10.4.6.2 Manufacturer's installation instructions shall provide details on signal strength verification for performance testing. Results shall be available through local indicators, *signal receiving centre* readings or through the service provider. Geographic *radio frequency* coverage shall be the responsibility of the installing company.

10.5 PACKET SWITCHED DATA NETWORK COMMUNICATORS

10.5.1 General

10.5.1.1 Packet switched communications is a method of communications characterized by the simultaneous and/or sequential *transmission* and reception of multiple signals over a private or public network. *Control unit* equipment may utilize but not be limited to:

A Corporate networks/intranet;

B Virtual private networks;

C High speed networks;

D Public switched networks; and

E Wireless networks.

10.5.2 Private, Corporate and High Speed Data Networks

10.5.2.1 A product or installation intended for active *communication channel* security shall employ a dedicated connection compliant with Subsection 11.2, Active Communication Channel Security, and the requirements of Clauses 10.5.2.1 through 10.5.2.10.

10.5.2.2 Communicators intended for Security Levels II, III and IV applications (see Table 11, Control Unit Features based on Security Level) shall employ an encryption scheme of a minimum of 128 bits, employ message authentication and comply with the requirements of Subsection 11.2, Active Communication Channel Security.

10.5.2.3 Where a server is employed for control over network addressing, encryption or re-*transmission*, such shall be designed to remain in the "on state" at all times and be in compliance with Clauses 13.1.2 and 13.4.1.

10.5.2.4 Network access and domain access policies shall be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

10.5.2.5 For active *communication channel* security, encryption shall be enabled at all times.

10.5.2.6 Evidence of a certificate of compliance for the validation of encryption algorithms of a minimum of 128 bits shall be provided.

10.5.2.7 Neither the *control unit* nor the *signal receiving centre* receiver shall be susceptible to security breaches in general-purpose operating systems.

10.5.2.8 Each message exchange between the *premises* and supervising station receiver equipment shall include the network address of the *premises* equipment, and a hashed (scrambled) key, which is changed on every message exchange. Alternatively, a system shall be able to accommodate a minimum

of 65 000 distinct account numbers with each having an additional authentication key that is changed each time the system is *armed*, or more frequently. The *codes* shall be part of each message sent between the *premises* and supervising station receiver equipment.

10.5.2.9 Refer to CAN/ULC-S302, Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems, for requirements for a secondary communications path, where 24 h standby cannot be facilitated for all communications interface components as routers, hubs, switches and other network components.

10.5.2.10 Installation manuals for products employing packet switched (network) communications as TCP/IP, UDP or equivalent shall also include recommendations for selecting the internet service providers that have redundant servers/systems, back-up power, routers with firewalls enabled and methods to identify and protect against “Denial of Service” attacks (i.e. via “spoofing”).

10.5.3 Public Switched and Wireless Data Networks

NOTE: Public switched and wireless data networks are network connections as listed in Clause 10.5.1.1 (C through E), employing a non-dedicated public switched network and/or third party internet service provider which sets network security policies.

10.5.3.1 *Communication channels* between a *signal receiving centre* and the protected *premises* shall be facilitated such that the communicator will restrict unauthorized access, which could otherwise *compromise* security.

10.5.3.2 Installation guidelines for *communication channel* security shall be provided with the control and/or communicator module to instruct on compliance to Section 11, Communication Channel Security, based on the security level of the system being configured

10.5.3.3 Power for network equipment such as hubs, switchers, routers, servers, modems, etc., shall be backed up or powered by an uninterruptible power supply (UPS), stand-by battery or the *control unit*, capable of facilitating 24 h standby, compliant with Clauses 13.1.2 and 13.4.1. Where such cannot be facilitated, the *control unit* shall be capable to support back-up communications for a secondary communications path and indicated in the manufacturer’s installation instruction, subject to the following:

A Security Level I and II shall use a dialer as a minimum;

B Security Level III shall use cellular control channel or long range radio as a minimum; and

C Security Level IV shall be equipped with 24 h standby power.

NOTE: Refer to Table 11 for the risk levels.

10.5.3.4 Communicators are not suitable for active *communication channel* security and medium or high risk applications unless such can be “on line” at all times, have a minimum 128 bit encryption scheme, have encryption enabled, network and domain security implemented and are in compliance with Subsection 11.2, Active Communication Channel Security.

