Edith Cowan University

Research Online

Australian Security and Intelligence Conference | Conferences, Symposia and Campus Events

2009

Consensual security risk assessment: Overcoming bias, conflicting interests and parochialism

Benjamin Beard

David J. Brooks

Follow this and additional works at: https://ro.ecu.edu.au/asi

 Part of the Hospitality Administration and Management Commons

Beard, B., & Brooks, D. J. (2009). Consensual security risk assessment: Overcoming bias, conflicting interests and parochialism. In D. M. Cook (Ed.)., *Proceedings of the 2nd Australian Security and Intelligence Conference, Kings Hotel, Perth, Western Australia, 1-3 December, 2009*. (pp. 41-54).
This Conference Proceeding is posted at Research Online.

Consensual security risk assessment: Overcoming bias, conflicting interests and parochialism

Benjamin Beard & David J. Brooks
Security Research Centre (SECAU)
Edith Cowan University

Abstract

In a risk assessment process, insular methods of data collection and analysis may lead to an inaccurate risk assessment as stakeholders hold individual biases, conflicting interests and parochial approaches to certain risks. The article considered these issues and tested a consensual risk assessment approach that can overcome many of these issues. A staged risk assessment process was applied within an entertainment complex in the Security, and Food and Beverage Departments. Eight supervisors from the two departments participated in the study, with each participants individually interviewed on their view of predefined risks followed by the same risks discussed within a facilitated group.

The study first identified a list of the twenty most important risks according to the two departmental managers. From this initial identification of risks, four supervisors from each department ranked, from highest to lowest, all twenty risks as individuals. Following this stage, the consensus activities involved four supervisors from one department who ranked all twenty risks as a group and with the aim that all participants had to agree. Finally, the consensus activity was repeated with all eight participants present. Such a staged approach allowed the various approaches and resulting outcomes from the various risk assessment methods to be compared. Such a comparison found that there was a need to gain common understanding or clear definition of risks within the group, that an individual's assessment of a risk was driven by their own perceptions and that less important risks held a more common view, whereas higher risk had a greater diversity of views.

Key words: security, risk, assessment, bias, consensus

INTRODUCTION

AS/NZS4360:2004 suggests that the risk assessment process should not be conducted or information gathered in isolation. Further to this view, HB167:2006 states that "people who work in an organisation often have very important information about weakness" (Standards Australia, 2006, p. 13). Taking an insular method of data collection may lead to inaccurate risk assessment, as stakeholders with vested interest may emphasise their own risks or worst, game the risk assessment process. Previous studies (Beard & Brooks, 2006) have demonstrated how a consensual risk assessment approach may result in a more acceptable risk assessment outcome when compared to individual assessments; therefore, this study further examined how this approach can be applied in another security risk management situation.

The field of risk management can be affected by small discrepancies in the information gathering process, resulting in significant impacts on the outcomes of a risk survey. To measure this affect, the research examined two methods of risk data collection in order to find the most appropriate approach. One method was *individual interviews* with the stakeholders. The second was a *facilitated risk meeting* with stakeholders to develop a consensus decision on risk. The method of data collection will be described and analysed, determining patterns and possible explanations.

RISK MANAGEMENT

Risk management provides a sensible approach to managing risk (Fischer & Green, 2004, p. 130) and a generic guideline is AS/NZS4360:2004 Risk Management. AS/NZS4360:2004 is often considered "almost a de facto global standard" (Jay, 2005, p.2) and has become an international template on dealing with risk, having been used in Canada, United Kingdom, and translated into Cantonese, Mandarin, Japanese, Korean, French and Spanish (Jay, 2005, p. 3). Most recently, AS/NZS4360 became the template for the International Standards Organisation ISO/FDIS 31000. Many industries use this framework and its applications are as broad as financial, engineering and security risk management (Jones & Smith, 2005a, p. 2).

The standard's definition of Risk is the likelihood of an event taking place that will have an impact upon the objectives of the organisation (Standards Australia, 2004, p. 4), combining likelihood and consequence in determining the amount of risk through a structured and logical approach. AS/NZS4360: 2004 Risk Management is the industry standard document for conducting risk projects and because of this, it formed the framework for the methodology of this study. Its flexibility and broad scope allowed the framework to be applied to the research of consensual risk analysis, as it is "widely used by security professionals and risk managers across Australia" (Jones & Smith, 2005b, p. 2).

The Australian Standard stages of the risk management process instruct that all relevant stakeholders need to be included in the process. According to the Standard, stakeholders are "those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk" (Standards Australia, 2004, p.6). Further to this aspect is the need to take a "consultative team" approach (Standards Australia, 2004, p. 19); however, it can be argued that the standard does not present the necessity of providing a consensual assessment (Koller, 1999; Koller, 2000), with an appropriate methodology with a consensus based stakeholder meeting.

The consensus methodology is supported by Koller (2000, p. 67), when he asserted that "maximum benefit from the risk processes is realized only when multiple opportunities are consistently assessed or compared", with a salient aspect of consistency being the arrival of a *consensus* (Koller, 2000, p. 68). The consensus approach may be supported, in particular for security risk, by the assumption that there is generally limited historical data. Without a consensus assessment, risks are assessed in isolation. Such an insular method of data collection and assessment may lead to inaccurate risk management, as stakeholders with vested interests may emphasise their *own* risks or *game* the risk assessment process. Also, assessors may bias the assessment process based on an individuals beliefs, perceptions and experience (Brooks, 2005).

CONSENSUAL RISK MANAGEMENT

AS/NZS4360:2004 Risk Management states that all stakeholders need to be involved in the risk management process; however, it does not specify how although a consensual risk approach is one of the options available. A consensual approach to risk management would ensure that all risks are detailed and agreed upon by all stakeholders (Koller, 2000, p. 222). This approach involves a round table meeting with all stakeholders that needs to end in some degree of a consensual outcome. By using this model, issues such as individual risk perceptions can be minimised and their impact on the final risk assessment minimised. When conducting a consensus risk assessment, group dynamics will also have some role and an independent facilitator should conduct the activity, considered a group analysis or working group (Chapman, 1998). The methodology used by Beard and Brooks (2006, p. 8) into consensual security risk management has been modified to provide more valid outcomes and several stages added to build upon limitations of the original study.

Whilst AS/NZS4360: 2004 Risk Management is an overarching risk framework, one area where it could be improved is with greater detail in respect to involvement of stakeholders and how this should be achieved (Standards Australia, 2004, p. 11). This aspect is of concern because of people's nature to adopt a parochial attitude towards their own vested interests. Heads of department will naturally try to skew risk assessments in their favour, ensuring budgets and structures remain or rise in their favour. This issue is of particular concern in the security industry, as *risk gaming* is a tool many security managers use in order to obtain approval from executive management for technologies they believe to be necessary and equivalent to the risk (Cubbage, 2005).

