IEC 61508 and ISO 26262
Tool Qualification
OEMx™ Development Process Tool Suite

Project:
OEMx™

Customer:
exida Innovation LLC
Sellersville, PA

Contract No.: Q24/10-031
Report No.: exi 24-10-025 R001
Version V1, Revision R2, January 6, 2025
Dave Butler

Management summary

This document describes the assessment of the 2.5 version of the OEMx™ Integrated Development Process Tool Suite from exida Innovation LLC.

Justification has been provided for a claim of TCL1.

OEMx has been shown to be compliant with requirements to the levels of SIL 4 for IEC 61508 and ASIL D for ISO 26262 (see section **Error! Reference source not found.** for specific editions of standards for each version). These tools may be used in the development of safety products if they are used in accordance with all instructions and constraints found in the standards and the user documentation for the tools.

Table of Contents

Management summary 2

1. Purpose and Scope 3

2. Project management 4
   - 2.1 *exida* 4
   - 2.2 Roles of the Parties Involved 4
   - 2.3 Reference documents 4
     - 2.3.1 Standards / Literature used 4
     - 2.3.2 Documentation provided by *exida* Innovation 4
     - 2.3.3 Documentation generated by *exida* 4

3. Scope of Assessment 5

4. Details of Assessment 5
   - 4.1 Requirement (ISO 26262-8 11.4.1) 5
   - 4.2 Validity of Predetermined Tool Qualification (ISO 26262-8 11.4.2) 5
   - 4.3 Usage Environment (ISO 26262-8 11.4.3) 5
   - 4.4 End User Usage of a Software Tool (ISO 26262-8 11.4.4) 5
   - 4.5 Evaluation of Software Tools (ISO 26262-8 11.4.5) 5
     - 4.5.1 REQx - Requirements Management Tool 5
     - 4.5.2 ARCHx – DFMEA/DDMA and FMEDA Information Gathering Tool 6
     - 4.5.3 FMEDAx – Reliability Metric Prediction Tool 6
   - 4.6 Qualification of a Software Tool (ISO 26262-8 11.4.6) 6
     - 4.6.1 Increased Confidence from Use 6
     - 4.6.2 Tool Version Control 7
     - 4.6.3 Tool Manuals 7
     - 4.6.4 Tool Error Recognition 7

5. Terms and Definitions 7

6. Status of the document 8
   - 6.1 Liability 8
   - 6.2 Version History 8
   - 6.3 Future Enhancements 8
   - 6.4 Release Signatures 8

1. Purpose and Scope

This assessment report covers the tool qualification of the 2.5+ version of OEMx including REQx, ARCHx, and FMEDAx.

2. Project management

2.1 *exida*

exida Certification LLC is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 400 billion hours of field failure data.

2.2 Roles of the Parties Involved

exida Innovation LLC	Developer of OEMx
exida Certification LLC	Performed Tool Qualification

2.3 Reference documents

2.3.1 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

ID	Document	Contents
[N1]	IEC 61508:2010, Parts 1	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	ISO 26262:2018, Part 8, Clause 11	Road vehicles — Functional safety — Part 8: Supporting processes

2.3.2 Documentation provided by *exida* Innovation

ID	File	Version	Date
[D1]	OEMx User Manual	2.5	9/11/2024
[D2]	OEMx Validation Test Plan	2.5	10/02/2024

2.3.3 Documentation generated by *exida*

ID	Filename	Document Contents
[R1]	exi 24-10-031 R001	This report
[R2]	*A Functional Safety Development Process Example,* White Paper, exida, Sellersville, PA, www.exida.com, V1R1, August 2024	Description of development process in which OEMx is used

3. Scope of Assessment

This assessment is applicable to OEMx V2.5+ including the REQx, ARCHX, and FMEDAx applications.

4. Details of Assessment

4.1 Requirement (ISO 26262-8 11.4.1)

IEC 61508, ISO 26262-8 Tool Qualification is needed for any functional safety development process.

4.2 Validity of Predetermined Tool Qualification (ISO 26262-8 11.4.2)

The confirmation review by an independent organization (*exida* Certification LLC) was performed. This meets the I3 level of independence from ISO 26262-2 which meets the requirements of ASIL D.

4.3 Usage Environment (ISO 26262-8 11.4.3)

The OEMx tools are intended to be used in a design process [R2].

4.4 End User Usage of a Software Tool (ISO 26262-8 11.4.4)

The usage of a software tool shall be planned and documented by the user of the tool. Needed information about OEMx is contained in [D1].

4.5 Evaluation of Software Tools (ISO 26262-8 11.4.5)

exida uses a three level set of TI definitions which expand upon ISO 26262 but are indicated by the descriptions in IEC 61508:

- TI3 – generates outputs which can directly or indirectly contribute to the executable code of the safety related system
- TI2 – supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software
- TI1 – generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system. No justification required.

These expand on ISO 26262 where TI2 merges the *exida* TI3 and TI2.

