Original Article

Intruder alarm systems: Is the security industry installing and maintaining alarm systems in compliance to Australian Standard AS2201?

David J. Brooks

Security Research Centre (SECAU), Edith Cowan University, 100 Joondalup Drive, Joondalup, WA 6027, Australia.

E-mail: d.brooks@ecu.edu.au

Abstract The study presents an insight into the compliance of installed intruder alarm systems against the relevant Australian Standard. A survey of 451 domestic and commercial intruder alarm systems was completed across the Perth metropolitan area, Western Australia. The gathered data were evaluated against Australian Standard AS2201.1 for the design, installation, commissioning and maintenance of intruder alarm systems to determine whether alarm installations complied with two parts of the standard, being that of control panel location and zone supervision. Security technicians are tested, and if they pass are awarded a licence, in part, against their knowledge and understanding of AS2201.1. The combination of the Western Australian Security Act and Australian Standard AS2201 provide what could be considered the most robust control of the intruder alarm installers sector within Australia. The Australian Standard AS2201.1 required that intruder alarm control equipment shall be located within the alarmed area, located outside the entry/exit point and operate in dual end-of-line supervision. Nevertheless, a significant proportion of the intruder alarms measured did not comply with AS2201.1, with 17.52 per cent of panels located outside an alarmed area, 14.86 per cent panels located in the entry/exit point, 45.90 per cent of the panels not capable of dual end-of-line supervision and 58.75 per cent of the systems configured in single end-of-line supervision. These items contravene sections of the Australian Standard AS2201.1 and would appear to demonstrate systemic failure within this sector of the security industry. Further to these findings, the study made a number of conclusions in an attempt to understand why such a level of non-compliance was found. Conclusions included a lack of industry-focused vocational training and education, limited industry self-regulation and supervision, restricted licensing regime, inappropriate legislation and not having a single federal approach to such matters. In addition, the introduction of a new performance based AS2201 standard may further decrease the ability to measure such non-compliance. However, no single aspect could be considered ineffective; rather, it is argued that all of these areas need to be addressed to significantly reduce the level of systemic non-compliance of intruder alarms systems.

Security Journal (2011) **24**, 101–117. doi:10.1057/sj.2009.12; published online 21 September 2009

Keywords: intruder alarms; legislation; compliance; Australian Standards; training; awareness

Introduction

In all Australian states and territories the State Police Services or their representative, through legislation, provide control of the security industry and their services. Some level of control is achieved through licensing arrangements, based on technical understanding and quality of character (Commercial Agents Unit, 2006). Intruder alarm systems form an integral part of security; however, it could be suggested that consumers have limited awareness of the quality of installation and technical understanding of such systems. Limited understanding may leave the consumer prone to poorly designed, installed, commissioned and maintained intruder alarm systems, resulting in vulnerable security systems.

Vulnerabilities with poorly installed intruder alarm systems may include incorrectly located system components, such as detectors, cabling and battery back-up that cannot meet system electrical demands, and inappropriate maintenance. For example, an incorrectly positioned detector could result in excessive false alarms, with a loss of system confidence and reduced alarm response. A poorly designed battery back-up capacity could result in premature system failure when the primary power is lost, where AS2201.1 specifies a minimum capacity of 16 hours (2007, p. 18). The application of legislation, licensing and standards attempt to reduce such system failures.

Background of the Study

As an industry, *security* has had rapid growth (Hemmens *et al*, 2001). In a recent study, census figures for a 10-year period from 1996 to 2006 showed that while the Australian population increased by 12 per cent and the police workforce by 15 per cent, the number of security providers grew by 41 per cent (Prenzler *et al*, p. 3). Such figures could indicate that the public is now highly dependent on private security services. Nevertheless, current issues suggested the need for more sophisticated regulation to improve conduct and quality of security service (Prenzler, 2005), with one such approach being security licensing.

Installer testing and training

In Australia, security agents or their employees who provide or deliver contract security services are required to be licensed by police authorities. Licensing requirements involve police screening of individuals to ensure that they are 'fit and proper people' to provide security services, that is, have no criminal record or known criminal associations. Licensing may also include examinations of basic technical knowledge, for example, knowledge of relevant Australian Standards and legislation, appropriate qualifications and annual checks of security business records (Tate, 1995, p. 29). Tate (1995) indicated that legislation covering the security industry did not necessarily specify the purpose or type of training.

Within Western Australia, security installer licensing is conducted by Commercial Agents Unit, a branch of the Western Australia Police Service. The branch is staffed by both sworn police officers and public servants, providing licensing to various cohorts of commercial security providers. These security cohorts include security agents, security consultants, security installers and security officers. Security agents hold the primary operators'

licence, security consultants sell security system and services, and security officers provide guarding and patrol services.

Security installers provide *contracted* electrical and electronic security systems for domestic premises and commercial businesses, as well as 24 hours maintenance and repairs. These systems include burglar alarms, closed circuit television systems, access control systems and security lighting. Much of this equipment is computerised and highly sophisticated, with updates and new versions being released on a regular basis. Systems such as do-it-yourself intruder alarms or those installed by an employee of their company are outside the scope of security installers and therefore, this study. Of the 4415 security licences issued in Western Australia in 2008, 346 were installer licences (Table 1).