10.6 INTERFACE WITH SIGNAL RECEIVING CENTRE AUTOMATION SYSTEM (SRCAS)

10.6.1 When a receiver is connected to a *Signal Receiving Centre Automation System (SRCAS)* signals shall be processed as indicated in the Clauses 10.6.2 through 10.6.4.

10.6.2 The communications between the receiver and the *SRCAS* shall be of an ack/nak type. i.e., handshaking and loss of connection to *SRCAS* shall be indicated at the receiver interface within 90 s.

10.6.3 When in communications with the *SRCAS*, the display and/or any hardcopy output of the receiver may be suppressed.

10.6.4 When the communications between the receiver and the *SRCAS* is lost for a maximum of 90 s, the receiver shall immediately return to a non-suppressed state and output shall start with the last signal not passed on to the *SRCAS* system.

11 COMMUNICATION CHANNEL SECURITY

11.1 GENERAL

11.1.1 *Communication channel* security is defined in following four (4) categories and is relevant to the extent of protection and application for a *control unit*. The actual level of *communication channel* security deployed in protected *premises* will be stipulated by the responsible authority :

A Security Level I: Active Level 1 or Passive Level 1;

B Security Level II: Active Level 2 or Passive Level 2;

C Security Level III: Active Level 3 or Passive Level 3; and

D Security Level IV: Active Level 4 or Active Level 3 plus minimum Passive Level 1

NOTE: Clause 11.1.1 provides direction on stipulating the level of *communication channel* security and extent of protection for the respective risk category.

11.2 ACTIVE COMMUNICATION CHANNEL SECURITY

11.2.1 General

11.2.1.1 Active *communication channel* security is where the status of the *control unit* is transmitted to the signal receiving unit at intervals less than 90 s. Active *communication channel* security may employ any technology carrier that facilitates the requirements of Clauses 11.2.1 through 11.2.6.14.

11.2.1.2 Where two-way *radio frequency* communications systems (two-way *radio frequency* multiplexed systems) are capable of providing a continuously supervised *communication channel*, such systems qualify for active *communication channel* security, providing that such products are in compliance with the respective clauses of Subsection 11.2, Active Communication Channel Security.

11.2.2 Level A1

11.2.2.1 The *communication channel* shall be supervised. Any fault on the *communication channel* that impedes communication shall result in an indication of the fault at the *signal receiving centre* within 180 s.

11.2.3 Level A2

11.2.3.1 The *communication channel* shall be supervised. Any fault in the *communication channel* that impedes communication shall result in an indication of the fault at the *signal receiving centre* within 180 s.

11.2.3.2 In addition to the requirements of Clause 11.2.3.1, *control units* affected by the fault condition shall be identified.

11.2.3.3 A *compromise* attempt of the *communication channel* between the *signal receiving centre* equipment and the protected *premises*, either by substitution of electrical resistance or by substitution of electrical potential, shall be automatically detected within 6 min. (See Subsection 11.2.6, Compromise Test.)

11.2.4 Level A3

11.2.4.1 The *communication channel* shall be supervised. Any fault in the *communication channel* that impedes communication shall result in an indication of the fault at the *signal receiving centre* within 180 s.

11.2.4.2 In addition to the requirements of Clause 11.2.4.1, *control units* affected by the fault condition shall be identified.

11.2.4.3 In addition, a *compromise* attempt of the *communication channel* between the *signal receiving centre* and the protected *premises*, by any or all of the following means, shall be automatically detected within 180 s:

A Substitution of randomly selected equipment. Equipment used to make substitutions is to be identical in all aspects to the original equipment. If 95% of these substitutions results in detection, the equipment is acceptable;

B Reintroduction into the system of information transmitted between the *signal receiving centre* and the protected *premises*. A *recording* device is to be used to collect the information from, and then reintroduce the information into the *communication channel*; or

C Introduction of a synthesized signal into the *communication channel* between the *signal receiving centre* and the protected *premises*. The signal is to be produced by a portable variable frequency signal generator capable of producing sinusoidal, square, and sawtooth waveforms.

