

Australia's Oil Refining Industry- Importance, Threats, and Emergency Response

Amanda East
School of Engineering
Security Science
Edith Cowan University

Bill Bailey
SECAU Security Research Centre
Edith Cowan University

Abstract

Australia's Oil Refining Industry- Importance, Threats, and Emergency Response.

Australia is heavily reliant on down-stream, or refined oil products for daily life and industrial purposes. The industry faces a range of threats and risk factors all of which have the capability to inflict significant damage. A major disruption to Australia's oil refining industry would have major consequences not only for the industry but on society and the economy as a whole. By assessing Australia's reliance on oil products, as well as considering the impact of major disruption to oil refining capabilities internationally, this paper seeks to assess the impact that such an event would have on Australian society, public and private industry and the economy. In the Australian context the industry is not adequately prepared to respond to, or recover from major disaster or disruption. There are a range of international strategies and policies which will be assessed in order to further prepare the Australian industry for a range of potential disasters. This paper uses the Kwinana oil refinery in Western Australia as a case study for considering potential threats, consequences and recovery strategies related to a major oil refinery disruption or disaster.

AUSTRALIA'S OIL REFINING INDUSTRY-IMPORTANCE, THREATS AND EMERGENCY RESPONSE

The Australian oil refining industry is very important to the social and industrial stability of the nation. In terms of size and production the Australian refining industry is relatively small. This being said the local oil refining industry is critical in supplying and maintaining national social and industrial activities. The majority of refinery output is used to supply the transport sector, however the agricultural industry, heavy industries, and general household activities are also reliant on locally produced oil products. If an Australian oil refinery were rendered unavailable for an extended period of time it would have significant consequences for the regional, and perhaps even national social and economic stability. Subsequently the industry needs to be prepared for the range of human and natural threats that it faces. Terrorists, insiders, criminals and natural disasters are all sources of threats which have the capacity to severely disrupt any, or all of the Australian oil refining facilities. There are a number of governmental and industrial measures in place to prevent and respond to any possible threats and risks. Thus far the Australian industry has avoided any major disaster, however must remain vigilant in securing against every form of threat.

AUSTRALIA'S OIL REFINING INDUSTRY

The Australian oil refining industry is made of seven privately owned refineries. Located in five states and owned by four major companies, these refineries provide Australia with 796 000 barrels of refined oil product each day (EIA, 2005). Two refineries, Kwinana (WA) and Bulwer (QLD) are owned by BP; Lytton (QLD) and Kurnell (NSW) are owned by Caltex; Shell runs two refineries, Geelong (VIC) and Clyde (NSW), while the Altona refinery in Melbourne (VIC) is owned by Mobil (AIP, 2005, p.5). The Kwinana refinery is the biggest with an output capacity of 138 000 barrel per day (bpd) (EIA, 2005). The Liquid Fuel Emergency Act (LFE Act, 1984) identifies the following as 'refined liquid petroleum products (S3.1)':

Petroleum products make up 46% of Australian refinery output, diesel 29%, and jet fuel 14% (AIP, p.6). Seventy five percent of Australian demand for petroleum products is supplied by local refineries, any disruption within the Australian industry would have significant social, and economic consequences. Only 30% of refinery feedstock is local crude oil (AIP, 2008, p.2), Australian crude oil is unsuitable for conversion into the primary refined product, petrol. Subsequently the majority of crude oil used in Australian refineries is imported from the Asian and the Middle Eastern refineries (AIP, 2008, p.2). As previously stated Australia is heavily reliant on the local oil refining industry, a range of social and industrial services rely on the stability and supply of the Australian oil refining sector.

AUSTRALIAN RELIANCE ON OIL PRODUCTS

Australian society relies heavily on oil products to provide and supply a range of essential social and industrial services. Oil is relied on for transportation, agricultural as well as industrial, and household purposes. The Australian Institute of Petroleum states that petroleum products are responsible for 52% of final energy consumed in Australia (n.d., p.1). Based on this data it can be assumed that the consequence of a major disruption to the refining industry would be significant. Without oil a significant number of vital social requirements, and industries would not be able to function at full capacity, or at all

