June 2, 2008

STANDARDS BULLETIN 2008-08

CAN/ULC-S319-05, Electronic Access Control Systems

FREQUENTLY ASKED QUESTIONS

The following *frequently asked questions* (*FAQ*) is being issued in response to a request for clarification on some of the testing protocol outlined in CAN/ULC-S319-05, Electronic Access Control Systems.

The responses have been endorsed by the ULC Committee on Security and Burglar Alarm Equipment and Systems, the ULC Subcommittee on Control Equipment, and the ULC Working Group on Access Controls.

Should you require any additional information, please contact Mahendra (Mike) Prasad at 416-757-5250 Ext. 61242 or email: mahendra.prasad@ca.ul.com

Yours truly,

G. Rae Dulmage

G. Rae Dulmage
Director, Standards Department & Government Relations Office

No.	Clause/Section	QUESTION	ANSWER
1	Section 1	Does the standard apply to computer equipment used in monitoring console?	Yes, the standard applies to computer equipment using monitoring console (i.e. computer equipment used in monitoring console), except for specific electrical performance tests of Section 7, as noted in Question 2. Classes II, III and IV equipment specify “monitoring” requirements. Such “monitoring” requirements, being performance based, apply irrespective of the type of equipment used. Should the monitoring equipment of an access control system also provide the monitoring of other “system(s)”, i.e. intrusion detection, compliance is required with both the monitoring requirements in CAN/ULC-S319-05 and in the standard applicable to the monitoring of other equipment. The operation of the access control system shall not be adversely be affected by the monitoring of such other system(s).
2	Section 1	UL 294 (Access Control System Units), sec. 1.2 and 27 outline an alternate method to evaluate monitoring console computers based upon testing of representative model with minimum system configuration. Can S319 take a similar approach?	As written, computer equipment is required to comply with all requirements of CAN/ULC-S319-05. However, the intent was only to test for system capability; not all of the electrical performance tests in Section 7. It was not intended for the following tests to apply to computer monitoring equipment if evidence is provided that the computer monitoring equipment complies with relevant Canadian safety standards, such as CSA/CSA-C22.2 No. 60950-1 (Information Technology Equipment-Safety-Part 1: General Requirements): • Subsections 7.3, 7.4, 7.5, 7.8 up to and including 7.38 Although this is not currently specified in CAN/ULC-S319, it is intended that for computer monitoring equipment, the manufacturer specify a minimum system configuration consisting of the following: (i) Operating system class, minimum revision levels/or kernel type and revision level (ii) Microprocessor type, minimum revision level and minimum clock speed (iii) Minimum disk storage (iv) Minimum memory requirements (v) Monitoring software revision level

No.	Clause/Section	QUESTION	ANSWER
3	5.2.3, table 6, 5.5.2.3, table 11 ALERT	Definition of ALERT does not specify where ALERT should occur. Section 5.2.3 and table 6 outline the requirements to ALERT in Monitoring console. Section 5.5.2.3 and table 11 require ALERT at portal for closing. No other requirements of ALERT at protected premises (local) in this standard. Does ALERT in this standard only refer to the signals at monitoring console and portal? No other ALERT required in controlled area?	Yes, the ALERT in this standard only refers to the signals at monitoring console and portal and no other ALERT is required in controlled area. Prescribed “Alert” requirements are only at the portal and at the monitoring console. “Alert” does not have the same meaning as “alarm”, which is for intrusion detection applications. Should an access control system also provide the intrusion detection functions, compliance is required with both the requirements of CAN/ULC S319 and of the applicable intrusion detection standard. The operation of the access control system shall not be adversely be affected by the intrusion detection functions.
4	5.4.1.3 Integrity of Communications	Its definition states “Communication Integrity exists as long as misleading actions or results are not accomplished by operation/request MALICIOUSLY ENTERED in the system by UNAUTHORIZED MEANS”. Does it mean Compromise Test (as in ULC-S304) is required between *reader*s and *access control units*? Or to verify Data Authentication is sufficient.	The extent of “ensuring communication integrity” is not defined under 5.4, but is defined in 5.3, Communication Channel Security, and verified in accordance with 7.39, Communication Security Compromise Test. The channel security starts from the reader to the monitoring console (per 5.4.1.3) for Level IV,
5	6.1.3 and 7.6.1 Trouble	Both sections refer to a “Trouble Signal”. However, Trouble Signal is not clearly defined in this standard. What are the requirements for trouble? Audible? Visual? Local? Monitoring console? What are the differences between “trouble” and “alert”?	“Trouble signal” has the same meaning as that used in CAN/ULC-S304, Signal Receiving Centre and Premise Burglar Alarm Control Units, but in CAN/ULC-S319-05, its referred as an “Alert” at the monitoring console, as specified in items 11 to 15 and 18 to 23 in Table 6, Monitoring Console Alert Requirements. Trouble and Alert are synonymous, however, it should be noted that Trouble causes an Alert.
6	5.1.7.1, table 4 item 9 to 14 Self Diagnostic	To what extend should Control Unit perform self-diagnostic? Control unit circuit only? Communication channel to the readers? Circuits in readers? What are the differences between self-diagnostic and electrical supervision?	“System self-diagnostic” is defined in the Glossary and some requirements are stated in Table 4. The frequency of system self-diagnostic is not defined and it is recognized that some conflicts exist between the communication channel security requirements and electrical supervision. The objective is to signal “faults”. The reporting of some faults is specified (e.g. for communication channel security).