Within Western Australia, alarm installers have to complete a relevant vocational Australian Qualification level two course, which is not necessarily the requirement in other parts of Australia (see Table 2). Such vocational training provides specific skills and knowledge to the participant within the area of study. For alarm installers this includes such topics as basic electronic circuit theory, cabling requirements, control panel connection and programming, and component operation and connection. Nevertheless, related industries such as electricians, electronic technicians and so on meet the requirements in regard to vocational qualifications.

The Western Australia Balga campus of Technical and Further Education (TAFE) provides a Certificate II course in Electro-technology Servicing (Security Systems). Successful completion of this course provides students with the knowledge and preparation to undertake a security installer's licence examination. With approximately 90 per cent of Western Australia security system installers working in the Perth metropolitan area, Balga TAFE is the only provider of this course in Perth (Department of Education and Training, 2006). In 2000, approximately 70 people commenced the Certificate II in Electronics (Security System Installation). In 2005, 31 students attended the course (D. Fleay, personal communication, 23 November 2005), although 291 new installer licences were issued.

Security installers must complete the intruder alarm examination before being licensed to install or maintain electronic alarm systems that, in part, is based on Australian Standard AS2201.1, Intruder Alarm Systems. Nevertheless, Australian Standards are not mandatory in application; however, AS2201 does provide a descriptive basis for intruder alarm designers, installers and maintainers to operate too. In addition, the installer's examination includes basic electronics skills, circuit calculations and component value calculations, requiring a minimum 80 per cent pass rate (Western Australia Police, 2009a). The intruder alarm licence authorises individuals to install security equipment controlled by the Act, being The

Table 1: Issued Western Australian licences

<i>Licences issued during:</i>	<i>2005</i>	<i>2008</i>
Security agent	177	212
Consultant	226	200
Installer	291	346
Officer	2183	3657
Total	2877	4415

Source: Commercial Agents Unit, West Australian Police, personal communication, 22 July 2009.

Security and Related Activities (Control) Act, 1996. This licence does not apply to installers of security equipment in vehicles, vessels or aircraft (Western Australia Police, 2009b).

Australian Federation

Each state or territory of Australia incorporates their own security licensing and operations legislation for commercial security practitioners. In general, federal security legislation only encompasses national security matters, such as national defence, critical infrastructure and so on. Such an approach leads to each state or territory having their own unique approach to the licensing of intruder alarm installers (Table 2).

Australian Standards

Standards Australia is Australia's peak standards organisation, although they are a public company limited by guarantee. The organisation is charged by the Australian Commonwealth

Table 2: Summary of Australian state and territory intruder detector installers

<i>State or Territory</i>	<i>Exam</i>	<i>Police check</i>	<i>Education level</i>	<i>Relevant Act</i>
Western Australia	Based on AS2201	Yes	Certificate 2	The Security and Related Activities (Control) Act 1996
New South Wales	None	Yes	Required ^a	Security Industry Act 1997 Security Industry Regulation 2007
South Australia	None	Yes	Certificate 2	Security and Investigations Agents Act 1995
Queensland	None	Yes	None ^b	Security Providers Act 2003
Northern Territory	None	Yes	None	None ^c
Tasmania	None	No	None ^d	Security and Investigations Agents Act 2003
Australian Capital Territory	None	Yes	Certificate 3 ^e	Security Industry Act 2003
Victoria	None	Yes	None ^f	Private Security Act 2004

Notes:

^aHowever, requirements are not defined (National Electrical and Communications Association, 2009; New South Wales Police Force, 2009).

^bCurrently security equipment installers do not have any current training requirements. However, there is discussion within the industry to determine whether the electronic security sector needs any training (Department of Employment, Economic Development and Innovation, 2009; Queensland Police Service, 2009).

^cAccording to the National Electrical and Communications Association (2009).

^dAccording to the Consumer Affairs and Fair Trading (2009).

^eAccording to Office of Regulatory Services (2009).

^fAccording to Victoria Police (2009).

Government to provide general oversight and governance of Australian Standards (Standards Australia, n.d.). Their four key areas of focus include national and international coordination, accreditation of other organisations to produce standards, development and update of standards, and design assessment (Standards Australia, 2009).

Australian Standards, as with most standards, are ‘published documents setting out specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform’ (Standards Australia, n.d. p. 2). Such an approach ensures that a common *language* is achieved within an industry, driven by the more progressive parts of industry, legislation and community expectations.

Study Objectives

The objectives of the project were to study the compliance of intruder alarm installations in Perth, Western Australia, against the requirements of Australian Standard AS2201.1. The study determined whether alarm installations are meeting two basic prescribed sections of the standard, being control panel location and zone supervision.

In addition, the study reviewed the training options available to intruder alarm installers in Western Australia, determined the knowledge required to be licensed as an installer in Western Australia and conducted significant on-site intruder alarm system evaluations across the Perth metropolitan area. The evaluation considered two questions regarding compliance with Australian Standard 2201.1:1998, namely *is the security control panel sited within a protected area* and *the type of zone input supervision, being single or dual end-of-line resistance?* These data were evaluated against the Security and Related Activities (Control) Act 1996 and AS2201.1 to determine the measure of compliance.