If skewed, baised or partially incorrect information is gathered in the earlier stages of the risk management process, than results at its completion will be invalid. The consensus approach should eliminate or reduce such discrepancies early in the risk assessment process by ensuring all parties agree and that no opinion overrides another. Such an approach should transcend many varying motives by gaining an outcome that is beneficial to all involved in the assessment (Koller, 2000, p. 228). Working group models have been successfully used to achieve an accurate and comprehensive risk management process and risk assessment in the construction industry (Chapman, 1998).

LITERATURE REVIEW

The area of risk and risk management has been widely documented in many industries as a way of making projects and facilities safer and more efficient. The application to the security industry allows for placement of resources into areas most needed. Security risk assessment and management is described as a method to identify the risks and the probable effects that they will have on the entity being protected to minimise that risk to an acceptable level (Fennelly, 2004, p. 9). The field of risk management in security has slowly evolved over the last few decades (Standards Australia, 2006) and the methods used grown.

AS/NZS4360 Risk Management standard presents a framework (Figure 1) on how risk managers could conduct an assessment,, being recognised throughout the world and used in many different languages (Jay, 2005, pp. 2-3). The standard provides a solid framework for the risk management process, beginning with *Establish the Context*, where the scope is set, and all stakeholders identified and involved. Next, the risks are *Identified, Analysed* and *Evaluated* and finally, risks are *Treated*. Concurrently with the risk assessment stages, the process is *Monitored and Reviewed* with stakeholders constantly *Communicated and Consulted* (Standards Australia, 2004).

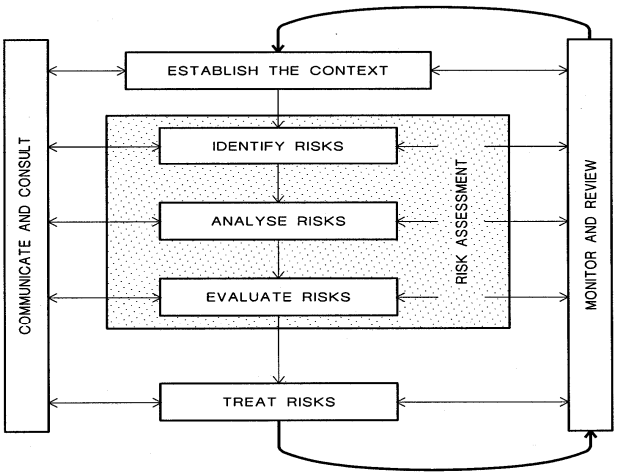

Figure 1 Risk management
(Standards Australia, 2004)

The field of project management uses a large amount of risk assessment, and several methods of data collection that are poignant to both the security industry and this study. Kerzner (2003) stated that risks needs consideration in project management, along with costing and schedule. He favours several methods for achieving, this including:

- Individual interviews with stakeholders
- The Delphi method and
- The Nominal Group Technique (Kerzner, 2003, p. 666)

Individual interviews involve the facilitator gathering information from each stakeholder and then conducting the analysis and evaluation stages. The Delphi method firstly selects a panel of experts, consisting of decision-makers, staff and leading project staff (Turoff, 1970). Each expert makes an opinion on the chosen risk subjects, which is anonymously compiled by the facilitator. This feedback is redistributed to the panellists, who then make new opinions based upon the new information. The process is completed as often as is necessary to achieve the desired level of accuracy.

The Nominal Group Technique (NGT) was developed from social-psychological studies into decision-making in groups (Delbecq, 1968). The NGT is similar to the Delphi method; however, the participants have direct contact and all ideas are placed onto a flip chart without discussion. These ideas are discussed in the group and prioritised using a mathematical aggregate and repeated as often as necessary (Kerzner, 2003, p. 666). These approaches are used in the construction and project management industries; however, restricted research has been conducted into evaluating their effectiveness against the standard brainstorming technique proposed in risk management guidelines (Standards Australia, 2006) or their use in the specific security risk management field.

A study conducted an analysis of brainstorming techniques, namely the Delphi method and NGT using the model of the determinates of group effectiveness (Chapman, 1998; Handy, 1983). Chapman stated that there are three distinct categories of risk data collection; identification solely by the facilitator, the facilitator interviewing stakeholders and the facilitator leading a *working group*. Using the model proposed by Handy, Chapman compiled a list of the strengths and weaknesses of the three types of working groups (1998). In general, the study found that generating a group of participants that would work well together was very low regardless of the technique used. The use of these techniques in project risk management are documented; however, studies into *working group* techniques within security risk management are restricted.

One such study was considered by Beard and Brooks (2006) and their study into the use of a consensus approach in security risk management. Such a consensus approach involved gathering together all of the stakeholders in various departments of an organisation and working through the analysis and evaluation stages with the conclusion being a consensus, or all around agreement. By comparing this method with individual interviews and facilitator evaluation, it was found that a more rounded assessment could be gained with a consensus method. Otherwise participants tended to adopt a parochial attitude towards risk that affected or could be considered relevant to their own department (Beard & Brooks, 2006). This study used this approach to develop a methodology and analysis of a consensus approach. The overall goal was to create a set of identified and analysed risks, with relevant treatment options regarding security and liquor licence requirements.

STUDY DESIGN

The design for the study (Figure 2) outlines the AS/NZS4360:2004 risk management framework (Figure 1) as the foundation for the study. Following this initial approach, the subsequent stage involved individual risk analysis for two distinct departments, with the final stage containing a consensus approach to risk analysis for Department 1 and both groups.

The study applied the risk assessment process in a large entertainment complex, within the Security Department (Department 1), and Food and Beverage Department (Department 2). The scope for the risk assessment process and the identification of the most significant risks concentrated on risks that affected both departments concerning infringements under the Liquor Licensing Act and the possible loss of the complex license. Eight supervisors, four from each department, participated in the study.

