

Subject 1776

October 3, 2018

SUMMARY OF TOPICS

The following changes in requirements to the Standard for High-Pressure Cleaning Machines, UL 1776, are being proposed for preliminary review and comment only:

1. For Preliminary Review Only: Rechargeable Battery-Powered High Pressure Cleaning Machine Requirements

2. For Preliminary Review Only: Pressure Deviation Limit

COMMENTS DUE: November 2, 2018

This proposal is for review and comment only (no ballot at this time). Please note that comments on a preliminary review document will not receive a response from the proposal author through CSDS. Instead, the proposal author will be asked to review the comments and adjust the proposals and/or supporting rationale as the author determines to be appropriate. The preliminary review process is an informal mechanism that provides authors with the opportunity to refine their proposals before they advance to the next stage in UL's standards development process.

In some cases, the author of the proposals may choose to discontinue them. In this case, the author need not do anything after preliminary review has ended. Normally, the next step in the process is the more formal STP ballot and stakeholder review process. Only comments posted during the STP ballot and stakeholder review process will be provided with a response in CSDS.

For your convenience in review, proposed additions to existing requirements are shown underlined and proposed deletions are shown ~~lined-out~~.

1. For Preliminary Review Only: Rechargeable Battery-Powered High Pressure Cleaning Machine Requirements

RATIONALE

Proposal submitted by: Darrin Conlon, UL LLC

These proposed requirements are intended to incorporate the use of UL 2595 in the investigation of battery-powered high pressure cleaning machine. UL 2595 is the Standard for General Requirements for Battery-Powered Appliances. It is a "horizontal" standard that is structured to be used in conjunction with end-product standards.

Action Items for the UL 1776 STP:

1. With respect to the safety critical function performance levels, the STP is requested to recommend the Performance Level (PL) for each specified safety critical function (SCF) in Table B2 in the proposal below. For each SCF, please recommend a PL of a, b, or c.

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM**



Documents

Document Sharing Hub

2. The STP is also requested to identify other relevant SCFs and their respective PL.

With respect to Safety Critical Functions (SCF) and Performance Levels (PL), ISO 13849-1 provides a simplified method for establishing the associated reliability of a safety critical control function in consideration of the risk of injury associated with its failure. The control function is assigned a Performance Level (PL) which then may be fulfilled with a control system that satisfies both structural requirements and minimum calculated failure rates expressed in $MTTF_d$ (Mean Time To Dangerous Failure).

Risk Assessment

The method of risk assessment used in ISO 13849-1 follows the same general approach as in ISO 12100, where primary consideration is given to the severity of the hazards and the frequency of encountering these hazards. The risk associated with that hazard is then subsequently reduced by consideration of the probability, P, for avoiding the hazard. In ISO 12100, this analysis is carried out using the original, unmitigated hazard followed by all the risk mitigation techniques used to determine the resulting residual risk of the appliance with respect to the hazard (and phase of use) under consideration.

When assessing a safety-critical function (SCF), this process is not so clear: In this case, the safety-critical function may be only one of many elements in the appliance design intended to reduce the risk associated with a hazard. The goal then is to establish the change in residual risk associated with the failure of the SCF and to determine the remaining residual risk and whether it is still acceptable. This method, taken from ISO 12100, is not well suited to be used in this manner and additional considerations must be taken into account to yield meaningful results. Part of the issue is due to the fact that a binary tree is used to generate one of a discrete number of PLs and this sometimes fails to recognize small differences in risk. While this makes this method easy to use, it introduces some problems in analysis.

Residual Risk Analysis

In recognition of the hazards associated with some appliances in general, UL appliance standards employ a number of risk mitigation techniques, built into the requirements of the standard, to reduce the risk to an acceptable level. These techniques are often intended to work together, as a system, to achieve the required risk reduction. An electronic control providing an SCF is often only one part of this system and its failure, therefore, does not leave the appliance without other risk mitigation elements. To assess the effect of the loss of an electronic control function two things are considered.

First, the control function must fulfill a required safety element of the standard. The standard is presumed to have left the appliance with an acceptable level of residual risk. Controls whose failure does not increase the risk beyond this already accepted level are not considered to be a SCF within this standard.

In addition, there must be a substantial impact on residual risk due to the failure of the SCF. To determine this, performance levels can be assessed both with and without the presence of the SCF, but with all other risk mitigation in place. It is possible that this will yield the same PL with or without the SCF.

If it is recognized that the SCF fulfills a required safety function, but the PL remains the same with or without its presence, then in these cases, a minimum level of PL = a is used.

While the method above yields meaningful results under conditions of normal operation, there are SCFs that are relied on to protect the user under conditions of reasonably foreseeable misuse or other cases where the risk occurs only under a specific set of unlikely preconditions. An example of this is the case in systems to protect against restart after power interruption, since restart requires the appliance to be switched on, plugged in and power interrupted and restored while the user is nearby.

In cases such as these, the unlikelihood associated with the event should dominate the analysis. The method used in ISO 13849-1, however, gives priority to the severity of the hazard (S, F, P) such that, for high severity cases, it would not be possible to assign a severity less than $PL = c$, because the frequency (F) is analyzed second. In cases such as these the order of analysis should be reversed (F, S, P) allowing the frequency of exposure to have a higher influence over the outcome.

Performance levels have been assigned in this standard reflecting common cases. There is recognition that there may be SCFs in the future not yet contemplated by this standard, and ISO 13849-1 along with this Appendix may be used for guidance in setting the appropriate performance level.

Performance Levels (PL)

ISO 13849-1 provides methods for achieving the various performance levels. These solutions generally require certain structures such as dual channel, single channel and single channel with diagnostics. Single and dual channel refer to the functional redundancy of the control. Since protective control and safety-critical function circuit evaluations have dual channel designs evaluated before performance levels of other structures are even considered, most of the interest in ISO 13849-1 is focused on single channel designs. While ISO 13849-1 permits diagnostic monitoring of lower reliability single channel systems as an alternative to unmonitored high reliability single channel, there is a concern that these diagnostics are unlikely to be noticed by an operator of the appliance under use conditions. As a result, the standard generally prohibits these solutions as an alternative to higher reliability designs.

As a result, the single channel designs afforded by this method require increasingly higher $MTTF_d$ as the PL increases due to increasing risk.

It may be possible that a case could exist where a diagnostic reflecting the unavailability of a SCF is present and recognizable well in advance of the operator being exposed to the increased risk. It could be appropriate in this case to consider a structure that provides a diagnostic as a means of achieving the required performance level.

The reliability of portions of the electronic circuit that are responsible for the safety-critical function are evaluated by the $MTTF_d$ (Mean Time To Dangerous Failure) calculations required to meet the necessary Performance Level (PL) associated with the safety-critical function as described in ISO 13849-1; see Annex H. In cases of single channel designs, the required $MTTF_d$ for each performance level is as follows:

PL = a: $MTTF_d = 5$ years;

PL = b: $MTTF_d = 20$ years;

PL = c: $MTTF_d = 50$ years.