Research Question

The purpose of the study was to measure the compliance of intruder alarm systems, with the research question being: *What measure of compliance are domestic and commercial intruder alarm systems installations when compared to AS2201.1:1998?* The significance of the study was to measure whether intruder alarm installers had learnt from their training and therefore, understanding of AS2201.1. This understanding required the placement of the intruder alarm system control panel within a protected area and to adequately protect the cables and devices of the system using single or dual end-of-line resistance supervision.

Understanding Security Technology

Learning and understanding the concepts associated with security technology – when applied to the protection of assets – can be considered at a range of levels, according to performance requirements. The cognitive domain can be structured as a hierarchy of understanding of levels of security technology (Smith and Robinson, 1999, p. 28), with security technology being one knowledge domain of many organisational security domains (Brooks, 2010). One of the most universally applied teaching and learning model is the Bloom’s

Taxonomy of Educational Objectives (Anderson, 1995; Green *et al*, 2002), and the study presents examples of how the taxonomy may be applied to security installers. Accordingly, levels of understanding range from simple to complex, and from concrete to abstract.

Bloom's revised taxonomy is based on a six level thinking process. The first three levels apply to training within the security industry and the second three levels apply to security education. A proposed hierarchy of understanding for security technology can be presented as thus:

- *Remembering* is the lowest form of the taxonomy and only requires recall or recognition of specific facts, universal principles or methods. Elementary understanding of concepts only requires recall of fragmented knowledge of security technology without application; for example, the use of passive infrared (PIR) detectors for the office area and dual-technology detectors for the warehouse.
- *Understanding* links new ideas or concepts and requires the learner to explain and summarise cognitive chunks of information. The comprehension level of understanding of security technology allows the individual to describe the context of the detection system; for example, PIR detectors should not be installed facing direct sunlight.
- *Applying* requires making use of what is already known with practical applications in both familiar and unfamiliar situations. An understanding at the application level will allow prediction of outcomes from a set of data or information; for example, calibrating and programming a pan-tilt-zoom camera.
- *Analysing* requires the deconstruction of information, ideas and concepts into parts so as to distinguish between sorts of information and categorisation. Understanding through analysis of an idea is a higher level of cognitive abstraction and requires a detailed comprehension of the function of the concept; for example, the probability of risk at each defensive layer in the protection of an asset.
- *Evaluating* is a skill developed in critical thinking in order to be able to justify a decision or course of action. The ability to integrate two or more major ideas into a coherent and internally consistent principle; for example, the integration of the protection-in-depth principle of asset protection with the crime prevention through environmental design strategy to synthesise a model that has both social awareness and target hardening features.
- *Creating* is encouraged in the development of new products, ideas or novel ways to solve problems. This level of understanding of the principles governing the concepts of security technology requires both qualitative and quantitative judgments (Oz-teachernet, 1995; Smith and Robinson, 1999, p. 29).

Protection of Assets

Protection-in-depth (Garcia, 2001) or *defence-in-depth* (Smith and Robinson, 1999; Smith, 2003) means that to accomplish their goal, an adversary should be required to avoid or defeat a number of protective devices in sequence. Often central to the protection of assets is an intruder alarm system.

An intruder alarm system comprises of a number of discrete components integrated as a system. In general, such components include an alarm control panel with a central processor,

input and output interfaces, power supply and battery back-up. In addition to the control panel, an alarm system will also comprise various types of detectors, including PIR, microwave, door reed switch and so on, and finally, a user interface as a keypad or remote radio frequency identification device (RFID), an external audible warning device, external visible light, and, for a monitored or back-to-base alarm, some form of external communication (Figure 1).

An intruder alarm system may be defined as a component or element of a physical protection system. The ultimate objective of a physical protection system is to prevent the accomplishment of overt or covert malevolent actions. Typical objectives are to prevent sabotage of critical equipment, theft of assets or information and protection of people. The physical protection system must accomplish its objectives by either deterrence or a combination of detection, delay, response (Garcia, 2001, p. 54) and recovery. Intruder alarm systems achieve two components of a physical protection system, as a deterrent and through adversary detection. Deterrence can be achieved through signage advising of the protection of premises by the intruder alarm system and by the prominent display of external warning devices, such as sirens and strobe lights.

Detection is the discovery of an adversary action and includes sensing of covert or overt actions. To discover such action, the following events need to occur:

1. A sensor reacts to a stimulus and initiates an alarm.
2. The information from the sensor is reported and displayed.
3. A person assesses the information, judges the alarm to be valid or invalid and initiates a response.

These events show that detection is not an instantaneous event. Included in the detection function of physical protection is entry control, which allows entry to authorised personnel and detects the attempted entry of unauthorised personnel and material (Garcia, 2001, p. 55). With an intruder alarm system, delay before detection is primarily a deterrent. Once detection has initiated the alarm system, the appropriate response may be to send a guard or advise the clientele. A monitored alarm system can report and display an intrusion within a very short time frame and the response time to intruder alarm systems is dependent on the proximity of the response personnel. The study concentrated on the element of detection being the primary security function of intruder alarm systems.

Figure 1: Typical intruder alarm system.

Notes: User interface = Keypad, RFID or other user interface device; D^1 = Detector that is, PIR, microwave, door reed switch and so on; TP^n = Anti-tamper device that is, micro-switch, magnet reed and so on; Comms = External communication, typically to a remote third person.