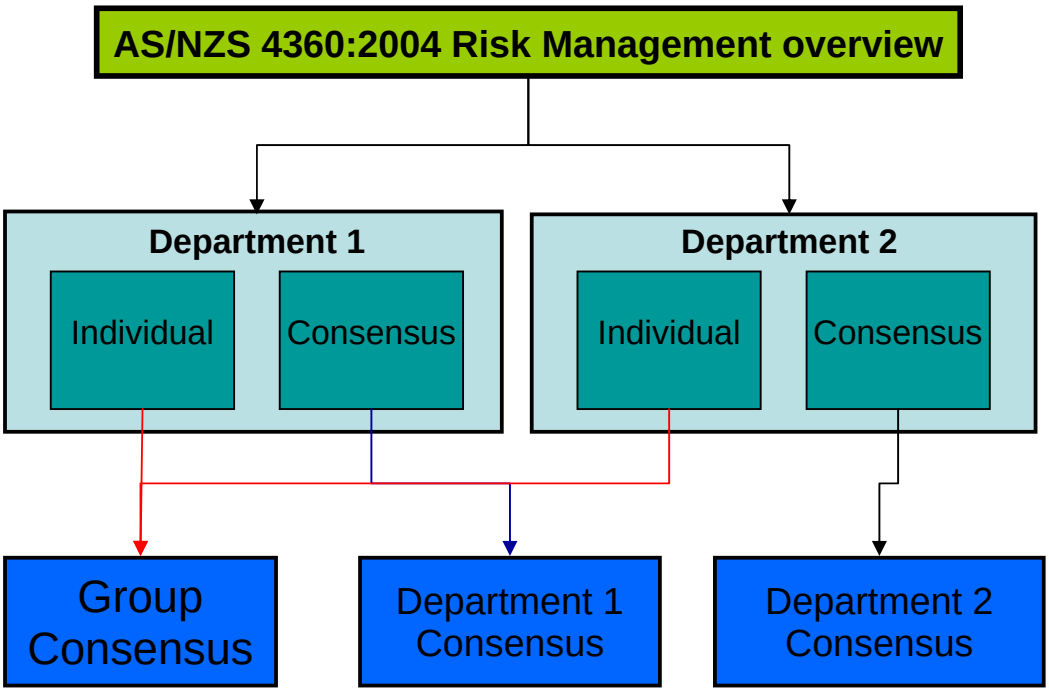

Figure 2 Study design

The study commenced with consultation with the site managers from both departments, with regard to the suitability and practicality of conducting the study. In addition, the scope for the identification and analysis of the risks was defined. In order to achieve a thorough research methodology, a pilot study was completed. This pilot study required a brainstorming session with the managers to create a list of ten risks. Using these 10 perceived risks, the managers individually listed the risks in order of highest to lowest (Cohen, Manion, & Morrison, 2000, p. 252). Again, using the 10 perceived risks, the managers ordered the risks by working together and arriving at a consensus of the risks from the highest to lowest. The results and comments gathered from this activity were used to improve the methodology for the larger group activities.

The first stage of the prime study was to identify the risks involved in the assessment, achieved with the assistance of the department managers (Standards Australia, 2004, p. 16). The managers brainstormed a list of twenty important risks that were to be assessed. These risks were listed on a survey form for the individual assessment activity and embedded into handout documents for the consensus activities. Following identification of risks, two methods of risk analysis were used and a comparison made. As individuals, four supervisors from Department 1 ranked all twenty risks from highest to lowest, repeated with four supervisors from Department 2.

The consensus activities involved arranging a meeting with all four supervisors from Department 1 that took part as an individual activity and having them rank all twenty risks. This activity was completed with a consensual outcome, as all participants had to agree as near as was practicable. Again, the activity was repeated with all eight participants present, which took longer due to the wider differences of opinion in the larger number of participants. The final stage for this activity was to discuss treatment options for the top five ranked risks.

ANALYSIS

The analysis of the primary data (Table 1) presents the average results for both the department's individual assessments, as well as the average of the individual assessments, Department 1's consensus assessment and the combined consensus assessment.

Risks	Department1 Av	Department2 Av	Individual Av	Department1 consensus	Overall consensus
Risk A	9.5	16	14.75	8	17
Risk B	11	12.75	13.25	1	2
Risk C	4.75	5	5.5	4	1
Risk D	10.75	9	9.875	11	14
Risk E	5.5	7	6.25	12	11
Risk F	15	11	13	15	8
Risk G	9.25	4.5	6.875	6	9
Risk H	4.25	4.25	4.25	5	4
Risk I	17.25	17.75	17.5	17	20
Risk J	8	7.5	7.75	13	12
Risk K	13.25	9	11.125	16	13
Risk L	13.25	14.5	13.875	9	15
Risk M	5.25	4	4.625	2	5
Risk N	10.75	9.75	10.25	14	6
Risk O	5.25	11.5	8.375	3	3
Risk P	14.25	15	14.625	19	16
Risk Q	8.75	9	8.875	10	10
Risk R	19.25	15	17.125	20	19
Risk S	17.5	16.75	16.25	18	18
Risk T	7.25	10.75	9	7	7

Table 1 Risk comparison between departments

In considering the differences between the collected data (Table 1), the views of the two departments are similar to some degrees. There is however same large variances when comparing the individual assessments to the two consensus assessments. When comparing the average individual security response to the security consensus, the results are relatively similar with some exceptions such as *Risk E* and *Risk J*. The combined consensus group results, when compared to the other results, demonstrate the most difference. Whilst most of the risks remain ranked in the same quartile, there was noticeable movement in the rankings.

The average risk rankings from the Department 1 individual responses, the Department 2 individual responses and an all responses were calculated. These results show that the individual risk rankings between the two departments did not vary as much as anticipated. *Risk A* and *Risk O* were the only risks with a significant discrepancy between the two departments.

The standard deviation of each cohort were extracted (Table 2). The lower the value of the standard deviation in the combined individual results, the more aligned the individual assessments are. This demonstrates that risks such as *Risk I* and *Risk K* are ranked in the consensus, as all of the participants had similar individual rankings and the variance between the assessments was low (2.67; 3.31). Nevertheless, there were risks with higher standard deviation values, such as *Risk D* (6.62) and *Risk B* (6.99), with a lower degree of consensus in the group activities. The differences between the two department's standard deviation values and the combined consensus values could indicate that there is differences in the departments with high values and that a particular risk, with a low standard deviation value, is considered equally by all members of the group.

Risks	Consensus	Department1	Department2	All individuals
Risk A	17	5.06	4.83	5.75
Risk B	2	6.68	8.22	6.99
Risk C	1	3.20	2.58	2.69
Risk D	14	7.41	6.73	6.62
Risk E	11	2.38	3.74	3.01
Risk F	8	4.08	5.94	5.18

Risk G	9	2.36	3.10	3.60
Risk H	4	2.87	2.62	2.54
Risk I	20	1.25	3.86	2.67
Risk J	12	5.35	5.68	5.11
Risk K	13	1.50	3.36	3.31
Risk L	15	7.32	1.00	4.88
Risk M	5	3.50	3.55	3.33
Risk N	6	5.37	3.20	4.13
Risk O	3	3.59	5.80	5.57
Risk P	16	3.86	1.82	2.82
Risk Q	10	3.30	2.58	2.74
Risk R	19	1.50	6.68	5.02
Risk S	18	1.29	3.86	2.69
Risk T	7	4.19	3.30	3.96

Table 2 Risk standard deviation comparison between departments

EVALUATION AND FINDINGS

The results detailed above demonstrate that the aim of comparing and contrasting the individual and consensual approaches to security risk assessment were achieved. Such an outcome allows several important assumptions to be made, including the need to gain common understanding or clear definition of risk within the group, that individual's assessment is driven by their own perceptions and that less important perceived risk held a more common view whereas higher risk had a greater diversity of views.

