Security perspectives in Renewables and Waste Management

By Dr Maher Magrabi
February 1, 2021

KEYWORDS: #renewables, waste management, security, risk management, risk assessment, cyber security

Sustainability and Environmental Protection underlie massive shifts in the energy industry and waste management. This article explores these sectors and sheds light on security considerations that need to be taken into account during development projects. It also provides a summary of security and risk considerations for planners and project managers involved in renewable energy and waste management projects.

Renewables

The future of the energy industry is being driven by global trends in sustainability, environmental protection, climate change policy, energy geopolitics and international security. Renewable energies are emerging as the preferred form of energy production and are rapidly becoming critical parts of national infrastructure. Renewable energy facilities include hydroelectric plants, solar farms, wind farms, and biorefineries, as shown in Figure 1.

Renewables can be further segmented into renewable power facilities that become part of the power grid and renewable fuel production facilities that are involved in the production of fuels such as biodiesel, ethanol, hydrogen etc. These facilities are located primarily in regional areas, and in some instances provide alternative revenue sources for farmers and landowners.

Given the remote location and criticality of these facilities as part of the national energy infrastructure, a risk management approach to security is a key consideration in their design and operation. Such an approach seeks to understand the risk exposure of these facilities and to develop effective mitigation strategies to deliver robust security outcomes.

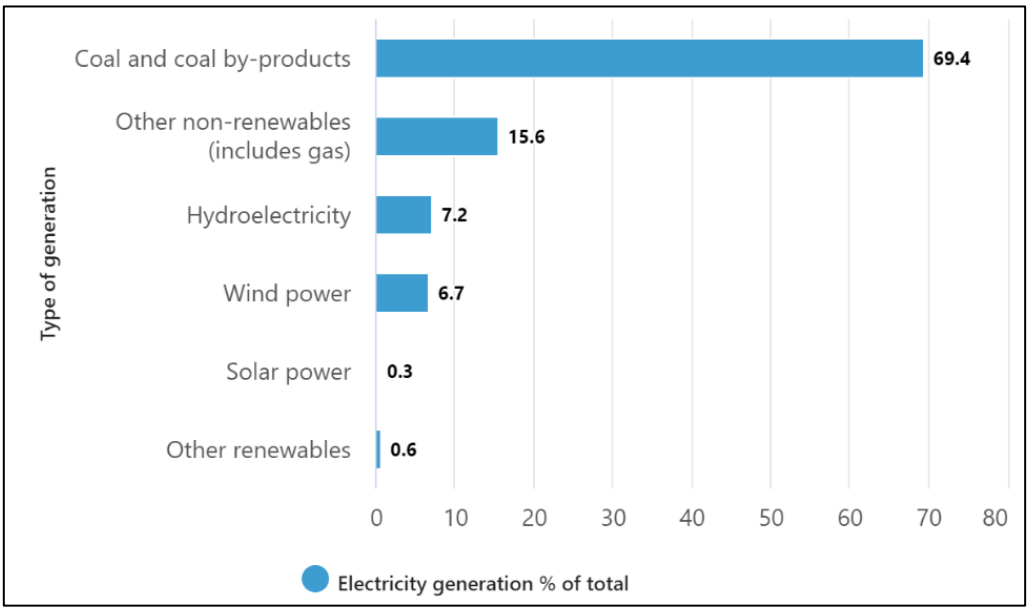

Figure 1. Renewable Energy Generation Sources.

The introduction of renewable energy generation into the power grid creates challenges such as variable generation and bi-directional power flow which are being met through deployment of advanced distribution and control system technologies. These technologies are heavily reliant on information – an example of which is depicted in Figure 2, representative of a residential or commercial building.

The resulting increase in interconnectedness at all levels and the necessary exposure of control systems to other networks creates insecure connections with known vulnerabilities (Stamp 2012). The emergence of these risks necessitates the design of cyber and physical security controls as an integral part of any renewable energy project.