Transport is the sector of Australian society which is most reliant on petroleum products. The oil refining industry is geared toward petroleum production to supply the nations transport requirements. All forms of transport, passenger cars, trucks, cargo transport- truck and rail, as well as air transport are reliant on petroleum products to fuel them. Of these, passenger cars or personal transport is responsible for the highest level of consumption. In Australia road transport accounts for nearly 80% of liquid petroleum use (Robinson, Fleay & Mayo, n.d., p.1; Taylor, n.d., p.10), two thirds of which can be attributed to passenger vehicles (Taylor, p.10). Considering that there are 13.2 million registered motor vehicles (passenger cars, commercial vehicles and trucks) in Australia (Robinson et al, p.1; ABARE, 2004, p.47) each averaging 15 300 kilometers (Robinson et al, p.1) per year it is understandable that Australia consumes 38 billion litres of fuel annually for road and off road vehicles (Green Car Congress, 2008). These numbers indicate that Australia has a very strong, but probably unrealised, reliance on the oil refining industry. Transport is relied on not only to transport people, but for the transportation of food, goods and services. If the oil refining industry were to suffer a serious disruption the social, and eventually economic consequences would be enormous.

The agricultural industry also has a strong direct, as well as indirect reliance on oil products. In Western Australia livestock and crop farmers, predominantly wheat, are responsible for 80% of petroleum product purchases by broadacre agriculture (Kingswell, p.2). The majority of the fuel and oil purchases are used in establishing and harvesting a range of grain crops (Kingswell, p.2). The dairy industry has a strong, but indirect reliance on oil products for the transportation of dairy products from farms to processing plants. As previously stated transportation is the sector most reliant on oil products, and agriculture relies on the transportation industry to maintain and ensure the success of their operations. Expenditure of grain and sheep dominant agricultural sectors on transport is 55.6 and 35.5 percent respectively (Kingwell, p.3), while expenditure on petroleum products by the grain dominant sector is 37.0 %, and 20.5 % for the sheep dominant sector (Kingwell, p.3). The export earnings for Australian agricultural commodities made up approximately 2.9% of annual GDP (ABS, 2005). Taking into account drought and other conditions the Australian agricultural industry has not been as successful recently as in previous years, even so the sector is very important to Australian society and economy, and would be significantly effected in the event of a major disruption to local oil supply.

The industrial sector, including mining and quarrying, iron and steel and construction accounts for 21% of Australian oil use (IEA, 2000, p.44). Within this sector, the mining industry is major consumer of diesel fuel (IEA, 2000, p.44). About 35 percent of energy needs within the mining sectors are met by electricity followed by fuel oil which accounts for 32 percent. Energy requirements in exploration and site preparation are reliant on transportation and drilling, which both require fuel oil (ITP, p.18). As the world's largest exporter of coal iron

ore, lead, diamonds, rutile, zinc and zirconium, and the second largest exporter of gold and uranium the mining industry contributes a significant amount to Australian's GDP. Since the mid 1980s the mining industry has contributed \$ 43 Billion to the Australian economy, that is 5% of annual GDP (ABS, 2005). Although the sector is not entirely reliant on oil products it could not function effectively without it, resulting in consequences for Australian exports and the economy.

Petroleum fuels (liquefied petroleum gas (LPG) and heating oil) accounted for 4.6% of household energy consumption in 1995. It is possible that this number has been reduced since due to the connection to natural gas, and upgrades in heating and cooling technology (G.Wilkenfeld, 1998, p.5). Of the petroleum fuels used in general household activities approximately 83.7% was used for heating, 13.3% for water heating and 3.0% for cooking (G.Wilkenfeld, 1998, p.9). Household consumption of oil is not particularly significant, however plays an important role in providing the services and luxuries that we have come to expect.

THREAT SOURCES

The oil industry has always faced a wide range of threats from a number of sources. In the current international security environment terrorism is the main security concern, however every industry must remain vigilant in defending against other sources, and types of threats. As Pavel Baev, a senior researcher at the International Peace Research Institute states,

“it was Katrina not Al-Qaeda that devastated the platforms and refineries along the U.S. Gulf coast in August 2005; it was a short circuit not a well-placed bomb that caused the massive blackout in Moscow in May 2005; and it was not a shoot-out but a labor strike that stopped the pipeline construction in Azerbaijan in November 2005 (Baev, 2006, p.33).”

As well as terrorism, the threat from environmental terrorism, insiders, cyber attacks, and natural disasters must be considered in protecting and defending all forms of major infrastructure.

The major threat to the oil and gas infrastructure is from highly motivated terrorists (Bajpai & Gupta, 2004, p.176). In 2006 there were 344 significant attacks against oil and gas targets compared with 265 in 2005 (Oil and Gas Industry-Terrorism Monitor(OGI-TM), 2007). These attacks resulted in significant loss of life and tens of billions of dollars in lost production as well as physical and reputational damage to many companies (OGI-TM, 2007). The oil and gas industry is not a new target for terrorism, however in recent years Al-Qaeda has vowed more strongly to cut the 'economic lifelines' of industrialised societies (Peck & Lord, p.4), the economic lifelines being oil infrastructure. In light of this and the fact that a number of significant terrorist organisations exist in the region surrounding Australia all forms of oil infrastructure, including refineries need to be prepared for and consider the consequences of a possible terrorist attack.