First, in conducting an analysis of risk management and assessment methods, the pilot study and scope and identification stages indicated that the situation and risks must be clearly defined. In addition, that the risk scope carefully controlled in order to give appropriate results toward the risk assessment task. This study achieved this in two stages, which shaped the remainder of the methodology and activities.

Second, the individual approach to risk analysis appeared to produce varying results in the risk rankings. Whilst this was expected, due to individual opinions, there were very few patterns in the differences in each department. Such limited differences infer that the participants did not adopt a parochial attitude towards the risks that affected their area the most. This appeared to contradict previous results, which purported that people skew risks to favour their interests (Beard & Brooks, 2006). Overall, the averages of the individual risk rankings did not vary greatly from the individual department average or combined individual averages. Such an outcome supports the argument that the participants from all departments viewed the majority of the risks with the same attitude and therefore, consensus results from both the individual and the combined rankings.

Nevertheless, the consensus rankings are slightly different to the results found in the individual results, perhaps caused by the collaborative thinking and discussion of the risks. By using a group of people to discuss an issue, the result may broaden the participant's perceptions and curb any extreme views on the subjects. The two consensus activities' produced differing sets of results; however, the majority of risk movement was contained. Such a result may indicate that the two consensus groups were both regarding the risks with the same levels of concern, improving the accuracy of the combined consensus results.

The standard deviation adds an interesting outcome to the findings. These figures indicated that if a risk had a low standard deviation value in the individual rankings, it therefore had a strong and accurate rating in the consensus rankings. Such an outcome could be expected when considering a common measure and therefore, risk view. It is of importance to note that the risks with the lower standard deviation values also had a lower risk ranking, often in the last five ranked risks. This result could highlight that there was little discrepancy amongst the participants with regard to those risks that was considered the least importance. Therefore, the risk that had a high ranking and a higher standard deviation was considered important by the participant. In addition, the discussion in the consensus groups was especially exhaustive for the rankings of these risks. The standard deviation process could prove to be useful to management of organisations conducting risk assessment, as a method of gauging accuracy and effectiveness of risk rankings.

LIMITATIONS OF THE STUDY

There were several elements of the study that could have been improved. The methodology was solid and well structured; however, there were minor problems with application due to the organisational aspects of having eight

managers of a busy company attend the one meeting. The reliability and validity aspects could have been addressed more thoroughly throughout the study. One approach to address the problem of validity would be to a have a third group of participants conducting risk ranking and use this as a control group for comparison. To improve reliability, repeating the entire process at another organisation would provide another data set for comparison. Finally, a larger study that used the methodology presented in this study could be applied to a larger and more diverse group within or across several similar organisations. Such a study would further validate the findings and assumptions put forward in this study.

CONCLUSION

Security risk management is increasing used to direct limited resources in the mitigation of threat; however, risk management can result in these limited resources directed in an inappropriate or less effective manner. Risk management should include a number of discrete steps, with risk assessment embedded within these steps and incorporating risk identification, analysis and risk evaluation. It is at this assessment stage that many factors may result in the risk management process being less than effective, including individuals perceptions of risk, parochial attitudes, invested interests, undefined risks, bias or a limited understanding of a risk. To overcome these issues, some form of group consensus should be achieved.

The article has presented a study that considered an approach that compared and contrasted individual and consensual approaches to security risk assessments. An organisation's group managers from two related divisions assessed a number of predefined risk, where the results were analysed and interpretations made. The study found that there was a need to gain common understanding or clear definition of risks within the group, that individual's assessment is driven by their own perceptions and that less important perceived risk held a more common view, whereas higher risk had a greater diversity of views. The study indicates that the use of different methods of risk assessment should consider the situation, using such approaches as group interviews, Delphi method and nominal group techniques. In addition, the results gathered from such group approaches can be used to ascertain accuracy and importantly, can confidently be used to allocate resources to minimise security threats.

REFERENCES

Beard, B., & Brooks, D. J. (2006). Security risk assessment: Group approach to a consensual outcome. *Proceeding of the 7th Australian Information Warfare and Security Conference*, 5-8.

Brooks, D. (2005). Is CCTV a social benefit? A psychometric study of perceived social risk. *Security Journal, 18*, 19-29.

Chapman, R. J. (1998). The effectiveness of working group risk identification and assessment techniques. *International Journal of Project Management, 16*(6), 333-343.

Cohen, L., Manion, L., & Morrison, K. (2000). *Research methods in education*: London: Routledge.

Cubbage, C. (2005). Module 1: introduction to security risk. [Handout]. Edith Cowan University, Perth.

Delbecq, A. L. (1968). The world within the span of control, managerial behaviour in groups of varied size. *Business Horizons, 11*(4), 47-57.

Fennelly, L. J. (2004). *Effective physical security*. Boston: Elsevier.

Fischer, R., & Green, G. (2004). *Introduction to security. (7th ed.).* Boston: Butterworth-Heinemann.

Handy, C. (1983). *Understanding organisations*. Middlesex: Penguin Books Ltd.

Jay, C. (2005, 17 March). Big debacles help shape a new science. *The Australian Financial Review,* p. 2.

Jones, D. E. L., & Smith, C. L. (2005b). *The development of a model for the testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS4360:2004 - risk management.* Paper presented at the 2005 Recent Advances in Counter-Terrorism and Technology Summit, Canberra.

Kerzner, H. (2003). *Project management: a systems approach to planning scheduling and controlling*. Hoboken: Wiley & Sons.

Koller, G. (1999). *Risk assessment and decision making in business and industry: A practical guide*. Boca Ratan: CRC Press.

Koller, G. (2000). *Risk modeling for determining value and decision making* Florida: CRC Press Ltd.

Standards Australia. (2004). *AS/NZS 4360:2004 Risk management.* Sydney: Standards Australia.

Standards Australia. (2006). *HB 167:2006 Security risk management*. Sydney: Standards Australia.

