

# SECURITY

*These days controls are expected to be in place to prevent someone being injured by doing "something silly". Owners of infrastructure have a duty of care to protect against injury resulting from unauthorised access.*

*By Simon Hensworth, Senior Security Consultant, GHD Perth Operating Centre.*

Australia's power transmission infrastructure is aging. It's not unusual to find sections of current transmission systems that are fifty years old or more. In some areas, and often in country areas, it's not just the infrastructure that is aging but also the facilities that go with it. Facilities like control buildings and switchyard fencing. A lot of these facilities were built when Australia was a very different place. There was a time when getting injured by "doing something silly" was considered to be your own fault. A lot has changed since these days: population, occupier's liability acts, culture, residential expansion and public opinion.

The security measures that were seen as adequate fifty years ago do not often appear appropriate by today's standards. A typical substation perimeter fence of yesteryear would most likely be a chain-link security fence, perhaps topped with one to three strands of barbed wire. Aged fences can often be compromised by lifting, climbing or unwinding them. Many have deteriorated over time and simply rust apart. This type of fencing might stop someone accidentally wandering into a substation but a determined intruder (or curious adventurer) can circumvent this type of fence usually in less than fifteen seconds and even without tools. Aging control buildings are usually located inside the perimeter fence or sit with one wall outside (or flush with) the perimeter fence. It is not unusual for these buildings to be fitted with external doors that are easily compromised. They sometimes have unsecured windows or vents. Some control building design elements assist climbing. Aged transmission infrastructure within switchyards is often constructed of lattice framework topped with live bus bars. These older designs facilitate climbing and may even resemble playground equipment to the uneducated eye or to younger children. Some live infrastructure at older sites is located at relatively low-level, sometimes without protective secondary fences. Warning/ danger signage at older sites can vary too. Some have obscure outdated signage that would not mean anything to people without electrical knowledge. Some infrastructure has no internal signage at all.

## POTENTIAL UNAUTHORISED ACCESS

Investigation of electrical infrastructure sites often results in identification of (potential) evidence of unauthorised access. Evidence of potential unauthorised access can include: jimmy-marks on substation doors and windows, damage to fencing that appears to be from climbing, graffiti on control buildings, toys and articles of clothing left around or remains of campfires inside substation sites. Evidence such as this suggests that either people are fearless of high voltage electricity, they do not understand the potential danger, or do not care.

## FREQUENCY AND IMPACT

Various incidents have occurred over the years throughout Australia involving transmission infrastructure including: theft, vandalism, accidents, injuries, fatalities and even suicides. A growing population, changing culture and residential expansion all contribute to increasing risk of these kinds of incidents. Australia's transmission infrastructure has been in place long enough for data to be collected on the frequency and impact of such incidents. Data on the frequency and impact of these types of incidents provide a good basis for conducting risk analysis to establish risk levels and appropriate levels of controls aimed at managing these risks.

There has been a recent focus in Australia for improving security around transmission infrastructure, in particular transmission substations. Energy Networks Australia has produced a National Guideline for the Prevention of Unauthorised Access to Electricity Infrastructure. The guidelines offer a range of strategies for minimising unauthorised access and managing risk including Physical Security, Electronic Security, Procedural Security, Defense in Depth and CPTED (Crime Prevention Through Environmental Design).

## HIGHER LEVELS OF SECURITY

Security improvements to transmission infrastructure has seen new physical security introduced to substations and electrical infrastructure depots including higher levels of security fencing, window grilles, locks, bollards and gates to prevent unauthorised access.

Electronic security upgrades have included: intruder detection systems, alarm systems, CCTV, access control and public address systems to warn intruders. These security measures can alert monitoring staff and authorities to security breaches and allow alarms to be instantly verified via CCTV.

Procedural security includes: risk management, security awareness, site maintenance, incident reporting and audit procedures.

## DEFENSE IN DEPTH

Defense in Depth is a security strategy that suggests security should not rely on any one security barrier/measure. For example, compromising one barrier (or security measure) should not provide an intruder with access to an entire facility. Rather, Defense in Depth suggests that security measures should be layered in succession, and most critical assets (or dangerous infrastructure) should be located centrally to provide maximum protection.

CPTED is based on embedding safety/security into the built environment. CPTED suggests that opportunities for crime can be reduced by maximising opportunities for Natural Surveillance, Territorial Reinforcement and Natural Access Control.

## SIGNIFICANT FINANCIAL INVESTMENT

With so many security strategies available, potentially totalling to a significant financial investment, it is vital to conduct preliminary risk assessments of sites to establish specific risk and determine what security strategies will most cost-effectively manage risk.

Newer substations have significantly improved designs and security measures than their aging counterparts. Security is always easier and more cost-effective if it can be introduced at the design stage. Improving security around aging, existing electrical infrastructure is challenging but is no less important.

## CONCLUSION

Now that the ENA's new National Guideline for the Prevention of Unauthorised Access to Electricity Infrastructure is in place, and the focus on security is becoming an organised, logically managed process, the future of Australia's power transmission infrastructure is more likely to deliver a service that is safer and more secure to the public at large.