Professor Z Y Dong
Head of School
School of Electrical and Information Engineering

Tuesday, January 28, 2014

Australian Energy Market Commission
PO Box A2449
Sydney South NMSW 1235

Dear AEMC Commissioner

AEMC 2013, Framework for Open Access and Common Communication Standards Review, 19 December 2013, Sydney

Reference: EMO0028

I would like to provide some response to the draft report of AEMC framework for open access and common communication standards review.

School of Electrical and Information Engineering of the University of Sydney has strong research and industrial involvement in smart grid technologies, most recently through the Smart Grid, Smart City demonstration project. The Ausgrid Centre of Excellent in Intelligent Electricity Networks/Centre for Future Energy Networks, and Centre of Excellence in Telecommunications form the key research team with world leading researchers in communications and smart grid technologies.

I am pleased to see this report as an important milestone towards more efficient market outcome through the utilization of smart meters.

The response I would like to give is mainly on the choice for interoperability and smart meter infrastructure security. The specific comments are given below:

Section 4.2.2 Introduction to interoperability
Under the interoperability spectrum, interchangeable is defined as where one meter could be swapped for another without any protocol impacts for all accredited parties seeking access to the meter. It looks like more consideration should be given for ‘interchangeable’ because the existence of application layers does not necessarily mean the device can be swapped as described in the report.

Section 4.3.4 Point-of-entry and level of access
The report states “ the security of the smart meter infrastructure is managed at the point of entry. If the point of entry is at the meter then security must be managed with a system of passwords. If the point of entry is remote from the meter then security will be managed by the SMP.”

and
"In addition to restricting access to the smart meter's functionality at the point of entry, accredited parties may also incur charges for using the meter's functions from the point of entry."
I would like to comment that security of the smart meter infrastructure is complex than just password control – although password control is among the most cost effective security measures. Security of the system involves a whole range of activities and factors, it will be difficult to maintain high level of security just to relay on password. Given that the smart meter infrastructure will be part of the overall smart grid/critical infrastructure, a much comprehensive approach in ensuring its security should be considered. Just list a few, intrusion detection, denial of services, application white listing and even physical break into the meter itself may potentially affect the security of the infrastructure.

In our recent work with the Defence Department on smart grid cyber security, consideration of the ICT system including the smart meters, the physical power system and the interactions between the ICT system and the power system all play important roles in ensuring security.

I would like to and am willing to explore this smart meter infrastructure security issue in greater detail and provide more feasible and economically efficient options.

Section 5.3.4 Areas for comment
The report asked

- "should an internationally accepted meter protocol form the foundation of the NEM common market protocol?"

I would like to recommend NOT to use an internationally accepted meter protocol form the foundation of the NEM common market protocol.

Firstly, the protocols for the meter and for the common market are different. Meter protocols are mainly for device communications, not specifically for market. I would like to recommend that AEMO develop its own NEM common market protocol which suits the specific needs of the Australian NEM. There are many organisations/research institutions capable of assisting AEMO to define such common market protocols, including our team in Sydney.

- "is DLMS/COSEM sufficiently well developed to be used as the foundation for a market protocol, given the potentially synergies that exist with smart grid interoperability and other meter standards?"

Yes

- "would the costs of developing an Australian specific services based common market protocol be likely to deliver sufficient benefits compared to using an internationally accepted metering protocol?"

Yes

Auistralian specific common market protocol is needed for the Austarlian market, whereas the internationally accepted metering protocol is not specific for the 'market' but rather for the meters. The NEM has been running with great security and operational efficiency since its establishment, as one of the model markets world-wide. With smart metering infrastructure introduced to the NEM, it is essential to have own protocol for the MARKET to maintain the service quality of the NEM.

A business case can be easily formed in support for the development of an Australian specific services based common market protocol.

- "would extensions to the B2B gateway present a viable option for the development of a services based common market protocol?"

This is possible, but may not be of high priority compared with other works.

Section 6.4 Consumer protection requirements
"Our focus for the remainder of this review is considering whether any of our recommendations under this review will pose new risks to consumers and what these risks may be"

One of the risks is the cyber security issue. With the amount of data involved, introduction of smart meter infrastructure, the risks of cyber related security issue will for sure continue to increase. For example, the intrusion of possible attacks on the cyber network, which may then affect the physical power network (which may cause blackouts), then affect the NEM market (which for example may cause manipulated price spikes). People having access (e.g. legitimate passwords) to the infrastructure may easily login and perform such undesirable actions to cause security or market problems. Concerns also exist for the privacy issues relating to customer data. It is recommended that a comprehensive study on cyber security issues with this new framework for open access and common communication standards are needed.

The above are some of the comments I would like to make for this draft report. I am happy to participate in the development of the framework.

Thank you for your attention to this.

Yours sincerely

Professor Joe Dong
Head of School of Electrical and Information Engineering
The University of Sydney