Turoff, M. (1970). The design of a policy Delphi. *Technological Forecasting and Social Change, 2*(2), 149-171.

COPYRIGHT

Benjamin Beard & David J Brooks ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Energy Security: An Australian Nuclear Power Industry

Geoff I Swan
secau -Security Research Centre
Edith Cowan University

Abstract

Climate change and energy security are driving a worldwide renaissance in nuclear power. An Australian nuclear power industry has also been seriously investigated by the Australian government and its agencies. This paper provides a broad overview of the nuclear fuel cycle and the nuclear power industry. It identifies aspects that are sensitive to nuclear terrorism and nuclear weapons proliferation to help security professionals identify threats and prepare for a possible Australian nuclear power industry.

Keywords

nuclear power, energy security, uranium, radiation

INTRODUCTION

It has been fairly widely accepted for decades in the scientific community that massive amounts of carbon dioxide (CO_2) emitted into the atmosphere by humans would increase the "greenhouse effect" resulting in global warming and other climate change. The most recent fourth assessment report of the Intergovernmental Panel on Climate Change (IPCC, 2007) makes it clear that carbon dioxide is the most important anthropogenic greenhouse gas affecting the Earth's energy balance, with the primary source being the burning of fossil fuels (coal, oil and gas). A global warming of 0.2˚C per decade is projected over the next two decades and rises of several degrees this century are expected if CO_2 emissions are not reduced.

In Australia, over 96% of electricity generation (in terms of fuel inputs) is from coal, gas and oil (ABARE, 2009a). Hydroelectricity is our main "clean" electricity generation source which does not emit carbon dioxide. Although significant growth is likely in other "renewable" sources like wind generators, these are currently not suitable for base load power. Nuclear power plants can supply large amounts of base load power and do not emit greenhouse gases. With Australia's natural wealth in uranium the nuclear option is being promoted, by some, as a "clean" source of base load power and an effective medium term action to reduce climate change.

The year 2006 was pivotal in Australia with a nuclear power industry being seriously investigated through two comprehensive reports. The first report was commissioned by the Australian Nuclear Science and Technology Organisation (ANSTO) to look at the economics of nuclear power in the Australian context (Gittus, 2006). In the second half of the year, a taskforce was appointed by the Prime Minister to investigate and report on uranium mining, value-added processing, and the contribution of a nuclear energy industry in Australia (Commonwealth of Australia, 2006). In summary, while high commercial and technology barriers could make Australian conversion, enrichment and fuel fabrication facilities difficult to build, there was support for an expansion of uranium mining, and nuclear power was considered economically feasible. The release in late 2006 of Al Gore's academy award winning documentary film on climate change "An Inconvenient Truth" (2006), enhanced public perceptions of a crisis that is driving the debate on nuclear power in Australia.

Despite having huge natural energy resources, Australia could find its energy security under threat from the international community that may not accept our huge carbon footprint. Australia has recently overtaken the United States of America as the world's biggest emitter of CO_2 per capita (Maplecroft, 2009), and globally enforced carbon emission caps may emerge as part of a global response to climate change. Australia may be forced to quickly reduce our reliance on fossil fuels or face sanction.

This paper provides a broad overview of the nuclear power industry with the nuclear fuel cycle described in sufficient detail for security professionals to better appreciate security issues. Reference will be made to those aspects of most concern for nuclear terrorism and nuclear weapons proliferation. Regulation, safeguards and international experience are also addressed.

NUCLEAR FUEL

Overview

Figure 1 shows a schematic diagram of the nuclear fuel cycle for nuclear fission power reactors. The front end of the nuclear reactor can be considered as two stages. Firstly, uranium ore is mined and processed to produce yellowcake (U_3O_8). This normally occurs at or near the mine site. Secondly, specialist facilities are needed to enrich uranium and produce fuel that a nuclear power station can use to produce electricity. Finally, the spent fuel is managed through storage, reprocessing and waste disposal.

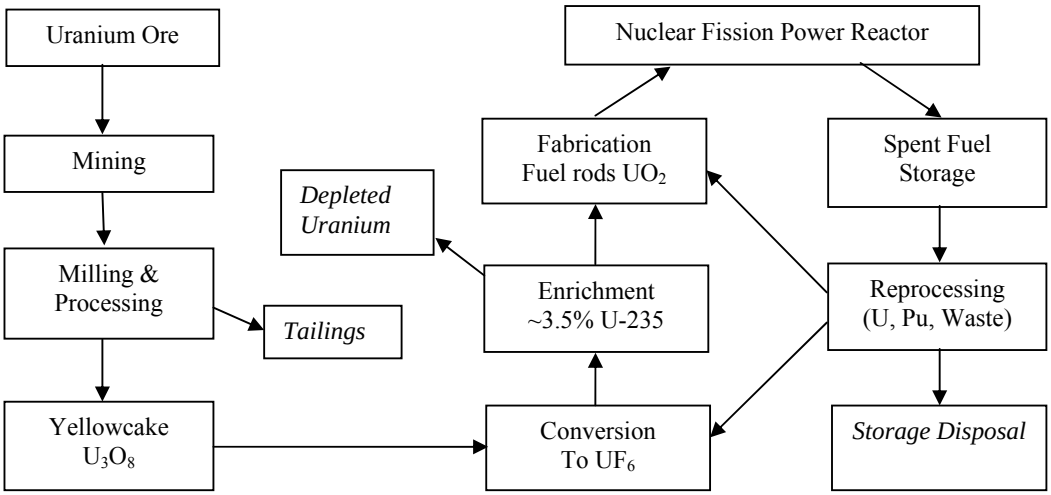

Figure 1. Schematic diagram of nuclear fission power reactor fuel cycle

Uranium ore to yellowcake

Australia has the world's largest known recoverable uranium deposits (23%) in the world with major producers Canada and Kazakhstan account for about 60% of world supply of uranium for nuclear reactors from mines (World Nuclear Association, 2009). Natural uranium on Earth is radioactive and made up of 99.3% U-238 and just 0.7% U-235. Both U-238 and U-235 are alpha particle emitters with half lives of 4.5 billion years and 704 million years respectively (Thornton and Rex, 2006). The long half lives and dispersed nature of the uranium deposits make them not particularly radioactive. In the financial year 2007/2008, the three currently operating Australian mines at Ranger (NT), Olympic Dam (SA), and a small mine at Beverly (SA), produced a total of 10,101 tonnes of yellowcake (ABARE, 2009b). Yellowcake has a low specific radioactivity and is transported in 200 litre drums and loaded into shipping containers for enrichment overseas. World uranium mining will probably need to greatly expand in the coming decades due to an increasing number of nuclear power stations and a probable reduction in (currently 40%) nuclear fuel derived from decommissioned American and Russian nuclear warheads (ASNO, 2008) under the Treaty on the Reduction and Limitation of Strategic Offensive Arms (START).