The TD Definitions are:

- TD3 – Low confidence in error detection (use when TD2 or TD3 are not justified) 0 – 60%
- TD2 – Medium level of confidence that an error / erroneous output is detected 61% - 90%
- TD1 – High level of confidence that an error / erroneous output is detected 90%+

4.5.1 REQx - Requirements Management Tool

REQx is a requirements management tool with Test tracking and implementation tracking capability. An error in REQx may delete/remove an important requirement. Therefore, it is rated as TI2. As requirements are presented to a review committee, error detectability is TD1, at least 90% probability that an error will be detected. This results in a tool confidence level of TCL1.

4.5.2 ARCHx – DFMEA/DDMA and FMEDA Information Gathering Tool

ARCHx is a tool that can be used as a DFMEA/DDMA architecture design verification tool. The biggest risk in DFMEA is failing to identify a functional failure mode although this is not a failure of the tool. Expert team members are needed to help prevent this when guidewords are used. ARCHx supplies expert Knowledge Bases to reduce the risk of overlooked functional failure modes. An error in the ARCHx tool may not prevent/delete/remove an important failure mode. Therefore, it is rated as TI2. As DFMEA results are presented to a review committee, error detectability is TD1, at least 90% probability that an error will be detected. This results in a tool confidence level of TCL1.

A second use of ARCHx is as a tool to gather the information needed for FMEDA. In that application, a tool error may delete/remove/modify important information. However, this is recognized in the FMEDA as the information is needed to proceed. Therefore, when used in this application, ARCHx is classified as TI1. No further justification is required.

4.5.3 FMEDAx – Reliability Metric Prediction Tool

FMEDAx is a tool used to predict reliability metrics. These are used for business and qualification purposes but do not directly or indirectly contribute to the executable code (including data) of the safety-related system. The highest risk is component failure mode assignment by the user (Underallocation or Overallocation) which is detected by the tool and displayed as shown below.

OA	Overallocated – warning to user	Overallocated – warning to user	0
UA	Underallocated assume worst case	Underallocated assume worst case	0

Other errors are detected and warning symbols are displayed. OEMx provides many “Checks” or “Warnings.” These include:

- Any object in the tree marked as “Need Review” will display at a lighter color and start with “*”
- Deviation Objects without an assigned Potential Impact will end with a ⚠ symbol
- FMEDAx Components without an assigned CRD will end with a symbol
- FMEDAx Components missing Functional Failure Mode links will end with a symbol
- FMEDAx Components with missing “Function” field will end with a symbol

Undetected calculation errors in the software may mislead design decisions. Therefore, it is rated as TI2. A reasonability check on all results is recommended by using www.SILSafeData.com which displays expected results for many device types. In addition, FMEDA results are presented to a review committee. For safety certified devices, the results are carefully reviewed by *exida* Certification experts. These detection methods justify error detectability of TD1. This results in a tool confidence level of TCL1.

4.6 Qualification of a Software Tool (ISO 26262-8 11.4.6)

ISO 26262 requires no qualification methods (e.g., increased confidence from use, validation/testing) at TCL1. However, *exida* recommends qualification for all software tools with the following activities:

4.6.1 Increased Confidence from Use

An effective development process needs tools that are understood by those who use them. Perhaps the most important method for understanding tool functionality is usage. Tools must be used by those who are competent. Tool training and competency evaluation are the responsibility of the user. *exida* Innovation offers training courses in DFMEA/DDMA and FMEDA.

4.6.2 Tool Version Control

All tools must be under version control so that a consistent version is used within a project. Tool version should be archived in case of need in future device changes. This is the responsibility of the user.

4.6.3 Tool Manuals

Tool Manuals shall be available for all those using a tool. In OEMx, the User Manual [D1] is embedded within tool and available from the main menu.

5. Terms and Definitions

ASIL	Automotive Safety Integrity Level
DFMEA	Design Failure Modes and Effects Analysis
DDMA	An enhanced DFMEA with Functional Safety Parameters added called Design Deviation and Mitigation Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
SIL	Safety Integrity Level
TD	Tool [error] Detection
TI	Tool Impact
TCL	Tool Confidence Level

6. Status of the document

6.1 Liability

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

6.2 Version History

Contract Number	Report Number	Revision Notes
Q24/10-031	exi 24-10-031 R001 V1R1	Added definitions and modified acronym for TCL from "Tool Claim Limit" to "Tool Confidence Level", VAM – 1/7/2025
Q24/10-031	exi 24-10-031 R001 V1R0	Complete and Review; DEB - 10/4/2024

Review: V1, R1: Valerie Motto, 10/04/2024

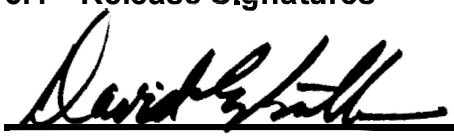
V1, R2: Dr. William Goble, added additional warning symbols.

Status: Released, 10/04/2024

6.3 Future Enhancements

Future enhancements prepared at the request of the client.

6.4 Release Signatures



David Butler, Principal Safety Engineer

Valerie Motto, Senior Safety Engineer

- END OF DOCUMENT