(See Subsection 11.2.6, Compromise Test.)

11.2.5 Level A4

11.2.5.1 The *communication channel* shall be supervised. Any fault in the *communication channel* that impedes communication shall result in an indication of the fault at the *signal receiving centre* at all times.

11.2.5.2 In addition to the requirements of Clause 11.2.5.1, *control units* affected by the fault condition shall be identified.

11.2.5.3 In addition, a *compromise* attempt of the communication channel between the *signal receiving centre* and the protected *premises*, by any or all of the following means, shall be automatically detected within 180 s:

A Substitution of selected equipment. Equipment used to make substitutions shall be identical in all aspects to the original equipment including such things as system address, optional features, connected battery, etc;

B Reintroduction into the system of analogue information transmitted between the *signal receiving centre* and the protected *premises*. A *recording* device shall be used to record the transmitted signal and to synchronize the playback of the *recording* with the signal received at the protected *premises*; and

C Reintroduction into the system of digital information that has been transmitted between the *signal receiving centre* and the protected premise. A device that has been programmed accordingly shall be used to store and analyze the digital data that is being transmitted in order to produce a signal generator, which simulates the transmitted signal.

(See Subsection 11.2.6, Compromise Test.)

11.2.6 Compromise Test

11.2.6.1 A *compromise* attempt of any of the *communication channel* security requirements specified in Subsection 11.2, Active Communication Channel Security, shall cause an alarm signal.

11.2.6.2 A signal caused by a *compromise* attempt need not be distinguished from a normal alarm signal for Level A1, Level A2, and Level A3.

11.2.6.3 A signal caused by a *compromise* attempt shall be distinguished from the normal alarm signal for *communication channel* security Level A4

11.2.6.4 If a number of systems depend on one *communication channel*, the system against which a *compromise* attempt is made in accordance with Subsection 11.2, Active Communication Channel Security, shall be identified and the attempt shall not cause signals that appear to originate in one of the other systems on that line or channel.

11.2.6.5 The *compromise* attempts described in Subsection 11.2, Active Communication Channel Security, are to be conducted at the protected *premises* at the end of the *communication channel*, at terminals or at a *point* located outside of the protected *premises*.

11.2.6.6 The *compromise* equipment is to be introduced by a quick-action multiple-pole switch so that the transfer is accomplished in 5 ms or less.

11.2.6.7 Voltmeters, ammeters, ohmmeters, and frequency meters, each with accuracy within 5% or less, are to be used to determine the adjustment of the *compromise* equipment employed in Clauses 11.2.3.3 and 11.2.4.3.

11.2.6.8 The amplitude of the *compromise* signal introduced as described in Clause 11.2.4.3 (B and C) is not to exceed ±10% of the intended signal.

11.2.6.9 The deviation of the frequency used for the *compromise* signal introduced in Clause 11.2.4.3 is not to exceed ±10% of the intended signal frequency.

11.2.6.10 Supervision signals between *premises* alarm equipment and *signal receiving centre* shall be managed by the *signal receiving centre* alarm receiver equipment and not an intermediary network agent, device or server.

Exception: Where such intermediary signal receiving centre and equipment comply with this Standard, such exceptions are acceptable.

11.2.6.11 Remote panel programming or configuration access shall require the use of a valid password, the panel's account or network address, and a hardware or software key to enable a remote programming mode. If an internet connection is used, the data shall be encrypted and an audit trail shall be created in the *control unit* and/or the *signal receiving centre* equipment listing the data change.

11.2.6.12 Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in CAN/CSA-C22.2 No. 950-1, Information Technology Equipment-Safety - Part 1: General Requirements. Where network interfaces, such as the following, are internal to the *control unit* or receiver, compliance to CAN/CSA-C22.2 No. 950-1 is adequate. Such components include, but are not limited to:

A Hubs;

B Routers;

C Network interface devices;

D Third party communications service providers;

E Digital *control unit* line (DSL) modems; and

F Cable modems.

11.2.6.13 For communications equipment employed at the protected *premises* or *signal receiving centre* and intended to facilitate packet switched communications, as defined in this standard, 24 h back-up power is required. Where such cannot be facilitated, the *control unit* will need to support back-up communications for a secondary communications path.