Conversion, enrichment and fuel fabrication

Through chemical reactions, yellowcake (U_3O_8) is converted to uranium hexafluoride (UF_6) before the technologically challenging task of enriching the U-235 abundance from its natural 0.7% to between 3% and 5%. This is necessary for use in almost all nuclear power reactors as it is the U-235 isotope that is fissile and can therefore produce energy. Whilst other enrichment methods have been used in the past or are under development, the centrifuge method now dominates the international uranium enrichment industry. When uranium hexafluoride is fed into a swiftly rotating cylinder (centrifuge) there is a slight separation of the isotopes with the lighter $^{235}UF_6$ having a slightly higher concentration near the axis and the heavier $^{238}UF_6$ having a slightly higher concentration in the outer regions. By withdrawing uranium hexafluoride from near the axis and repeating the process through a series of centrifuges the uranium hexafluoride can be enriched to reactor grade. The centrifuge method requires about one tenth of the energy required in the diffusion method that was common up to the 1970s. Urenco have been building a national enrichment facility in New Mexico to supply the US market using state of the art centrifuge technology with first production expected towards the end of 2009 (Urenco, 2009). After enrichment, uranium hexafluoride is converted to uranium dioxide (UO_2) pellets for use as fuel in nuclear power reactors. Further details can be found in Bennet and Thomson (1989).

Enrichment of the U-235 isotope to between 3% and 20% is referred to as low-enriched uranium. Greater than 20% is high-enriched uranium with more than 90% considered weapons grade. Commercial enrichment technology and expertise could be fairly easily adapted to produce weapons grade uranium for use in a nuclear weapons program. Much effort is therefore devoted to restricting this highly sensitive dual use technology as a critical step in preventing the proliferation of nuclear weapons.

The usually unwanted U-235 deficient tails, known as depleted uranium, does have uses in other areas due to its chemical properties and high specific gravity of 18.7. It is found in counterweights (including keels of yachts) and in highly penetrating anti-tank ammunition.

NUCLEAR POWER PLANTS AND SPENT FUEL MANAGEMENT

Nuclear power plants

The World Nuclear Association (2009, August) reported that there are 436 operating nuclear power plants worldwide generating 372 GW of electricity. The two most common reactor types are the Pressurised Water Reactor (PWR) and the Boiling Water Reactor (BWR) with 260 and 92 plants respectively (Hore-Lacy, 2003). A succinct and up to date overview of current and proposed nuclear reactor types can be found in Norman, Worrall and Hesketh (2007).

At the heart of nuclear power is the induced fission process that occurs in the reactor core. When U-235 absorbs a thermal (slow) neutron, the compound U-236 nucleus created quickly splits into two daughter nuclei and two or three neutrons. One example of a neutron induced U-235 fission reaction is given below.

$$ {}^{1}_{0}n + {}^{235}_{92}U \rightarrow {}^{236}_{92}U \rightarrow {}^{141}_{56}Ba + {}^{92}_{36}Kr + 3{}^{1}_{0}n + Energy $$

There are two important aspects to the nuclear fission reaction. Firstly the energy produced from U-235 fission is enormous and over a million times more than that produced by burning the same mass of coal. The daily requirements for a 1000MW power plant is about 3 kilograms of U-235 compared with about 8 million kilograms of coal (Thornton and Rex, 2006). Secondly, the fission produces neutrons that, when slowed down (moderated), may be absorbed by other U-235 nuclei to produce a self-sustaining nuclear chain reaction. Details of how the nuclear reaction is controlled, neutrons moderated, and heat energy transferred away to electrical generators can be found in most university level physics textbooks including those by Thornton and Rex (2006), Serway and Jewett (2008), and Halliday, Resnick and Walker (2008).

In addition to power reactors, there are over 250 research reactors in the world where the two primary functions are to produce high flux neutron beams for material science research and (through irradiation) manufacture radiopharmaceuticals for nuclear medicine. Some of these reactors use high-enriched uranium of up to 95% U-235, which unfortunately is also suitable for nuclear weapons. The new Australian research reactor, OPEL, uses low-enriched uranium (just) of 20%, which improves security and nuclear safeguards (ANSTO, 2005). Research reactors typically require higher enrichment than reactors optimised for commercial power generation. In addition, there are breeder reactors (Thornton and Rex, 2006) where fast neutrons from U-235 fission are absorbed by U-238, which then beta decays to produce (breed) Plutonium (Pu-239) that is also fissile. Inherent problems with breeder reactors make them relatively uncommon.

Spent fuel management: storage and reprocessing

After 1-2 years, the used (or spent) nuclear fuel elements need to be removed from the reactor. Typically this used fuel is about 95% U-238, 1% Pu-239 (from transmutation of U-238 when a fast neutron is absorbed), 1% U-235, and 3% fission waste products (World Nuclear Association, n.d.). These waste products are highly radioactive and would be most dangerous if they were acquired by terrorists. Interim storage on site in large cooling ponds is required for several years to provide radiation protection, remove heat from further fission events, and (with the decay of short life radioactive isotopes) make the material easier to handle later.

The spent fuel is either moved for reprocessing (after a few years of interim storage) or is left as waste until final waste storage facilities are ready. Although technologies for storing waste more permanently are being developed, the current thinking is to place suitably sealed waste in deep and stable geological repositories. Former Australian Prime Minister Bob Hawke has recently called on Australia to consider developing a nuclear waste industry that could be a source of income and contribute to energy security worldwide given geologically safe and remote storage options (The Australian, 2009).

Reprocessing begins with the dissolving of spent fuel rods in acid to separate uranium and plutonium from the 3% waste products from the fission (World Nuclear Association, n.d.). These waste products are highly radioactive and require long term storage in drums. The uranium recovered can be recycled by going through the conversion and enrichment process again. It can also be used with the plutonium, which like uranium also produces energy through

neutron induced fission, to produce mixed oxide (MOX) fuel rods. One of many safeguards in a reprocessing plant is to avoid storing separated plutonium by mixing in a 50/50 ratio with uranium (Pickett, 2008)

SAFETY, NON-PROLIFERATION AND NUCLEAR TERRORISM

Nuclear weapons: U-235 or Pu-239?