Agricultural, forest, mineral, petroleum and ecosystem sites and water resources have been identified as being particularly vulnerable targets for environmental terrorism (O'Lear, 2003, p.140). Although not the most significant threat to oil refineries activists are capable of causing disruption and disturbance to oil refinery staff and operations. During times of peace, aspects of the environment, including human manipulated landscapes, could be targets of intentional acts of destruction intended to communicate a particular message (O'Lear, 2003, p.140). Environmental terrorists are not of major concern to the Australian oil refining sector. However oil refineries do have the potential to cause significant environmental damage, and petroleum sites are targets for environmental terrorism. The Australian sector must be wary of the threat that environmental terrorists and activists pose.

Insiders, employees of a particular company or organisation, are also a major threat to the security and productivity of their company. The threat they pose may be maliciously motivated, or purely accidental. As has been previously stated terrorism is a major threat to the oil industry. It is possible that in some cases terrorists may be working in collusion with internal disgruntled employees (Bajpai & Gupta, 2007, p.176) to achieve their objective. That being said disgruntled employees can cause serious disruption of their own accord through fraudulent activity, sale of corporate information, or cyber attacks (Stoneburner, Goguer & Feringa, 2002, p.14). However the major threat posed by employees working in oil refineries is accidents. Around the world, plant and refinery employees are injured or killed on the job almost every day, many of the accidents take place as a result of the negligence of other employees, employers, or third parties (Nelson, 2007). In facilities that process hazardous materials, and performs such a vital social function, there must be a significant emphasis placed on preventing malicious or accidental incidents from within.

The increased reliance computers and networks to control and maintain oil refineries and their functions has led to the development of another, major threat source. The Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) provide the critical service of monitoring and controlling the functions and delivery of the essential services of most critical infrastructure. These systems are used within refineries and to control pipelines, however they were developed purely for functional purposes with no security concerns considered, as a result they are vulnerable to cyber threats. These vulnerabilities leave oil companies, and their facilities susceptible to exploitation, attack and theft of proprietary information (Sevounts, 2006, p.79). Oil facilities have always been targets of malicious attack, and now that many of them are reliant on systems that are vulnerable to cyber threats there is an increased priority placed on securing systems, and defending against the cyber threat (Sevounts, 2006, p.79).

Natural disasters are a major cause of damage and disruption to oil refinery operations. Of all the threats listed, the threat from natural sources is potentially the most damaging. Measures can be implemented to reduce the effects of natural disaster, however they can still cause extensive damage and nothing can be done to prevent their occurrence. Australia is susceptible to a range of natural disasters, all of which can create significant damage and disruption.

PREPAREDNESS

The government has developed a range of strategies and initiatives by which to further enhance the security of critical infrastructure. The majority of government strategies are targeted at 'critical infrastructure' as a whole, rather than each individual sector. This being said the security of oil refineries is covered by a range of energy sector legislation, and critical infrastructure initiatives.

The Liquid Fuel Emergency Act is the legislation developed in order control the production and release of fuel in times of a national fuel crisis. Unless there is a national crisis oil companies are responsible for their own activities and security issues. The Act enables the government to control the output and use of oil products in periods of major emergency. The Act states that, "The Minister may... direct a relevant fuel industry corporation:

(a) to maintain at all times after a specified day, at specified places in Australia, specified quantities of reserve supplies of a specified kind of liquid fuel; or

(b) to accumulate, by a specified day, specified quantities of reserve supplies of a specified kind of liquid fuel and to maintain, at all times after that day, such quantities of reserve supplies of liquid fuel of that kind at specified places in Australia (S12:1a, b)."

The legislation can only be considered in extreme situations where rationing across multiple jurisdictions would be necessary for an extended period and be beyond the capability of the industry to manage on its own (AIP, 2008, p.14). Enacted in 1984 the legislation has never been required to be introduced. Although the Act is not directly related to oil refineries it is the only legislation which Australia can introduce in a time of severe disruption to any part of the oil industry.

The Australian government has implemented a number of initiatives and measures to assist in development and enhancement Australia's critical infrastructure security. These measures are relevant to, and aimed at all industries classified as critical infrastructure. The government strategies intend to increase communication between the government and private sectors on matters of security threats and improvements.

