand, *Risk Assessment of Technological Systems*, AS/NZS 3931:1998.
11. Standards Australia & Standards New Zealand, *Risk Management* AS/NZS 4360:2004.
12. Standards Australia/International Electrotechnical commission, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC 61508-SER:2005.
13. Tweeddale, M, *Managing Risk and Reliability of Process Plants*, Gulf Professional Publishing, 2003.
14. Villemeur, A *Reliability, Maintainability and Safety Assessment: Methods and Techniques Vols. 1-2*, Vol. 1, trans. Anne Carter & Marie-Christine Lartisien. John Wiley & Sons, Chichester, 1992.