Plutonium has clear advantages over uranium for the construction and delivery of nuclear weapons. Firstly, Pu-239 can undergo induced fission more easily than U-235 as it captures both slow and fast neutrons. Secondly, the Pu-239 fission reaction also produces on average 2.7 neutrons per fission compare with 2.3 neutrons for U-235. A runaway chain reaction is therefore easier to create for Pu-239 which allows for the development of smaller nuclear warheads that can be more easily delivered by ballistic missiles where size and shape are critical. Pu-239 is an alpha emitter with a half life of 24 thousand years and is highly toxic.

Pakistan and the Khan network

The case of Pakistan and the Kahn network is illustrative of how easily technology and expertise can proliferate across international borders (Nuclear Engineering International Magazine, 2004). Back in the 1970's, Pakistan began acquiring enrichment technology including the design details for advanced Zippe-type centrifuges (after German Scientist Gernot Zippe) from a European enrichment facility operated by Urenco. Pakistan was able to develop its own enrichment capability and successfully tested a nuclear fission bomb in 1998. It is believed that this technology, through the Abdul Khan network, was sold on the black market to Libya, North Korea and Iran. Although Libya has since renounced its nuclear program, North Korea announced its first successful nuclear fission bomb test on October 9, 2006, and Iran, despite UN sanctions (UN Security Council, 2008), is expanding its uranium enrichment capabilities. Other Middle Eastern countries are also investigating the nuclear option.

Regulation and safeguards

The International Atomic Energy Agency (IAEA) was established in 1957 as an independent organisation within the United Nations (UN) to promote safe, secure and peaceful nuclear technologies. The three main pillars of nuclear cooperation that underpin its mission are the promotion of safeguards and verification, safety and security, and science and technology. The IAEA has also responded to recent terrorist attacks through its coordination and strengthening of international approaches to promote nuclear security (IAEA, 2007).

Diversion of nuclear material and technology in the nuclear power industry to nuclear weapons programs is and has been a major problem and concern of the international community. The 1968 Non-Proliferation of Nuclear Weapons Treaty (NPT) aimed to restrict nuclear weapons to the five nuclear powers at the time: USA, Soviet Union (now Russia), China, France and the United Kingdom. Since the NPT came into force in 1970, India, Pakistan and North Korea have conducted nuclear weapons tests, Israel is believed to be a nuclear power and Iran is believed to be close to becoming a nuclear power. India, Pakistan and Israel have never been signatories to the NPT. South Africa was a small nuclear power before deciding to voluntarily disarm and Ukraine, Kazakhstan, and Belarus also briefly possessed nuclear weapons (Doyle, 2008). Given that much nuclear technology and expertise is common to the nuclear power industry and nuclear weapons programs, it has always been difficult for the IAEA, as the international body responsible, to inspect and verify solely peaceful intentions or operations. Additional protocols have been introduced to strengthen the non-proliferation safeguards in the NPT, but there was no general agreement to make these compulsory at the last five-yearly NPT review conference (NPT Review Conference, 2005). In September 2009 United States President Barack Obama chaired an historic summit of the security council which adopted resolution 1887 (2009) with 14 heads of state for broad progress on long-stalled efforts to staunch the proliferation of nuclear weapons and ensure reductions in existing weapons stockpiles, as well as control over fissile material (UN Security Council SC/9746, 2009).

In Australia, the Australian Safeguards and Non-Proliferation Office (ASNO) within the Federal Department of Foreign Affairs and Trade (DFAT) is charged with ensuring that nuclear materials and items are used only for authorised purposes and that our international treaty commitments, including the NPT, are met. ASNO also reports to the IAEA and arranges site visits. Australia's nuclear reactor at Lucas heights and three uranium mines with associated storage and transport operations are major responsibilities for ASNO. An Australian nuclear power industry would result in a huge increase in the storage and transport of radioactive materials. Further details of ASNO's role can be obtained in the 2007-2008 Annual Report (ASNO, 2008). Note that health and safety relating to radiation is mostly regulated by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA, 2009).

Proliferation and nuclear terrorism

Access to enrichment technology and expertise is the biggest stumbling block in producing the highly enriched U-235 required for a uranium bomb from uranium ore. Reprocessing technology of spent fuel rods from power reactors is

critical to extracting the Pu-239 required for the more versatile Plutonium bomb. It would seem logical that international and domestic concerns for the proliferation of nuclear weapons may limit the scope of an Australian nuclear power industry. However, a key finding of the second report (Commonwealth of Australia, 2006) is that increased Australian involvement in the fuel cycle would not change the proliferation risks or make Australia's energy grid more vulnerable to terrorist attack. Given international experience the author does not agree with this finding with respect to proliferation risks.

A nuclear power industry would create additional sources of highly radioactive material that would need to be secured at nuclear facilities and in transportation between facilities around the country. This material could be diverted for use in a Radiological Dispersal Device (RDD) to harm and terrorise a population. Natural disasters and accidental human intervention can also result in the dispersal of radioactive material (Swan, 2008). The ability to detect small amounts of radioactivity in a range of situations has become a bigger priority with increasing resources being allocated to tackle the problem. For example, in 2007 the Domestic Nuclear Detection Office (DNDO) of the US Department of Homeland Security (DHS) announced 10 contracts worth US$8.8 million to perform exploratory research in advanced nuclear detection technology (DHS, 2007)

The difficulties of ensuring that access to sensitive information, materials, technology and critical people are appropriately controlled would be a substantial and complex undertaking for security professionals. For example, major infrastructure, like nuclear power plants and enrichment facilities would require high level physical security and effective policies and procedures for materials and personnel. Transportation of sensitive/dangerous materials over large distances is an issue and the monitoring and guarding of highly radioactive waste in remote depositories would also need to be addressed.

AN AUSTRALIAN NUCLEAR POWER INDUSTRY?

The British Prime Minister recently signalled that he would like Britain to play a major role in building an extra 1,000 nuclear power stations around the world (The Independent, 2008). However, the change of federal government (from Coalition to Labour) in late 2007 has reduced the likelihood of Australia building nuclear power stations in the near future, although there is growing pressure within the ALP to more seriously revisit this option in response to climate change. In any case, the Australian uranium mining industry is preparing for rapid expansion and according to two recent comprehensive reports (Gittus, 2006 ; Commonwealth of Australia, 2006) nuclear power is a realistic option for Australia.

The ANSTO report (Gittus, 2006) concludes that nuclear power is demonstrably the safest way of generating electricity and is an excellent source of supplies. It is reported that the fatality rate per unit of electricity is one thousand times as great for coal, oil and gas than it is for nuclear. It is estimated that although the risk of a terrorist attack on an Australian nuclear power station is 50% higher since 9-11, the risk is still very low. This paper seeks to broadly identify critical segments in the nuclear fuel cycle for terrorism and/or proliferation that have the potential to cause great harm. The overall security risks are significant and would need to be mitigated.