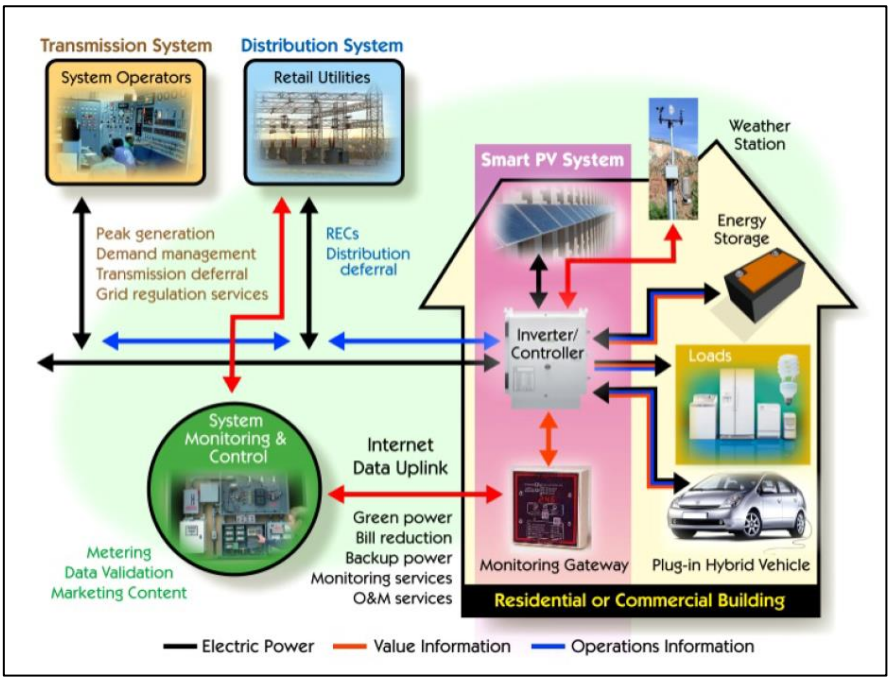

Figure 2. Introduction of Renewable Generation Technologies to the Power Grid.

Waste Management

Waste Management involves the process of collection, sorting, recycling and disposal of waste and is driven by sustainability and environmental protection. According to the latest available data, Australia generates 76 million tonnes of waste with approximately $17 billion spent on waste services per annum (ABS, 2020b). Waste Management entails landfill, recycling, energy recovery and exports as shown in Figure 3.

Being a policy priority of the Australian Government, Waste Management Facilities are critical elements of sustainable development. With an increasing number of facilities along different parts of the waste stream, security and safety are vital considerations for these projects. Whether these are waste disposal sites, recycling drop-off and processing facilities, transfer stations, resource or material recovery facilities, landfills – or the transport infrastructure they all utilise – a sound, risk-based security strategy developed from the planning stages can be realised through the design and construction stage, producing stable operational security outcomes through the life of the project.