11.2.6.14 Where a third party satellite or *signal processing centre* is an integral part of a switched packet network communicator, the following requirements shall apply:

A Where a third party satellite or *signal processing centre* simply “passes through” switched communications packets, no investigation is required by a recognized testing laboratory for such communications facilities and equipment; and

B Where a third party satellite or *signal processing centre* re-transmits or manipulates switched communications packets, such facilities and equipment shall be investigated by a recognized testing laboratory to ensure compliance with this Standard.

11.3 PASSIVE COMMUNICATION CHANNEL SECURITY

11.3.1 General

12.3.1.1 Passive *communication channel* security services may employ any technology carrier which facilitates the requirements of Clauses 11.3.1.2 through 11.3.4.5.

11.3.1.2 Passive *communication channel* security is where the communication capability between the *control unit* and the *signal receiving centre* is tested (verified, confirmed) at intervals greater than 90 s but in no case exceeding 24 h, changes in the status of the *control unit* are communicated to the *signal receiving centre* within 90 s and failure of one of the *communication channels* is annunciated at the signal receiving centre within 240 s.

11.3.1.3 *Primary communication channels* and *secondary communication channels* may be comprised of the following to meet the requirements of the respective levels of *communication channel* security, as defined in Clauses 11.3.2.1 through 11.3.4.5. These are examples and are not intended to be limited to the technologies shown:

A Public Switched Telephone Line (PSTN);

B Public cellular network;

C Cellular control channel;

D One-way radio;

E Two-way radio; and

F Public Switched Data Network (PSDN).

11.3.1.4 All self-contained equipment shall meet the requirements of this Standard and shall facilitate electrical supervision in compliance with requirements contained within this Standard.

11.3.1.5 Equipment employed to provide *radio frequency communication channel* security shall be in accordance with this Standard and facilitate tamper protection and electrical supervision, and shall meet all other requirements to facilitate an installation in accordance with CAN-ULC-S302, Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems.

11.3.2 Level P1

11.3.2.1 The *control unit* utilizes a single *communication channel* as the primary means of communication. For passive Level P1, *control units* shall employ one of the following *communication channels*:

A One telephone line (number);

B A *one-way radio alarm system*;

C A one-way private radio alarm system;

D A private microwave radio system; or

E An alternative *radio frequency* communications technology that is in compliance with the requirements of Subsection 10.4, Radio Frequency Communications; and CAN/ULC-S301, Standard for Signal Receiving Centre Burglar Alarm Systems and Operations.

11.3.2.2 The *control unit* shall transmit over a single channel to the receiver once every 24 h.

11.3.2.3 The *control unit* shall monitor the *communication channel* to detect a loss of the channel and initiate a local *trouble signal* within 180 s.

11.3.2.4 In the event of a failure in the *communication channel*, all alarm and *trouble signals* shall be annunciated locally.

11.3.3 Level P2

11.3.3.1 The *control unit* shall utilize at least two *communication channels*, one being a telephone line (number) and the other being a *radio frequency communication channel* or alternative network. For passive Level P2, a *control unit* shall employ one of the following combinations of *communication channels*:

A One telephone line (number) and one cellular control channel or public cellular telephone connection;

B One telephone line (number) and a one-way radio system;

C One telephone line (number) and a one-way private radio alarm system;

D One telephone line (number) and a private microwave radio system; or

E One telephone line (number) and alternative *radio frequency* communications equipment that is in compliance with the requirements of Subsection 10.4, Radio Frequency Communications; and CAN/ULC-S301 Standard for Signal Receiving Centre Burglar Alarm Systems and Operations.

11.3.3.2 The *control unit* shall communicate to the *signal receiving centre* equipment once every 24 h.

Exception: Where two communication channels are used, it is permitted to test each communication channel at alternating 24 h intervals.

11.3.3.3 Failure of either channel is reported to the *signal receiving centre* on the other channel within 240 s.

11.3.3.4 The first attempt to send a status change signal shall utilize the *primary communication channel*. Where the *primary communication channel* is known to have failed, *transmission* attempts over the alternate channel (where so required) shall occur.

