Address removed

28 October 2016

ACTPLA (epdcustomerservices@act.gov.au)
PO BOX 365 MITCHELL ACT 2911

Dear Sir,

PROPOSAL APPLICATION NUMBER 201600038
BLOCK 11, SECTION 21, 36 COURANGA CRESCENT, HUME
(PLASTIC TO LIQUID FUEL FACILITY)

I have a background in cyber security and I wish to ascertain the level of hardware and software system security that will be built in to the proposed fuel refinery[1] at Hume.

This is relevant because:

- the company proposes to store a large volume of flammable and explosive material on site (larger than anything else in the ACT);
- the production process uses extremes of temperature where sabotage might readily cause fire or explosion; and
- the site is extremely close to regionally- and nationally-important businesses in Hume, a major Federal government data centre and thousands of residents in Gilmore, Chisholm, Macarthur and Tralee.

In sum, a cyber attack upon the proposed facility poses a significant risk to the health and safety of thousands of lives and serious damage to the environment. The facility in-and-of itself will be an attractive target for a politically motivated cyber attack seeking to embarrass the Australian government or disrupt its seat of power. The prospect of causing an event larger and more disruptive than the fire at Mitchell a few years ago may also be attractive to terrorists simply because of its scale.

The consequences of a cyber attack on the facility seem to have been ignored in the draft EIS. This is particularly worrying because the Yokogawa STARDOM FCN controller the company proposes to use was revealed to be vulnerable to remote exploitation by attackers with "low skill" in September 2016.[2]

[1] According to Foy, the facility will turn plastic into "gas and liquids resembling crude oil" which is then boiled to produce fuels. It is, for all intents and purposes, a fuel refinery.
[2] https://www.auscert.org.au/render.html?it=38662

For the purposes of this letter, I will term all the hardware and software used to control the plant and its operation as the 'industrial control system' (ICS). This definition is broad to encompass the Process Logic Control System (PLCS) mentioned in the EIS and any other software or hardware used to control any aspect of the plant's operation. Also, for the purposes of this letter, a cyber attack is anything that may cause unauthorized changes to commands, codes, safety systems or alarm thresholds which could cause inaccurate information to be sent to operators or damage to the facility that causes environmental impacts and/or harm to life and limb. Neither definition is intended to be prescriptive nor is this an exhaustive analysis of the issue.

ACTPLA should consider this issue critically and carefully. A rudimentary internet search puts this problem in perspective: oil companies like BP in America experience up to 50,000 cyber attacks per day[3] and Shell in the UK have already warned that a cyber attack on oil facilities could "cost lives".[4]

In the light of this information, ACTPLA would be criminally negligent if the Authority did not exercise due diligence in assuring the ACT government that the proponents are capable of safely managing a facility of this scale in the event of a cyber attack. If ACTPLA does not have the expertise in-house to make such a determination it should be sourced from elsewhere (possibly the ACT Commissioner for Sustainability and the Environment) before advice is provided to Ministers. The EIS relies heavily on the company's experience in Berkeley Vale to attest to their experience, however, the Berkeley Vale facility is a fraction the size of the one proposed for Hume and is not permitted by the NSW government to process plastic – it is effectively a different facility.

Will the ICS be connected to the internet?

The EIS indicates the continuous emission monitoring system will be linked to a PLCS for the purposes of taking action to control out-of-tolerance emissions. Will the output of the emission monitoring system and PLCS be available to any third-parties for independent verification of the results? (If not, what assurances do the public have that the emissions from the site are within the claimed level and that the PLCS system actually works as claimed?)

Will hardware and software used in the facility will be accredited by any external agency and to what standard? What companies are producing the ICS hardware and software? What company is fulfilling the systems integrator role? (That is – critically - ensuring proprietary software from different companies work safely together?)

Regardless of whether or not the ICS will be connected to the internet, how often will the software be updated and what is the mechanism for doing so?

[3] http://www.cnbc.com/id/100529483
[4] http://www.bbc.com/news/technology-16137573

What level of assurance do the manufacturer(s) of the software offer? What assurances of safety and security does the systems integrator offer?