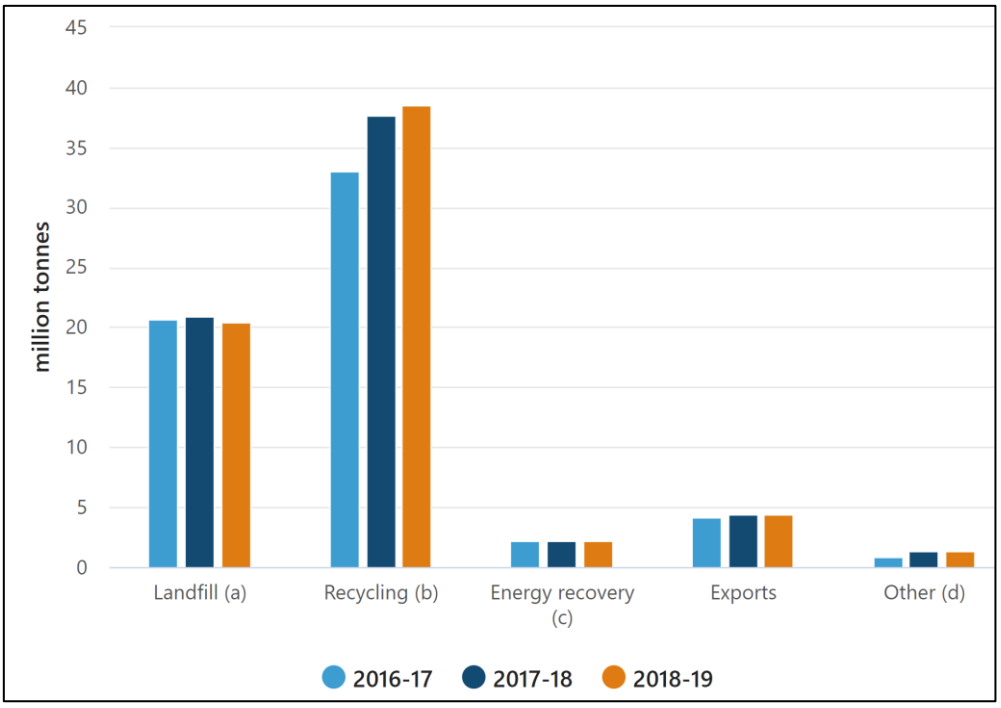

Figure 3. Waste Management - Industry breakdown (Source: Australian Bureau of Statistics, ABS 2020b).

Security Risk Management from Planning through to Operation

Security is a key consideration right from the planning stages of renewable energy and waste management projects. A risk management approach ensures that risks pertinent to the project are identified early and are addressed during the design stage as well as in the operational stage of the project. These risks can include the following:

- Crime risks such as trespass, vandalism, and theft;
- Terrorism related risks such as sabotage and targeted attacks; and
- Cyber risks such as hostile surveillance, sabotage through Cyber Network Attacks (CNA) and Cyber Network Exploitation (CNE).

The cyber risk category is particularly significant given that the threat actors can carry out their attacks remotely and can be state-based actors motivated by national interest, or non-state actors motivated by criminal motives (or political agendas in the case of terrorism).

<u>Planning Stage</u>

Security at the planning stage involves the preparation of a security risk assessment report. The report comprises establishing the context for the project through developing an extensive understanding of the crime risk context, identifying the risks, engaging with project stakeholders, and preparing a risk control plan.

An essential component at the planning stage is a security review of the architectural plans and the application of Crime Prevention Through Environmental Design (CPTED) principles as a part of the risk control plan. A security review during the planning stage ensures that the project requirements factor in security considerations, and that they are incorporated from both a design and operational perspective.

Design Stage

This stage includes the design development of the security requirements identified during the planning stage. Effective security design is a risk management process whose efficacy is measured in terms of risk mitigation outcomes. While this includes traditional security measures such as video surveillance and electronic access control systems, it also extends to the development of effective cybersecurity strategies and organisational security policy. An important consideration at the design stage is to understand the interdependencies inherent in any such project or plant, and to develop a security design that is viable, robust and future-proof.

Operational Stage

Security outcomes are not just about the number of cameras or the physical security of the premises. Security outcomes are achieved when security becomes a cultural value of the organisation and its importance is understood by all the operational stakeholders. Re-framing security in terms of governance, personnel management, information systems and physical security can help develop a total security management plan (TSMP). A TSMP will consider not only the risk mitigation measures that are relevant in terms the security risk assessment process, but also the ongoing budgeting and management of this key element so that the infrastructure's management remains sustainable into the future.

References

ABS (2020a). Energy Use and Electricity Generation, Australia 2016-17, https://www.abs.gov.au/statistics/industry/energy/energy-use-and-electricity-generation-australia/latest-release. Accessed: 26/01/2021.

ABS (2020b). Waste Account, Australia, Experimental Estimates, 2018-19 financial year | Australian Bureau of Statistics (abs.gov.au), https://www.abs.gov.au/statistics/environment/environmental-management/waste-account-australia-experimental-estimates/latest-release. Accessed: 26/01/2021

AEMO (2020). Renewable Integration Study Stage 1 report, April 2020, https://aemo.com.au/-/media/files/major-publications/ris/2020/renewable-integration-study-stage-1.pdf?la=en, Accessed: 26/01/2021.

Stamp, J (2012) Cyber Security for Renewable Energy, Sandia National Laboratories.