The Security Industry

Security training content is decided variously in different Australian states and territories by Department of Consumer Affairs, Police Agencies or TAFE departments. Nevertheless, a common requirement is that licensing courses satisfy legal requirements and are, in some way, accredited. Currently, licence applicants usually need to demonstrate technical competence before a licence is issued. Developing compulsory training, according to accredited industry competency standards, could facilitate standardisation of respective state licensing requirements that, in turn, would enhance the mobility of security occupations. In the absence of an industry training framework and the consequential reliance on enterprise training, the security industry appears to have territorial attitudes to training (Tate, 1995, p. 34), a view supported by Brooks (2010), who stated that the security industry has heterogeneous occupations, which can be applied within the alarm installer domain.

The risk of an enterprise losing its investment in trained security staff to its competitors is real and causes a circumspect approach to training. The development of a security industry training system will increase the pool of industry expertise, reduce the risk of defection of valuable employees, foster a more open approach to training and create a more flexible workforce. Security industry training tends to be in the form of short technical courses to satisfy legislative requirements or to enhance existing technical skills. Such an approach exemplifies a work community sustained by mature age recruits who acquire vocational skills in other occupations and require bridging training for a security occupation. According to Tate (1995) this may partly explain why the industry appears to need a significant emphasis on high level behavioural skills, rather than technical skills.

Intruder alarm installers

The structure and function of intruder alarm intruders may be divided into four discrete groups (Tate, 1995, p. 30), a view supported by Smith and Robinson (1999, p. 30). These four discrete groups include installers, senior installers, technicians and senior technicians.

- *Senior technicians* were mainly employed by companies dealing with electronic equipment and were regarded as highly skilled.
- *Technicians* were most commonly employed in companies dealing with alarms, monitors, security doors and grilles, and fire detection services. They were regarded as being highly or adequately skilled.
- *Senior installers* were mainly employed in small- and medium-sized companies, primarily dealing with alarms and security doors. Two-thirds were considered to be highly skilled, with the remainder adequately skilled.
- *Installers* were primarily employed by companies with less than 20 staff dealing in alarms, locks and security doors, with the largest number employed by companies of five or less staff and many not having TAFE qualifications.

Common practice within the security industry was for those with trade qualifications to advance to the positions of technicians, while those with some form of security industry training advanced to the position of installers. Currently, security systems installers are

drafted either from other industries and cross-trained on the job or trained as apprentices by the major security companies. It is argued that the weakness in this system is that there is no security apprenticeship course that satisfies specified industry standards. Trainees enrol in the apprenticeship course modules approximating those required by the industry, for example, electro technology servicing, electronics and electrics, while developing specific security skills on the job (Tate, 1995, pp. 36–37).

Given the size, scope and importance of the security industry, the availability of training is very limited at all levels. Training is mainly in response to legislative and enterprise requirements, and based on a work force trained in other industries. On-the-job training is provided for unqualified intruder alarm system, with just-in-time technical training supplied by the manufacture on-the-job for new products or technology. Nevertheless, some major security companies offer electronics servicing apprenticeships based on enterprise standards.

The Study

A statistical valid random population survey ($n=451$) was conducted by technicians ($n=8$) from one of the larger West Australian security companies (McLaughlin, 2008). Morrison (cited in Cohen *et al*, 2005, p. 94) indicated that an appropriate random sample size for a population in excess of one million people – the size of West Australia's major metropolitan centre of Perth – should be 384. The technicians surveyed both domestic and commercial intruder alarm systems within Perth. The surveys were randomly attached to a third of the technician's maintenance dockets that directed them to complete both scheduled and reactive maintenance to intruder alarm systems, instigated by the owners of the alarm systems.

The locality of the intruder alarm control panel and the tamper monitoring resistance protection of its detection devices were measured. In combination, these two aspects of security installation determined, to a degree, the ability of installers to design, install and maintain alarm systems in compliance to Australia Standard AS2201.1. Under the principles of defence-in-depth, the control panel of an intruder alarm system should be located within the alarmed area, protected by one of its own detection devices. Upon activation, the detector protecting the control panel should trigger an instant alarm, that is, without delay. This detection method was the basis for the survey questions 1 and 2. Survey question 1 asked – *Is the Control Panel or its Data Gathering Panel (DGP's) directly covered by an alarm detection device i.e., reed switch or PIR?* Survey question 2 asked – *Is the Control Panel or (DGP) located in an entry/exit area?*

Intruder alarm zone supervision

Australian Standard AS2201.1:1998. Section 3.11 stated that for wired detection circuits:

Every wired detection circuit shall be a monitored circuit and shall generate an alarm condition on occurrence of any of the following events:

1. All short circuits and all open circuits.
2. Any series or parallel substitution of the end-of-line component by a component of value equal to that specified by the manufacturer. (p. 15)

Monitoring of a detection circuit through zone supervision is usually accomplished by a set resistance determined by the manufacturer of the control panel for each particular intruder alarm system; nevertheless, common resistance configurations are used (Table 3). The number and configuration of resistors (R) indicates the type of end-of-line, with single end-of-line (Figure 2) being the least secure and dual end-of-line (Figure 3) being the most secure. The dual end-of-line configuration results in making it much more difficult for an intruder to comprise the connection between the detector and control panel.