11.3.3.5 In the event that any *digital alarm communicator transmitter* signal *transmission* is unsuccessful, the information shall be transmitted by means of an alternate or secondary communications path. The *digital alarm communicator transmitter* shall continue its normal *transmission* sequence.

11.3.4 Level P3

11.3.4.1 The *control unit* shall utilize at least two passive *communication channels*, each employing different technologies and different carriers. For passive Level P3, a *control unit* shall employ two of any of the following alternatives of *communication channels* simultaneously:

A Public cellular telephone connection;

B Control channel cellular;

C One-way radio system;

D One-way private radio alarm system;

E Private microwave radio system; or

F Alternate communication equipment complying with this Standard.

11.3.4.2 The *control unit* shall communicate to the receiver once every 24 h.

Exception: Where two communication channels are used, it is permitted to test each communication channel at alternating 24 h intervals.

11.3.4.3 Failure of either channel is reported to the *signal receiving centre* on the other channel within 240 s.

11.3.4.4 An attempt to send a status change signal shall utilize both *primary* and *secondary communication channel*.

11.3.4.5 Equipment employed to provide a *radio frequency communication channel* shall meet the requirements of this Standard, shall facilitate tamper protection and electrical supervision, and shall meet all other requirements to facilitate installations to CAN/ULC-S302, Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems.

11.4 COMMUNICATION CHANNEL SECURITY APPLICATIONS

11.4.1 Application of extent of protection, security level, and *communication channel* security shall be as specified in Table 11.

12 POWER SUPPLIES

12.1 GENERAL

12.1.1 These requirements apply to a power supply located at the protected *premises* and intended to supply energy to the product at the protected *premises*. Power supply requirements for the product at a *signal receiving centre*, *satellite centre*, or *repeater station* are specified in CAN/ULC S301, Signal Receiving Centre Burglar Alarm Systems and Operations.

12.1.2 A product shall not depend solely on commercial power if failure thereof will cause a *false alarm* or render the system inoperative.

12.1.3 Acceptable sources of standby power for the product shall include rechargeable batteries on full float or trickle charge or non-rechargeable batteries.

12.1.4 A battery provided with the product, other than a non-rechargeable battery having an *open circuit* potential of 42.4 V or less, shall be protected by a fuse or circuit breaker rated at not less than 130% nor more than 200% of the maximum operating load on the battery, or comply with Class 2, low-energy power circuit requirements.

12.1.5 If the product is equipped with terminals for the connection of standby power, the terminals shall be marked with, or reference a drawing that shows, their power ratings including voltage, current, and capacity of batteries in ampere hours, and the number and type of batteries to be used.

12.2 RECHARGEABLE BATTERIES

12.2.1 A rechargeable battery shall have sealed cells with spray trap vents and shall be floated or trickle charged.

12.2.2 Batteries shall be located and mounted so that terminals of adjacent cells will be prevented from coming in contact with each other or with metal parts of the battery enclosure as a result of shifting of the batteries. The mounting arrangement shall permit ready access to the cells, if such access is required to check the specific gravity of the electrolyte.

12.2.3 A conditioning charge shall be limited so that, at the maximum obtainable rate of charge, the battery gases will not affect any part of the *control unit*.

12.2.4 The interior of metal cabinets used to enclose vented rechargeable batteries shall be painted with two coats of acid resistant and alkali resistant compound, or shall be protected by baked enamel.

12.2.5 Cabinets used to enclose liquid electrolyte batteries shall be constructed so that the condition of the elements may be observed without disturbing the cells.

12.2.6 If the battery is contained in a compartment in the same cabinet that houses instruments, the cells shall be located below the instrument compartment, or otherwise arranged to reduce the risk of damage to the instruments as a result of leakage or fumes from the battery.

12.2.7 The product manufacturer shall provide all specifications, information, and calculations necessary to determine that the battery is used within its specifications, and confirm that the charging method used complies with the battery manufacturer's specifications and continues to provide a charging current under all conditions of intended use.

12.2.8 All conditions of battery discharge shall comply with the battery manufacturer's specifications, with regard to rate of discharge and with automatic voltage cut-off, if required to prevent polarity reversal or damage.

12.2.9 If two or more cells are used in series or parallel, the conditions of use shall provide for equalization of cells in compliance with the battery manufacturer's specifications.