To what international standard for safety-criticality were the software components individually developed? To what international standard for safety-criticality is the integrated system to be built? Are the various elements of the ICS used in any other comparable plastic-to-fuel facilities elsewhere in the world? What is its individual and collective safety record? How many days production have been lost to faulty software / hardware in the ICS? Why is the NSW government insisting the system be accredited in another jurisdiction before approving an extension of the Berkeley Vale facility? Is it because of concerns about safety? If not, what is the NSW government's concern?

Are the companies providing the software accredited to ISO9001 or similar? How frequently will the software be patched and updated and what is the mechanism for doing so? Will trusted employees of the original developer be used to update / patch the software or will local Foy employees be used? What educating and training do those personnel receive and how many 'trained' operators will be on site 24/7? After updating or patching the software, what standard testing process will be used and how long will the plant be off-line while testing occurs? Is the software able to be tested in a "safe mode" or can testing only be carried out during production? Will vehicle movements in and out of the facility be stopped while testing occurs? What system or systems does Foy employ at Berkeley Vale to safely upgrade ICS hardware and software?

Of the staff operating the ICS 24/7 at Hume, what level of ICT security training will be mandated? Will staff be appropriately educated to recognise and respond to cyber attack? Within Foy, what expertise exists to ensure that the suppliers and integrators of the hardware and software are able to meet their safety obligations? Who is the Foy Chief Technology Officer? Who is the company Chief Security Officer? What sort of professional insurance do these board members hold and will it cover the cost of cleaning up after an incident? Will the company put a cyber security team in place to ensure the hardware and software suppliers are acting appropriately? What level of understanding exists within the company with regard to designing and managing a secure network or does the company simply trust manufacturers such as Yokogawa? Will Foy operate a hardware and software configuration management system for the facility? How many staff will be employed in ensuring the configuration management and testing of the hardware and software used in the ICS? Will these staff have other jobs (i.e. will their safety and security responsibilities be secondary)?

Are the safety systems proposed to be used on site separate from the ICS? If so, are they connected to the internet? Regardless of the answer, what is the plan to update, patch and test those systems?

Will any element of the ICS be wireless-based and if so, what additional security will be introduced in order to protect against intruders in relatively close proximity (eg. someone attempting to use a cyber attack to gain entry to the premises for the purposes of physically destroying the facility)?

Will the control and operation of the plant be centralised or decentralised? In the event of sabotage or deliberate act, or even a fire in the main control room, can the facility be safely shut down from one or more alternate sites? Will these alternate sites be at 36 Couranga Crescent or at another, geographically remote site such as Berkeley Vale in order to give some redundancy to the ICS?

Are there any single points of failure in the ICS? Has this design been validated by an impartial third party to verify the answer?

What levels of physical access security is proposed in order to restrict access to all ICS devices?

In conclusion, the extremely serious impacts of a cyber attack on a facility of the type proposed for Hume, which is in such close proximity to businesses and residences, should be cause for careful and detailed consideration. The proponents are a mining company, where the prospect and consequences of a cyber attack are probably remote and minimal. Their facility at Berkeley Vale is not the same as proposed for Hume and also operating at a fraction of the scale proposed for Hume. Their expertise in this complicated and quickly changing area should not be taken for granted and should be carefully scrutinised to ensure the people of the ACT are not exposed to the potentially calamitous effects of an all-too-real modern phenomena.

Finally, in all likelihood, very few members of the public who attended the single community consultation meeting at Rose Cottage understand these issues, nor should they be expected to. It is, however, incumbent upon those advising the ACT government to assure the ACT public that this issue has been fully and carefully explored and the proponents required to demonstrate they are capable of operating this plant safely.

For additional information, additional submissions or a copy of this letter, please see: http://www.canberrapowerstation.info/

Please acknowledge receipt of this submission to the address above.

Yours faithfully,

Original signed
Name removed

Copies to:

The ACT Commissioner for Sustainability and the Environment
(Attn: Dr Kate Auty)
GPO Box 158 CANBERRA ACT 2601 (envcomm@act.gov.au)

ACT Government Capital Woodland and Wetlands Conservation Trust
Unit 8, 41-15 Tennant Street Fyshwick ACT 2609