The Business Liaison Unit (BLU), a part of the Australian Security Intelligence Organisation (ASIO), was developed in order to provide a forum by which Australian businesses could interface with the Australian intelligence community (ASIO). The BLU aims to ensure that owners and operators of critical infrastructure can access ASIO information on security issues which affects their assets, operations and personnel (ASIO).

The Trusted Information Sharing Network (TISN) is another government program aimed at increasing the security of critical infrastructure through increased communication.

The TISN brings business and government together with the purpose of sharing ideas and expertise to develop solutions to common, as well as complex, security concerns and problems.

The Computer Network Vulnerability Assessment (CNVA) Program is part of the TISN. It is a government grants scheme developed to help secure critical infrastructure. Through the program funding is provided to help owners and operators of critical infrastructure identify the vulnerabilities of their information and communication systems (CNVA, 2008). It also allows for the examination of security implications of IT infrastructure changes, and assesses potential and existing physical and personnel security issues (CNVA, 2008).

The Australian industry has a number of strategies it can implement in times of supply emergency. In times of extreme emergency they can be introduced in combination with government strategies. The mechanisms which the industry uses to adjust supply include purchase and ship product from a refinery in another state which may take several days to arrive, or from Singapore the shortest time frame is about three weeks (AIP, n.d., p.7). In times of long term disruption product can be purchased and shipped from other overseas sources, delivery of which is likely to take several weeks (AIP, p.7). When there is a significant disruption or reduction to supply and production companies may restrain or limit supplies to industrial and local consumers (AIP, p.7).

RECOVERY STRATEGIES

In terms of maintaining supply of refined oil products the only existing options are to import from other national refineries, increase the capacity of existing refineries, or import products from overseas. The best recovery strategy for the Australian oil refining industry is found in the physical layout of the industry. Australian refineries are not located in close proximity, or owned by the same companies, subsequently it is highly unlikely that the entire industry can be affected by a single disaster or disruption. No natural disaster has the capability to disrupt every refinery, unlike in America where over 40% of national refining capacity is found in two states which are vulnerable to severe weather conditions (Parformak, 2007, p.4). The Australian refineries are owned by different companies, with no communication or cyber connection, making it impossible to shut down the entire system via a single cyber attack. Perhaps the only event that has the capability to impact the nation by disrupting oil refinery production is a highly organised and coordinated terrorist group with the ability to infiltrate the physical and personnel security procedures of the Australian refineries.

The production capacity of the Australian refineries is equal, no refinery is far superior in terms of production. If one or two refineries were to be disrupted it is probable that other refineries could supply the effected region for a short period of time without being severely effected themselves. This being the case the most useful and immediately available measures for recovering, or dealing with an oil related emergency are market-driven, voluntary and compulsory demand restraint (IEA, 2000, p.39). In the Australian context the implementation of measures to reduce industrial and general consumption of oil products is the most effective means by which to recover from a major disruption, while still maintaining social and economic stability.

In terms of size and production the Australian oil refining industry is relatively small, however extremely important in supplying the country with oil products. The majority of locally refined oil products are used domestically, meaning that Australian society and industries are reliant on the local oil refining sector. Australian refineries produce a full range of oil products, the majority of which are used to supply the transportation industry, as well as the agricultural and mining sector. Thus far the industry has been free of malicious, or extremely damaging events, however it does face a range of potentially disastrous threats. Terrorists, insiders, cyber criminals, activists and natural disasters are all sources that threaten the security of the oil refining industry. The consequences of a major disruption would be significant. There are a range of governmental strategies in place to develop and enhance the security of Australia's critical infrastructure, and the industry itself has plans by which it intends to continue in spite of a major disruption. Although the Australian industry has not yet faced any serious disasters it must continue to develop measures to secure, and ensure the continuity of the industry in the event of a major disaster, otherwise there will be major consequences to Australian society, industry and economy.