Single or split end-of-line resistors will satisfy clause 3.11 (a) only if the alarm system is armed. If disarmed, an open circuit or short circuit will show as a normal fault, for example, an open door or movement in front of a sensor. As for clause 3.11 (b), such substitutions are not always detected by single and split end-of-line systems. However, dual end-of-line resistance is designed to detect open circuit, short circuit and resistor substitution whether

Table 3: Common zone supervision configurations

<i>Zone supervision</i>	<i>Resistance configuration</i>
Single end-of-line	One resistor in series or parallel per zone
Split end-of-line	Two resistors, one for each zone, used to zone double a control panel and increase its number of allowable zones from say 4 to 8, 6 to 12 or 8 to 16 by using appropriately sized resistors as specified by the manufacturer
Dual end-of-line	Two resistors in series and parallel per zone

Source: Adjusted from Standards Australia, 1998.

Figure 2: Single end-of-line (Normally open circuit).

Figure 3: Dual end-of-line (Normally open circuit).

the alarm system is armed or not. Hence, not all intruder alarm control panels being used comply with AS 2201.1:1998 clause 3.11, being capable of dual end-of-line monitoring. This section of the Standard provided the basis of the third and fourth survey questions. Survey question 3 asked – *What is the form of zone supervision* and survey question 4 asked – *Is the control panel capable of dual end-of-line resistance?*

The collected survey data were transposed into an Excel sheet, listing the response to each of the four questions within the relevant postcode area. Postcodes in the Perth metropolitan area are designated as either north or south of the centrally located Swan River. Postcodes 60xx are determined north and postcodes 61xx are determined south. These data were evaluated and compared to the appropriate provisions in Australian Standard AS2201.1 and the Security and Related Activities (Control) Act 1996 for compliance.

Analysis

The survey data were analysed with interpretations resulting in a number of significant findings. These included the measure of Australian Standard AS2201.1 compliance in the intruder alarm panel location and zone supervision. In addition, the findings allowed conclusions to be made regarding the current security industry, legislation and system of licensing and training.

Survey question 1 asked if the control panel was directly covered by an alarm detection device. Of the alarm systems surveyed, it was found that 82.48 per cent of the control panels were directly covered by an alarm detection device, with the remaining 17.52 per cent not directly covered. Survey question 2 asked if the control panel was located in an entry/exit area. In 85.14 per cent of the alarm systems surveyed the control panel was located outside the entry/exit area, with the remainder located within this area.

Survey question 3 asked the configuration of zone supervision. It was found that 57.87 per cent of the alarm systems surveyed were operating under single resistor zone supervision, with the remainder connected in dual end-of-line resistance. Survey question 4 asked if the control panel was capable of dual end-of-line resistance. Of the alarm systems surveyed, 62.08 per cent of the control panels were capable of dual end-of-line resistance; however, 37.92 per cent of the control panels did not have this capability.

When analysing the responses to questions 3 and 4 in combination, 21 per cent of the control panels capable of dual end-of-line supervision reverted to single end-of-line resistance. In regard to the responses to the combination of questions 1 and 2, 30 per cent were found to have their control panels located in an entry/exit area and not directly covered by an alarm detection device.

Results and Interpretations

The analysis resulted in a number of significant findings, including the inappropriate locality of the intruder alarm control panels to both AS2201.1 and, according to the defence-in-depth principle, that a significant number of the control panels was not capable of dual end-of-line zone supervision, failing to meet the requirement laid down in the Australian Standard. These findings resulted in a number of conclusions as to why there were such

significant failings in the installation of intruder alarm systems to the explicit requirement of the standard.

Australian Standard AS2201.1, Section 2: installation and location of control equipment, states that alarm control equipment shall be located within the alarmed area. The alarmed area is that part of an area to which detection is afforded by an intruder alarm system (1998, p. 6) and the study found 17.52 per cent of the alarms observed did not comply with this part of the standard. Under the principles of defence-in-depth (Garcia, 2001; Smith, 2003), the control panel should not be located within an access route. Such a locality would allow all personnel passing through that area to view the panel and have some prior knowledge of that particular system. In addition, the entry/exit area allows a pre-set time for legitimate users to access the intruder alarm controlling equipment for arming and disarming. Personnel gaining unauthorised access to this area would be granted the same entry time as authorised personnel, creating a period of vulnerability for the alarm systems operating and controlling mechanism. Of the alarm systems visited, 30 per cent had the main control panel within the access route.

Some brands of control panel surveyed during the study were only capable of using single end-of-line resistors for zone supervision. One hundred and seventy-one of the surveyed systems did not have dual end-of-line capability and a further 94 systems – capable of dual end-of-line – were configured in single end-of-line zone supervision, resulting in a combined total of 58.75 per cent panels having non-compliant zone supervision. AS2201.1 indicates a monitored circuit (supervised circuit) is a circuit arranged to provide an alarm condition in the event of interference to, or failure of, the circuit (1998, p. 7). Thus tamper-detection devices should be included in the intruder alarm system and provide an appropriate warning signal while the alarm system is disarmed, should interference or failure of the circuit occur (1998, pp. 13–14). However, according to Coupe and Kaur (2005, p. 58) less than 1 per cent of burglars disabled business intruder alarms, although in offender interviews over a third of burglars stated that they could neutralise such systems. Therefore, it could be suggested that dual end-of-line is not necessarily required, with single end-of-line suitable for lower risk installations. Such an approach is put forward in the revised edition of AS2201. Nevertheless, greater consideration should perhaps be given to the locality of control panels and their detectors.