No.	Clause/Section	QUESTION	ANSWER
			Frequency of system self-diagnostic to be considered in the next edition of CAN/ULC-S319. It was intended that unless supervised through other means, self diagnostic is be applied for items 11 to 15, and 18 to 23 in Table 6, Monitoring Console Alert Requirements.
7	4.2 Marking	Marking requirements of section 4.2 only apply to Portal Locking Devices. Why do more marking requirements apply to portal locking devices than to the control unit?	It was intended for 4.2.1 to apply to all access control devices, where applicable; not only to portal locking devices. This intent can be clarified in the next edition of CAN/ULC-S319 as follows (or blend 4.2, Portal Locking Devices, into 4.1, General): 4.2 Access Control Devices ~~Portal Locking Devices~~ 4.2.1 In addition to requirements identified in Clauses 4.1.1 and 4.1.2, the markings on ~~portal locking devices~~ access control devices shall provide the following information…
8	5.1.2.2 Minimum 64 user access levels	Need some guidance how to test or verify 64 levels.	It is required that a minimum of 64 combination of where and when a credentials may satisfy “access granted”. This can be verified from system literature.
9	5.1.3.1	Where were these "types of portal construction" originated?	With regards to 5.1.3.1 (B), it was intended for reference to “Type” to be “Class” for the four classes of equipment defined in this standard. This will clarified in the next edition of CAN/ULC-S319.
10	5.4.3.5 Separation	Need a clarification of what type of "separation" is required.	Separation” has the same meaning as “destruction by removal”. Intent is that the token will be unusable if there is any separation of the encoded information from the token.
11	5.4.5.2.5	Does it mean that for motion detectors, a keylock is required in addition to tamper switches?	The idea is to make it difficult to modify settings by having to remove some “locking” devices such as a screw. A keylock would satisfy the requirements but may be excessive.
12	7.5.2.1, 7.5.3	Should conditions in 7.5.2.1 (over- and under- voltage) also apply to 7.5.3 Power-Limited Circuits?	It was intended for 7.5.2.1-7.5.2.4 to apply to all output circuits, not just Non Power-Limited Circuit. Current requirements appear to be based, in part, on UL 1034 (Burglary-Resistant Electric Locking Mechanisms). This will clarified in the next edition of CAN/ULC-S319 by deleting title 7.5.2 (Non