REFERENCES

- Australian Bureau of Agricultural and Resource Economics. (2004). *Energy in Australia*. Retrieved from Australian Government: <http://www.environment.gov.au/soe/2006/publications/drs/pubs/562/set/hs31energy-in-australia-2004.pdf>
- ASIO. (n.d.). *Business Liaison Unit*. Retrieved from Australian Government: <http://blu.asio.gov.au/>
- Australian Bureau of Statistics. (2005). *Year Book Australia 2005: 100 years of change in Australian industry*. Retrieved from <http://www.abs.gov.au/Ausstats/abs@.nsf/Previousproducts/1301.0Feature%20Article212005?opendocument&tabname=Summary&prodno=1301.0&issue=2005&num=&view=>
- Australian Institute of Petroleum. (n.d.). *Supply Security*. Retrieved from <http://www.aip.com.au/pdf/supply.pdf>
- Australian Institute of Petroleum. (2005). *Downstream Petroleum*. Retrieved from http://www.aip.com.au/pdf/Downstream_Petroleum_2005_Report.pdf
- Australian Institute of Petroleum. (2008, April). *Maintaining Supply Reliability in Australia*. Australian Institute of Petroleum. www.aip.com.au/pdf/AIP%20Paper%20-%20Maintaining%20Supply%20Reliability.pdf
- Baev, P. (2006). Re-evaluating the Risks of Terrorist Attacks Against Energy Infrastructure in Eurasia. *China and Eurasia Forum Quarterly* , 4:2, p.33-38.
- Bajpai, S. & Gupta, J. (2007). Securing oil and gas infrastructure. *Journal of Petroleum Science and Engineering* , 55, 174-186.
- Bajpai, S. & Gupta, J. (2004). Site Security for Process Plants. *Journal of Loss Prevention in the Process Industries* , 18:4-6, 301-309.
- CNVA. (2008). *Fact Sheet*. Retrieved from [http://ag.gov.au/agd/WWW/rwpattach.nsf/VAP/\(930C12A9101F61D43493D44C70E84EAA\)~CNVA+Fact+Sheet+June+2008.PDF/\\$file/CNVA+Fact+Sheet+June+2008.PDF](http://ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~CNVA+Fact+Sheet+June+2008.PDF/$file/CNVA+Fact+Sheet+June+2008.PDF)
- Energy Information Administration. (2005). *Output of Refined Petroleum Products: All Countries, Year 2004 for the International Energy Annual 2005*. Retrieved from <http://www.eia.doe.gov/emeu/international/oilproduction.html>

- G Wilkenfeld and Associates. (1998). *Household Energy Use in Australia: End Uses, Greenhouse Gas Emissions and Energy Efficiency Program Coverage*. Retrieved from <http://www.energyrating.gov.au/library/pubs/hhenergy1998.pdf>
- Green Car Congress. (2008). *Jamieson Report Calls for Fastracking Development of Electric Vehicles in Australia*. Retrieved from <http://www.greencarcongress.com/2008/07/jamison-report.html>
- International Energy Agency. (2000). *Oil Supply Security: The Emergency Response Potential of IEA Countries 2000*. Retrieved from International Energy Agency: <http://www.iea.org/dbtw-wpd/textbase/nppdf/free/2000/oilsecu2001.pdf>
- ITP Mining. (n.d.). *Energy and Environmental Profile of the US Mining Industry*. Retrieved from www1.eere.energy.gov/industry/mining/pdfs/overview.pdf
- Kingwell, R. (n.d.). *Oil and Agriculture: Now and in the Future*. Retrieved From: www.aspo-australia.org.au/References/Kingwell-Oil-in-Agriculture-2003.pdf
- Liquid Fuel Emergency Act. (1984). Retrieved from http://www.austlii.edu.au/au/legis/cth/consol_act/lfea1984213/s3.html
- Nelson, S. (2007). *Plant/Refinery Accidents*. Retrieved from Law Office of Scott. A. Nelson: <http://www.oceanlawusa.com/html/plant-refinery.html>
- Oil and Gas Industry- Terrorism Monitor (OGI- TM). (2007). Retrieved from http://www.ogi-tm.com/ogi_latest_threats.php
- O'Lear, S. (2003). Environmental Terrorism: A Critique. *Geopolitics*. 8:3, 127-150
- Parfomak, P. (2007). *CRS Report for Congress: Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*.
- Peck, B. & Lord, A. (n.d.). *The US Strategic Petroleum Reserve: Needed Changes to Counter Today's Threats to Energy Security*. Retrieved from Strategic Studies Institute: <http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil456.pdf>
- Robinson, B., Fleay, B., & Mayo, S. (n.d.). *The Impact of Oil Depletion on Australia*. Retrieved from http://www.aspo-australia.org.au/References/Abstract_Lisbon_Robinson.pdf
- Sevounts, G. (2006). Addressing Cyber Security in the Oil and Gas Industry. *Pipeline and Gas Journal* , 233:3, 79-80.
- Stoneburner, G., Goguer, A., Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- Taylor, M. (2004). *Australia's approach to managing an oil emergency*. Retrieved from International Energy Agency: http://www.iea.org/Textbase/work/2004/cambodia/bj_session4.3-Australian%20paper.pdf

William Bailey and Amanda East, Edith Cowan University © 2008. The author/s assign Edith CowanUniversity 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.