During the survey, 31 different control panel models and versions were encountered, with just one installed control panel type being capable of only dual end-of-line zone supervision. Twenty-four control panel models and versions of the control equipment were able to be only connected or programmed with single zone supervision and six control panel models and versions had the ability to be programmed to use either single or dual zone supervision. These figures demonstrate that there is a large amount of security control equipment that has been imported, retailed and installed – with many that may be still available to the Western Australian security installer – that does not fully comply with the Australian Standard AS2201.1 for intruder alarm systems.

In considering the study results, the following conclusions have been drawn:

1. A significant number of current installers either do not comply or understand the applied Australian Standard 2201.1.
2. The security industry licensing regime is, to a degree, ineffective in providing compliant intruder alarm systems.

3. The security industry, through self-regulation, appears to be ineffective in maintaining compliance.
4. Further education, training or awareness needs to be applied to the installer group to raise compliance standards. Such a view supports Tate's (1995) comments on the lack of structured training within the security industry. The intent of such education should be to have alarm installers attaining an *analysis* or *evaluation* level of thinking.
5. The introduction of the revised 2007 edition of the intruder alarm system Australian Standard will reduce the ability to ensure compliance, due to the performance and risk-based approach of the revised standard.
6. There needs to be a single federal approach to security legislation, licensing and monitoring.

This statistically significant study has provided an insight into the non-compliant quality of intruder alarm system installation; however, during the period of the study, a new revised version of the Australian Standard AS2201 was released.

Evaluation with current Australian Standards

The Australian Standard for intruder alarm systems AS2201:1998 was revised and superseded in 2007. Amendments include the standard placement requirements on the location of the control equipment and new requirements on the types of zone supervision to be used for differing classes of intruder alarm installations. These requirements provide a new focus to the research question.

The control panel of an intruder alarm system can be classed as a major asset to the electronic alarm and would benefit from successive barriers of protection, a fundamental principle of the defence-in-depth strategy (Smith, 2003, p. 9). AS2201.1:1998 required that control equipment *shall* be located within the alarmed area and *shall* be in such a position to minimise the risk of interference (p. 8). In support of the previous edition, AS2201.1:2007 requires that control equipment *shall* also be located within the alarmed area and where practical, *shall* not be visible from outside the alarmed area (p. 9). The term *shall* could be considered a mandatory requirement specifying the absolute minimum parameters, whereas the term *should* specifies optional, voluntary and informative parts.

Australian Standard AS201.1:1998 specified the minimum requirements for intruder alarm equipment and installed systems. Zone supervision required that every detection circuit shall be a *monitored circuit* and shall generate an alarm condition on occurrence of all short circuits, all open circuits and any substitution of the end-of-line component (p. 14), namely a dual end-of-line. A monitored circuit (supervised circuit) is a circuit arranged to provide an alarm condition in the event of interference to, or failure of, the circuit (p. 7). Australian Standard AS2201.1:2007 specifies the minimum requirements for the design, installation, commissioning and maintenance of intruder alarm systems. It classifies equipment and system's interconnected by wire, such as detection devices and control equipment that applies to intruder alarm systems in private and commercial premises (p. 5).

Prior to the intruder alarm design and installation a risk assessment *should* be conducted, classified and documented in conjunction with the client (p. 5), a fundamental change between the old and new Australian Standards. Such an approach may improve the placement of the

alarm detectors, as more than a third of alarm systems do not activate, as detectors were either not sited at the point of intruder entry or were contrary to the pattern of intruder movements (Coupe and Kaur, 2005, p. 58). As the data for this study were collected before the release of the new version of the standard, information involving risk assessments was not collected. The classification of risk, through likelihood and consequence, is itself fundamental to the function of security (Brooks, 2010) and is covered by Australia Standards AS4360:2004 Risk Management (Standards Australia, 2004) and HB167:2006 Security Risk Management (Standards Australia, 2006).

The adoption of this form of risk assessment may improve the type of zone supervision being required for the security systems, in particular those classed as being of a higher risk. Whereas security systems of the lower classes are deemed to have minimal consequence of an attack risk profile (Standards Australia, 2007, p. 33). Compliance at this level requires the generation of an alarm condition on all short circuits and open circuits to the monitored wired detection circuit, using at least one end-of-line device (p. 22). This type of fault will only indicate an alarm if the system is armed. Alarm systems assessed as class 3 and above in risk classification, require the use of a three or four state monitored circuits capable of detecting and processing separate alarm conditions for fault or tamper when the system is disarmed, using at least two end-of-line devices (pp. 25–26). Complexity may arise when the client and installer differ on their risk assessments for particular premises.

In addition, the standard requires that on each maintenance visit a report shall be presented to the client confirming that maintenance has been carried out and the status of current compliance. The report may also contain recommendations for alterations that would improve system performance and/or alterations necessary to maintain compliance (Standards Australia, 2007, p. 29). Such an approach can only increase both the clients and installers understanding of the system.

