STANDARDS UPDATE NOTICE (SUN)
ISSUED: May 30, 2019

STANDARD INFORMATION

This SUN establishes continuing certification for currently Listed CSA C22.2 No. 0.8 certification reports.

Standard Number: CSA C22.2 No. 0.8
Standard Name: Safety Functions Incorporating Electronic Technology
Standard Edition and Issue Date: 4th Edition dated February 1, 2019
Date of Revision: February 1, 2019
Date of Previous Revision of Standard: 3rd Edition Reaffirmed 2016

EFFECTIVE DATE OF NEW/REVISED REQUIREMENTS

Effective Date: February 1, 2020

IMPACT, OVERVIEW, AND ACTION REQUIRED

Impact Statement:

- February 1, 2020 is the effective date. New and revised products submitted for certification on and after the effective date will be required to be investigated to the latest version of the appropriate Standard in effect.

- Existing certifications will be allowed to continue to be certified after February 1, 2020 provided there are no changes to the design that require a certification decision or until a new/revised requirement in the appropriate Standard is determined as “Action Required” to require a file review in the future. For example, if changes to the design, ratings, or the use of alternate components requiring a certification decision are submitted after the effective date, the product needs to be evaluated to the latest version of the Standard.

Overview of Changes:

- Addition of requirements for corrupted data
- Addition of requirements for management of unintended or unauthorized access

Specific details of new/revised requirements are found in table below.

Client Action Required:

Current Listings Not Active? – Please immediately identify any current Listing Reports or products that are no longer active and should be removed from our records. We will do this at no charge as long as Intertek is notified in writing prior to the review of your reports.

STANDARD INFORMATION

CLAUSE	VERDICT	COMMENT
		Additions to existing requirements are underlined and deletions are shown ~~lined out~~ below.
5	Info	**Functional safety requirements**
5.4	Info	**Safety requirements and design**
5.4.10	Info	**Remote control — Wireless devices**
5.4.10.5		***New clause added;*** Corrupted data shall not lead to an unsafe state. Faults caused by transmission errors shall be detected. Corrupted messages shall result in a retry with a maximum of three retries, after which the system shall indicate an error and go to a safe state.
5.4.11		***New clause added;*** **Management of unintended or unauthorized access** Devices with communication ports shall have considerations for management of unintended or unauthorized access, e.g., cybersecurity, considering accepted industry good practice, and cybersecurity standards and legislation. Remote modification of protective functions, firmware/software, configuration, etc. shall be triggered by or accepted by an operator action at the device. Note: Standards with cybersecurity management features should be used.
		CUSTOMERS PLEASE NOTE: This Table and column "Verdict" can be used in determining how your current or future production is or will be in compliance with new/revised requirements.