IEC 61508 Assessment Recommendations

Project:
SLATE and 7800

Customer:
Honeywell
Houston, TX
USA

Contract No.: Q23/07-078
Report No.: HON 23/07-078 R001
Version V1, Revision R0, December 8, 2023
Molly O'Brien

Confidential Information

Table of Contents

1 Purpose and Scope

This document lists the Recommendations for Future Improvement (**RFI's**), resulting from the surveillance project for the Honeywell SLATE and 7800. RFI's include non-compliances, whose resolutions are permitted to be deferred until after issuance of an initial or renewed certificate. This can occur for various reasons, such as to allow earlier issuance of a certificate or to defer work that is not immediately required (e.g., documentation updates, optional suggestions, etc.).

These RFI's may be related to areas / topics which need to be improved for a successful First Change Audit and/or Surveillance Audit or may just be optional suggested improvements. Accordingly, each RFI is categorized as a First Change Audit Requirement (**FCAR**), a Surveillance Audit Requirement (**SAR**) or Opportunity for Improvement (**OFI**).

- **FCAR's** are required to be implemented prior to the next time the change process is used to make a change to the certified product, or to develop a new product to be certified. This is because the purpose of a First Change Audit is to make sure the **FCAR's** have been implemented, and that the change related tasks are being performed properly per the change process prior to the release of the changed product to the field. Once this audit is successfully passed, the manufacturer is permitted to make future design changes without the need for 3rd party functional safety audits during the certification period.
- **SAR's** are improvement requests, which need to be implemented prior to the next Surveillance Audit. A Surveillance Audit is generally performed just prior to the Surveillance Audit due date and its results determine whether the certificate may be renewed for another certification period.
- **OFI's** are optional recommendations, given to the manufacturer as a possible place to improve the development process or documentation. Implementing these recommendations is not required to comply with the standard.

RFI's are sometimes phrased very specifically, to clarify the topic as precisely as possible. Where a specific recommendation is made, it should be understood to be an example of a possible solution, for which there may be other solutions. Any solution can be accepted, if it fulfills the objective of the identified weakness in the process or documentation.

2 List of Recommendations for Future Improvement

exida ID	Action Item ID	RFI Category	Action Item
FFA	AID-001	SAR	IEC 61508 requires that Field Incident Reporting is done in a formal way. Currently Honeywell is categorizing all returns as Warranty and tracking the cost of returns. The return process needs to be strengthened to include categorizing failures into logical causes. An example of causes is shown below. The frequency of returns by cause should be evaluated several times per year to detect any systematic issue that may be affecting product quality and/or reliability. Example Return Categorization: • Order Entry / BOM Error • Assembly • Manufacturing • Quality • Design • End User Caused • Shipping / Packaging IEC 61508 guidance on field incident report can be found in IEC 61508:2010 Part 1 Clause 5.2.2, Clause 6.2.5 (f), and Clause 6.2.6.
SM	AID-002	SAR	Please review and clarify ambiguous wording in the SLATE Safety Manual. For example: • The SLATE Safety Manual (Revision 10, Section 2.10) lists “non SIL” function for the Limit Control Module, including temperature inputs that are used in some optional safety functions, i.e., skipping the purge step when the temperature is hot enough. Some of these inputs are SIL rated and have been analyzed in detail in the FMEDA. Clarify what inputs can be used for safety, so this is clear to the reader. • The SLATE includes many modules and can be used in different configurations. If there are SLATE configurations that do not meet SIL 3 with HFT=0, please clarify this for the reader.

3 Reference Documents

The services delivered by *exida* were performed based on the following standards:

N1 IEC 61508:2010, 1-3 Functional Safety of E/E/PE Safety-Related Systems

4 Status of the Document

4.1 Liability

exida prepares reports based on methods advocated in International standards. *exida* accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

4.2 Version History

Contract Number	Report Number	Revision Notes
Q23/07-078	HON 23/07-078 R001 V1, R0	Initial version of this report. The RFIs are new in this surveillance audit. MOB 12/8/23.

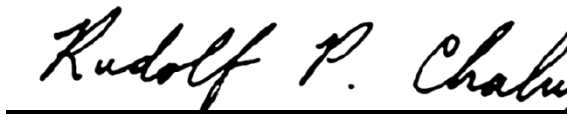
Review: Chris O'Brien, *exida*, 12/28/23
Status: Released 12/28/23

4.3 Future Enhancements

At request of client.

4.4 Release Signatures

Dr. Molly O'Brien, CFSP, Senior Safety Engineer



Rudolf P. Chalupa, CFSE, Senior Safety Engineer