Limitations of Study Outcome

During the data collection period a revised Australian Standard was released for public comment as DR0550 and later, mandated as AS2201.1:2007. It was determined to use the collected data and compare for compatibility, with both versions of the standard. The completed survey questions had not taken into account the new requirements to class security alarm systems through the risk profile of likelihood and consequences of attack and produce a risk assessment (Standards Australia, 2007, p. 5). Without this risk assessment classification for each of the 451 surveyed sites, it was difficult to determine the type of zone supervision required for each surveyed site. In addition, such a fundamental change in the standard, from a prescriptive to a performance approach, will not necessarily improve non-compliance aspects found within this study. Moreover, it is argued that this will only further reduce transparency in performance.

It was determined to use trained security personnel from a single security company to execute the survey questionnaire at each site due to the expertise needed to elicit the requested information. This determination therefore restricted the input of data to installations preformed or maintained by just one security company. The chosen security company was selected for the large volume of alarm installations under its control, including systems

purchased or taken over from other security businesses. This approach may have produced a more diverse sample of the Perth industry, but did not mitigate the fact of control and maintenance by a single entity. Although tests of reliability and viability were considered acceptable, similar studies using different companies may be deemed necessary to further validate a lack of compliance found in this study across the entire industry.

The survey concentrated on the aspects of the alarm control panel and its device protection, being one part of a complete and compliant alarm installation. Further security aspects, such as device location, type and suitability, electromagnetic conformance, audible warning devices, external visible alarms, power supplies, batteries and maintenance requirements were not considered. Australian Standard AS2201.1:2007 now places a mandatory requirement on the alarm installation company to provide inspection visits at regular intervals for demonstration of compliance, which was not considered.

Further Research

Research into the security industry is at an early stage in development. There are numerous opportunities to explore how the industry benefits the community and how much better the industry can adapt to these needs. The questions of compliance with Australian Standard AS2201:2007 could benefit from greater in-depth research. Aspects such as detection device location, type and suitability, maintenance requirements and so on could be components of useful further research into this significant domain of the security industry.

The completed survey questions had not taken into account the recent Australian Standard AS2201:2007 requirements to class intruder alarm systems through the likelihood and consequences of attack to produce a risk assessment. Further research could determine whether this risk assessment classification system was being performed by security companies, whether the classification profiles were appropriate to the particular alarm systems and the amount or quality of the clients input to the assessment process. In addition, similar studies using different companies may be deemed necessary to further demonstrate the lack of compliance across the intruder alarm industry.

Further research may also determine if any perceived non-compliance is owing to lack of knowledge of the appropriate standards or systemic within the security industry. Conclusions were made based on data collected during the study and through the literature review. Nevertheless, the resulting conclusions could be further validated through in-depth interviews with practitioners and regulators to gain their views on the level on non-compliance. In addition, such a study could be completed within the European Union states, United States or any other state that has such a legislative approach to the intruder alarm industry.

Summary

The combination of the Security Act (Security and Related Activities (Control) Act 1996) and Australian Standard for intruder alarm systems (Standards Australia, 1998; Standards Australia, 2007) provides specific regulation for the installation of West Australian intruder alarm systems. Both the Security Act and integration of AS2201 provides what could be considered the most robust control of the security installer sector within Australia.

Nevertheless, the increased importance of security is the need to have an intruder alarm system installed to an appropriate and relevant standard.

The study measured 451 commercial and domestic intruder alarms systems in Perth, Western Australia for compliance against Australian Standard AS2201, resulting in a number of significant findings. The first finding was that a percentage of the inspected intruder alarm systems failed to comply with the AS2201.1 standard in that the control panel was not located within an alarmed area (17.52 per cent) and that the panel was located within an entry/exit location (14.86 per cent). Second, a large proportion of the alarm systems were installed in single end-of-line configuration (58.75 per cent). In addition, a significant number of the intruder alarm control panels that are imported, distributed and installed by the security industry did not have AS2201.1 capability for dual end-of-line supervision (37.92 per cent). These aspects demonstrated a significant level of non-compliance for installed intruder alarm systems that appeared to be systemic throughout the intruder alarm industry.

Conclusions put forward to explain this high level of non-compliance include a lack of industry-focused vocational training, and that the security industry cannot provide an appropriate level of self-regulation and, therefore, supervision. Many installers are trained on-the-job, resulting in incorrect practices and procedures being passed onto new installers. The current licensing regime is, to some degree, ineffective in testing entry requirements and monitoring continual performance, with state legislation lagging behind the industry. However, no single aspect could be considered ineffective; rather, it is argued that all these areas need to be addressed.

With the introduction of the new Australian Standard AS2201:2007, which uses a risk-based approach to define intruder detection requirement, the issues are likely to continue because of greater complexity of the standard and a performance-based approach. However, one benefit with the new standard may be the requirement for installers to provide maintenance reports that detail compliance levels of current systems, although, how this may be accepted by consumers has to be monitored. Nevertheless, the study has shown that there are significant questions to be addressed on intruder alarm system installation compliance and the industry's systemic failure in such a regulated environment.