Australia's current role in the world nuclear power industry is that of a major miner of uranium ore and exporter of yellowcake. Australia has no conversion or enrichment capability, no fuel fabrication facility, no nuclear power stations and no reprocessing facilities. Our reactor expertise revolves around the scientific use of one small research reactor at Lucas Heights near Sydney. An Australian nuclear power industry would require a huge influx of technology, expertise, and radioactive materials which together would have far reaching and complex security implications. Adapting from international best practice where possible, there would be a need to develop expertise for the Australian context to provide security for whatever segment of the nuclear industry we chose to develop. Finally, nuclear power is one of many highly politicised issues in Australia and that some elements of the community may choose to inflate or deflate public perception of risks to suit their own purposes.

REFERENCES

ABARE (2009a, February). *Energy in Australia 2009*. Retrieved August, 2009 from http://www.abare.gov.au/publications_html/energy/energy_09/energy_09.html

ABARE (2009b, June). *Australian Mineral Statistics 2009: March quarter 2009*. Retrieved August, 2009 from http://www.abareconomics.com/publications_html/ams/ams_09/ams_jun09.pdf

An Inconvenient Truth [Film]. (2006). Paramount Classics, USA

ANSTO. (2005, June). *Open Pool Australian Light-Water Reactor (OPAL)*. Retrieved August, 2008 from http://www.ansto.gov.au/__data/assets/pdf_file/0003/3558/OPAL_brochure.pdf

ASNO (2008). *ASNO Annual Report 2007-2008*. Retrieved August, 2009 from http://www.asno.dfat.gov.au/annual_report_0708/ASNO_2007_08_ar.pdf

ARPANSA (2009). *ARPANSA*. Retrieved August, 2009 from http://www.arpansa.gov.au/

Bennet, D. J., & Thomson, J. R. (1989). *The Elements of Nuclear Power* (3rd ed.). New York: John Wiley & Sons.

Commonwealth of Australia (2006). *Uranium Mining, Processing and Nuclear Energy – Opportunities for Australia?*. Retrieved April, 2007 from http://www.dpmc.gov.au/umpner/reports.cfm

DHS (2007). *DHS Awards $8.8 Million for Exploratory Research on Advance Nuclear Detection Technology*. Retrieved August, 2008 from http://www.dhs.gov/xnews/releases/pr_1174940537634.shtm

Doyle, J. E. (2008). Dismantling Nuclear Weapons Activities: Politics and Technology. In J. E. Doyle (Ed.), *Nuclear Safeguards, security, and non-proliferation.* (pp.283-287). Burlington USA: Butterworth-Heinemann.

Gittus, J. H. (2006). *Introducing Nuclear Power to Australia: An Economic Comparison*. Retrieved June 5, 2006 from http://www.ansto.gov.au/ansto/nuclear_options_paper.pdf

Halliday, D., Resnick, R., & Walker, J. (2008). *Fundamentals of physics extended* (8th ed.). New York: John Wiley & Sons.

Hore-Lacy, I. (2003). *Nuclear Electricity* (7th ed.). Melbourne: Uranium Information Centre. Retrieved August, 2008 at http://www.uic.com.au/ne.htm

IAEA (2007). *Promoting Nuclear Security: What the IAEA is doing*. Retrieved August, 2008 from http://www.iaea.org/Publications/Factsheets/English/nuclsecurity.pdf

IPCC (2007). *Intergovernmental Panel on Climate Change*. Retrieved April, 2007 from http://www.ipcc.ch/

Maplecroft (2009, September). *Australia overtakes USA as top polluter.* Retrieved September, 2009 from http://www.maplecroft.com/news/australia_overtakes_usa_as_top_polluter_09.php

Norman, P., Worrall, A. & Hesketh, K. (2007). A new dawn for nuclear power. *Physics World*, **20** (7) 25-30. Bristol: IOP Publishing.

Nuclear Engineering International Magazine (2004). *Tracking the Technology*. Retrieved April, 2007 from http://www.neimagazine.com/story.asp?sectioncode=76&storyCode=2024442

http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0216/r2/br0216r2.pdf

NPT Review Conference (2005). *2005 NPT Review Conference*. Retrieved April, 2007 from http://www.un.org/events/npt2005/index.html

Pickett, S. E. (2008). Case Study: Safeguards Implementation at the Rokkasho Reprocessing Plant. In J. E. Doyle (Ed.), *Nuclear Safeguards, security, and non-proliferation.* (pp.165-178). Burlington USA: Butterworth-Heinemann.

Serway, R.A., & Jewett, J.W. (2008). *Physics for scientists and engineers with modern physics* (7th ed.). Belmont USA: Brooks/Cole-Thomson Learning.

Swan, G. I. (2008). Nuclear security case study: earthquake in Sichuan Province, China. *Australian Security Magazine*, September/October 2008, pp54-55, Sydney: Yaffa Publishing Group. Retrieved August 2009 from http://www.securitymanagement.com.au/article.php?action=view&article_id=100

The Australian (2009, August 19). *Bob Hawke in new plug for nuclear waste industry.* Retrieved Retrieved August 2009 from http://www.theaustralian.news.com.au/business/story/0,,25950445-36418,00.html

The Independent (2008, June 13). *Brown says world needs 1,000 extra nuclear power stations*. Retrieved August, 2008 from http://www.independent.co.uk/news/uk/home-news/brown-says-world-needs-1000-extra-nuclear-power-stations-846238.html

Thornton, S.T., & Rex, A. (2006). *Modern physics for scientists and engineers.* (3rd ed.). Belmont USA: Brooks/Cole-Thompson Learning.

UN Security Council (2008, March). *Security Council SC/9268*. Retrieved August, 2008 from http://www.un.org/News/Press/docs/2008/sc9268.doc.htm

UN Security Council (2009, September). *Security Council SC/9746*. Retrieved September, 2009 from http://www.un.org/News/Press/docs/2009/sc9746.doc.htm

Urenco. (2009). *LES: What we will do*. Retrieved August, 2009 from http://www.urenco.com/content/150/-What-we-will-do-.aspx

World Nuclear Association (2009, July). *World Uranium Mining*. Retrieved August, 2009 from http://www.world-nuclear.org/info/inf23.html

World Nuclear Association (2009, August). *World Nuclear Power Reactors 2008-2009 and Uranium Requirements*. Retrieved August, 2009 from http://www.world-nuclear.org/info/reactors.htm

World Nuclear Association (n.d.). *How it works*. Retrieved April, 2007 from http://www.world-nuclear.org/how/how.html

COPYRIGHT

Geoff Swan ©2009. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.