No.	Clause/Section	QUESTION	ANSWER
			Power-Limited Circuit) and moving 7.5.21-7.5.2.4 into Section 7.5.1, starting from 7.5.1.3.
13	7.6.3 Manual battery test feature	Is a battery capacity test required in the manual test feature?	Yes, it can be effectively tested with a load test
14	7.6.3 Manual battery test feature	What kind of interface of battery status can be acceptable? Red/green LED for pass/fail? LCD to indicate voltage and capacity?	No specific requirements for indication as long as the "manual test feature effectively tests the capability of electronic components or the battery"
15	7.6.4 Supervision	What is the definition of "Protection circuit conductors"?	Protection circuit conductors are input circuit conductors (which have line supervision), such as for connection with readers, motions sensors, door status sensors, tamper switch, etc.
16	7.6.4 Supervision	Do the conductors connecting control unit and portal locking devices need to be supervised?	No, however, protection circuit conductors for connecting bond sensors in Class IV electromagnetic locks need to be supervised (Clause 5.6.7).
17	7.7.4.5, 7.7.4.7 Extended Power Failure	Does "Extended Power Failure" refer to the period in table 24 (30 min to 4 hr)?	Yes - extended power failure is defined in Clause 7.7.4.7 and Table 24, as the time in excess of minimum duration.
18	7.17.9 Temperature Test	Do "10% of Zones" refer to input zones?	Zones refer to any circuit that needs to be supervised (i.e. zones = protection circuits)
19	7.25 Drop Test	Can this test be waived for permanently mounted cord connected products? Answer: This is a "boiler plate" requirement. Whether the test can be waived is a question of consistency with requirements of similar standards.	This test is same as that in CAN/ULC-S303-M91 (Local Burglar Alarm Units), ULC-S306-03 (Intrusions Detection Units), UL294 (Access Control System Units). For the next edition of CAN/ULC-S319 it is recommended to waive this test for permanently mounted cord-connected products.
20	7.33 Static Discharge Test	Maintaining 10% +/- 5% RH in a humidity chambers could be a burden for most of the test labs, especially if a technician has to stay in the chamber to perform the test. Is the intent of the standard that 10%+/-5% RH has to be maintained while the lab technician is conducting the test? Or it is the samples to be pre-conditioned in this environment.	This test is same as that in ULC-S306-03 (Intrusion Detection Units). For the next edition of CAN/ULC-S319 it is recommended to re-evaluate this level of humidity and consider specifying a higher value for humidity.
21	7.35 Corrosion	Can the exception for control unit also apply to monitoring console equipments (computers etc), which are supposed to be installed in the similar or better indoor environment as control units?	Yes

No.	Clause/Section	QUESTION	ANSWER
22	7.36 Stability	(i) Similar to 7.35, can monitoring console equipments also be exempted? (ii) Therefore, can we further interpret that only non-inherently stable products, such as motion detectors, biometric readers are subject to this test?	(i) Yes, monitoring console equipments can also be exempted, similar to 7.35. (ii) No, it cannot be interpreted that only non-inherently stable products, such as motion detectors, biometric readers are subject to this test. However, for the future, consideration will be given for this test to apply only to non-inherently stable products in the next edition of CAN/ULC-S319.
23	9.1.2 Outdoor	Can same exception (mark for indoor use only) apply to readers for indoor use?	In addition to portal locking devices, there is a good probability that readers and REX may also be installed outdoors. Therefore, the intent of 9.1.2 is for other devices that may be installed outdoors. It will be recommended to revised 9.1.2 as follows for the next edition of CAN/ULC-S319: "Unless specified and marked for indoor use only (see Clause 7.10.2), products are assumed to be installed indoor and outdoor, or the like, and shall comply with the requirements specified in this Section."
24	9.3.1.7 Rain Test	Can a voltage meter with internal resistance higher than 30 k Ohm be used for this test? Answer: This is a question of consistency with methods used with similar standards.	This requirement is based on CAN/ULC-S303-M91 (Local Burglar Alarm Units) and ULC-S306-03 (Intrusion Detection Units). For the next edition of CAN/ULC-S319, It will be recommended to revise 9.3.1.7 to indicate that minimum 30 KΩ resistance should be used.
25	9.3.1.8 Rain Test	This section specifies 900 mm between the central nozzle and the EUT, while 1400 mm is shown on Figure 17. Which distance should we apply? (for reference: 1400 mm in UL294)	1400 mm is from the centre of the nozzle to the focal point; not to the EUT. All dimensions are correct as specified and consistent with other ULC standards.
26	9.3.5 Corrosion	Only 9.3.5.2.5 gives number of samples (3) of portal locking device for salt spray test. How many samples are required for each corrosion test?	One sample for each of the 3 environments (total of 3 samples) per 9.3.5.1.1.