References

- Anderson, L. (1995) Revised Bloom's taxonomy, <http://rite.ed.qut.edu.au/oz-teachernet/index.php?module,> accessed 1 December 2005.
- Brooks, D.J. (2010) What is security: Definition through knowledge categorisation. *Security Journal* 23(3): 225–239.
- Cohen, L., Manion, L. and Morrison, K. (2005) *Research Methods in Education*, 5th edn. New York: Routledge-Falmer.
- Commercial Agents Unit. (2006) Security installer licensing requirements, <http://www.police.wa.gov.au/services/services.asp?CommercialAgents>, accessed 4 December 2006.
- Consumer Affairs and Fair Trading. (2009) Security agents – Applying for a license, http://www.consumer.tas.gov.au/business_affairs/security_agents/applying_for_licence, accessed 12 June 2009.
- Coupe, T. and Kaur, S. (2005) The role of alarms and CCTV in detecting non-residential burglary. *Security Journal* 18(2): 53–72.
- Department of Education and Training. (2006) TAFEWA: Discover your future, [https://internal.lawley.wa.edu.au/curriculum/TAFE Handbook/MS95.htm](https://internal.lawley.wa.edu.au/curriculum/TAFE%20Handbook/MS95.htm), accessed 10 September 2009.

- Department of Employment, Economic Development and Innovation. (2009) Security equipment installer, <http://www.fairtrading.qld.gov.au/security-equipment-installer.htm>, accessed 5 June 2009.
- Garcia, M.L. (2001) *The Design and Evaluation of Physical Protection Systems*. Burlington, VA: Butterworth-Heinemann.
- Green, G., Edwards, K. and Netolicky, D. (2002) Bloom's taxonomy (CD-Rom). Peppermint Grove, Australia: Presbyterian Ladies College – Cottesloe.
- Hemmens, C., Maahs, J., Scarborough, K.E. and Collins, P.A. (2001) Watching the watchmen: State regulation of private security 1982–1998. *Security Journal* 14(4): 17–28.
- McLaughlin, R.E. (2008) A study of the compliance of alarm installations in Perth, Western Australia: Are security alarm systems being installed to Australian Standards AS2201.1-Clients premises – design, installation, commissioning and maintenance. Unpublished Master dissertation, Edith Cowan University, Perth, Western Australia.
- National Electrical and Communications Association. (2009) Security licensing and training for installers, http://www.neca.asn.au/filelibrary/AUS/Member_Services/Security_Licensing_and_Training_for_Installers.pdf, accessed 14 June 2009.
- New South Wales Police Force. (2009, January) Security license, http://www.police.nsw.gov.au/services/security_industry_registry/security_licence, accessed 3 June 2009.
- Office of Regulatory Services. (2009) Application for a security employee license. Office of Regulatory Services – Business & Industry Licensing, http://www.ors.act.gov.au/BIL/Forms/Industries/packages/GS01_ist.pdf, accessed 2 June 2009.
- Oz-Teachernet. (1995) Revised Bloom's taxonomy, <http://rite.ed.qut.edu.au/oz-teachernet/index.php?> accessed 1 December 2005.
- Prenzler, T. (2005) Mapping the Australian security industry. *Security Journal* 18(4): 51–64.
- Prenzler, T., Earle, K. and Sarre, R. (2009) Private security in Australia: Trends and key characteristics. *Trends and Issues in Crime and Criminal Justice*, no. 374, <http://www.aic.gov.au/en/publications/current%20series/tandi/361-380/tandi374.aspx>, accessed 10 September 2009.
- Queensland Police Service. (2009) Queensland Police Service/Security Industry Liaison Board, <http://www.police.qld.gov.au/programs/crimePrevention/security/>, accessed 6 June 2009.
- Security and Related Activities (Control) Act. (1996) Reprinted 2003. Perth, Australia: Government Printers.
- Smith, C.L. (2003) Understanding concepts in the defense in depth strategy. Paper presented at the Proceedings of the 2003 *International Carnahan Conference on Security Technology*, pp. 8–16.
- Smith, C.L. and Robinson, M. (1999) The understanding of security technology and its applications. Paper presented at the Proceeding of the 1999 *International Carnahan Conference on Security Technology*, pp. 26–37.
- Standards Australia. (1998) *AS/NZS 2201.1:1998 Intruder Alarm Systems – Part 1: Systems Installed in Client's Premises*. Homebush, Australia: Standards Australia.
- Standards Australia. (2004) *AS/NZS 4360: 2004 Risk Management*. Homebush, Australia: Standards Australia.
- Standards Australia. (2006) *HB 167:2006 Security Risk Management*. Homebush, Australia: Standards Australia.
- Standards Australia. (2007) *AS/NZS 2201.1:2007 Intruder Alarm Systems – Client's Premises – Design, Installation, Commissioning and Maintenance*. Homebush, Australia: Standards Australia.
- Standards Australia. (2009) About us, <http://www.standards.org.au/cat.asp?catid=21>, accessed 13 July 2009.
- Standards Australia. (no date) *Imagine a World Without Standards* [Brochure]. Homebush, Australia: Standards Australia.
- Tate, P.W. (1995) *Report on Security Industry Training: Case Study of an Emerging Industry*. Perth, Australia: Western Australian Department of Training. Western Australian Government Publishing.
- Victoria Police. (2009) Our services – private security, http://www.police.vic.gov.au/content.asp?Document_ID=109, accessed 6 June 2009.
- Western Australia Police. (2009a) Application for license, <http://www.police.wa.gov.au/LinkClick.aspx?fileticket=SI2%2bx145fOo%3d&tabid=1093>, accessed 7 June 2009.
- Western Australia Police. (2009b) License categories, <http://www.police.wa.gov.au/OurServices/CommercialAgentsUnit/LicenceCategories/tabid/1275/Default.aspx>, accessed 7 June 2009.