12.2.10 The conditions of storage shall comply with the battery manufacturer's specifications with regard to position, temperature, and state of charge.

12.2.11 If the battery is of a type that will lose capacity as a result of long periods of inactivity, provision shall be made for cycling of the battery to prevent the condition or for a method of detecting the existence of a capacity loss.

12.2.12 A warning of precautions necessary to prevent premature battery failure, if any precautions are necessary, shall be contained in the installation instructions and shall include position of mounting, temperature limits, state of charge, and periods of inactivity if the battery is of a type that may lose capacity due to these conditions. Markings on the product adjacent to the battery shall indicate either battery type and estimated life or a method of testing battery condition.

12.2.13 The battery shall be supervised for connection and low capacity. Failure and restoration shall provide unique *code*.

12.2.14 Provision shall be made for an automatic dynamic test of the standby battery confirming presence and capacity. Tests may be with each *arming* or delaying or periodically, no less than every 24 h. For servicing, a manual test feature shall also be provided.

12.3 NON-RECHARGEABLE BATTERIES

12.3.1 Compartments for non-rechargeable cells shall be constructed to prevent adjacent cell terminals from contacting each other or the metal enclosure

12.3.2 Non-rechargeable batteries shall be replaced as per the *control unit* manufacturer's recommendations.

12.4 POWER FAILURE

12.4.1 **(REV1)** A burglar alarm *control unit* operated from commercial power shall be provided with standby power sufficient to operate the equipment in the intended condition for 24 h.

Exception No. 1: For product intended for Security Level I applications, a minimum of 4 h standby power is required provided that a commercial power loss signal is transmitted to the signal receiving centre within 60 min of a sustained (more than 30 min) power outage.

Exception No. 2: A signal receiving centre signal may be supplied by one or more uninterruptible power supply (UPS) and/or an emergency electrical power generation system in accordance with CAN/ULC-S301, Standard for Signal Receiving Centre Burglar Alarm Systems and Operations.

12.4.2 **(REV1)** With standby power connected, the burglar alarm *control unit* shall comply with the following:

A Neither loss nor restoration of commercial power shall cause an alarm signal;

B With Exception No. 1 provided in Clause 12.4.1, the *control unit* shall be capable of transmitting commercial power loss signals within 12 h or when the 50% of the standby power capacity has been depleted, whichever comes first; and

C Should an alarm occur during a period of commercial power loss, the *control unit* shall be capable of transmitting commercial power loss signal to the *signal receiving centre* at the same time as the alarm signal, if such power loss signal has not been previously transmitted.

12.4.3 To determine compliance with the requirement in Clause 12.4.2, the *control unit* is to be energized in the normal supervisory condition and the supply circuit is to be interrupted for 60 s and then restored for 60 s for a total of 10 cycles of supply circuit interruption.

12.4.4 Compliance with the requirement in Clause 12.4.1 necessitates the automatic provision of a standby power supply in the event of commercial power loss so that the equipment will be maintained in the intended condition for 24 h for mercantile alarms and bank vault alarms.

12.4.5 Ultimate loss of battery power for the protection circuit shall result in an alarm or *trouble*.

Exception: This requirement does not apply if a signal indicating a power failure is transmitted to the signal receiving centre within 8 h after the beginning of the power failure.

12.4.6 In case of a total power failure, the *control unit* shall ignore and not transmit alarm supervisory information for a stabilization period of 120 s following restoration of power. Within 60 s at the end of the stabilization period, the *control unit* shall initiate the *transmission* of a power restoration signal *code*.

12.4.7 If the power supply is intended to provide a continuous output for the protection circuit and an intermittent output, such as for a *code* transmitter or an alarm sounding device, it shall comply with the requirements of Clause 12.2.7 while supplying the continuous output, but may provide power from the battery while supplying the intermittent output.

12.4.8 Under standby conditions, the continuous output shall not deplete the battery to a level where it cannot provide the intermittent output for the required period. This may be done by removing the constant load after the required standby time has been exceeded, and before the battery capacity has fallen below that required for the intermittent load.

12.4.9 Following an extended power failure and restoration of power, rechargeable batteries shall recharge to 85% of rated capacity within 24 h to provide the required power for standby operation.