



IEC 61508 and ISO 26262 Tool Qualification Assessment

Project:
PC-lint Plus

Customer:
Vector Informatik, GmbH
Stuttgart, Germany

Contract No.: Q22/10-029
Report No.: GIM 18-11-045 R001
Version V2, Revision R2, February 9, 2023
Dave Butler



Management Summary

The Functional Safety Assessment of the Vector Informatik PC-lint Plus development project, performed by *exida*, consisted of the following activities:

- *exida* assessed the development process, including the Modification process, used by Vector Informatik through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* assessed the development process, including the Modification process, used by Vector Informatik through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of ISO 26262. The assessment was executed using subsets of the ISO 26262 requirements tailored to the work scope of the development team.

This document describes the assessment for the Vector Informatik PC-lint Plus. The Vector Informatik PC-lint Plus tool has been shown to be compliant with development process requirements of IEC 61508. A suitable combination of validation testing and confidence in use, along with the assessment of the development process shows that the tool is compliant with development tool requirements from IEC 61508 and ISO 26262.

PC-lint Plus is compliant for use in the development of safety products, up to SIL 4 for IEC 61508 and ASIL D for ISO 26262, when used in accordance with all instructions and constraints in the user documentation for the tools.

NOTE: Vector Informatik, GmbH purchased Gimpel Software, LLC in 2022. For simplicity, references to Gimpel Software in this document, pertaining to the period of time prior to the purchase (when the initial certification assessment was performed), have been changed to refer to Vector Informatik.

Table of Contents

Management Summary	2
1. Purpose and Scope	5
1.1 Tools and Methods Used for the Assessment	5
2. Project Management.....	6
2.1 <i>exida</i>	6
2.2 Roles of the Parties Involved.....	6
2.3 Reference documents	6
2.3.1 Standards / Literature Used	6
2.3.2 Documentation provided by Vector Informatik, GmbH	6
2.3.3 Documentation generated by <i>exida</i>	7
2.4 Assessment Approach.....	8
3. Product Description	8
3.1 Software Version Number	8
4. Details of Assessment	9
4.1 IEC 61508 Requirements	9
4.1.1 On-line Support Tools.....	9
4.1.2 Selection of Off-line Support Tools	9
4.1.3 Product Manuals for T2 tools	9
4.1.4 Failure Mechanisms of Tools and Potential Mitigation Measures	9
4.1.5 Evidence of tool conformance to its documentation	9
4.1.6 Tool Compatibility	9
4.1.7 Modification Process.....	9
4.2 ISO 26262 Requirements.....	10
4.2.1 General Requirement	10
4.2.2 Validity of Predetermined Tool Confidence Level or Qualification	10
4.2.3 Environmental and Functional Constraints and General Operating Conditions. 10	
4.2.4 Planning Usage of a Software Tool.....	10
4.2.5 Required Information about the Tool.....	10
4.2.6 Description of Software Tool Usage.....	10
4.2.7 Intended Tool Usage and Tool Confidence Level.....	10
4.2.8 Qualification of Software Tools.....	11
4.2.9 Documentation of Tool Qualification	11
4.2.10 Validation of the Software Tool	11
4.2.11 Increased Confidence from Use.....	11
4.2.12 Evaluation of the Tool Development Process	11
5. 2023 IEC 61508 Functional Safety Surveillance Audit	12
5.1 Roles of the Parties Involved.....	12



5.2	Surveillance Methodology	12
5.2.1	Documentation provided by Vector Informatik	12
5.2.2	Surveillance Documentation generated by <i>exida</i>	13
5.3	Surveillance Results	13
5.3.1	Procedure Changes	13
5.3.2	Engineering Changes	13
5.3.3	Impact Analysis	13
5.3.4	Field History	14
5.3.5	Safety Manual	14
5.3.6	FMEDA Update	14
5.3.7	Evaluate use of certificate and/or certification mark	14
5.3.8	Previous Recommendations	14
5.4	Surveillance Audit Conclusion	14
6.	Terms and Definitions	14
7.	Status of the document	15
7.1	Liability	15
7.2	Version History	15
7.3	Future Enhancements	15
7.4	Release Signatures	15

1. Purpose and Scope

This document describes the results of the functional safety assessment of the Vector Informatik PC-lint Plus tool, by *exida*, according to the accredited *exida* certification scheme which includes the requirements of IEC 61508: 2010 and ISO 26262:2018.

The purpose of the assessment was to evaluate the compliance of:

- the PC-lint Plus tool development processes, procedures and techniques with the managerial IEC 61508-1 and -3 requirements
and
- the PC-lint Plus tool with the relevant software tool requirements in IEC 61508-3
and
- the PC-lint Plus tool with the relevant software tool requirements in ISO 26262-8

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

The results of this assessment provide the safety instrumentation engineer with confidence that sufficient attention has been given to systematic failures during the development process of the device and that the producer of the software has done all they could to pre-qualify the tool. The tool user may still need to meet some tool qualification requirements, such as: documenting the justification of the use of the tool in their process; documenting any mitigations external to the tool to further detect errors in the tool's output; etc.

1.1 Tools and Methods Used for the Assessment

This assessment was carried out by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508. Additionally, ISO 26262 tool requirements, that are not met by compliance with the IEC 61508 requirements were identified and assessed.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The Original assessment was planned by *exida* and Vector Informatik (see [R2]).

The assessment steps and results were continuously documented by *exida* (see [R1]).

The 2023 Surveillance Audit steps and results were documented by *exida* (see [R3]).

2. Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability 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 350 billion hours of field failure data.

2.2 Roles of the Parties Involved

Vector Informatik	Developer of PC-lint Plus static analyzer tool
<i>exida</i>	Performed Tools Assessment

Vector Informatik contracted *exida* with the IEC 61508 and ISO 26262 Functional Safety Assessment of the above-mentioned software.

2.3 Reference documents

Note: Documents revised after the 2020 audit are listed in Section 5 2023 IEC 61508 Functional Safety Surveillance Audit.

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, Part 3	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 3: Software requirements
[N2]	ISO 26262:2018, Parts 8	Road vehicles — Functional safety — Part 8: Supporting processes

2.3.2 Documentation provided by Vector Informatik, GmbH

ID	File	Version	Date
D049	arch.pdf		10/17/2019
D023b	coding_guidelines.pdf		10/23/2019
D004b	configuration_auditing_report_form.pdf		10/23/2019
D004	configuration_management.pdf		10/23/2019
D019	customer_notification_procedure.pdf		10/23/2019
D010	documentation_change.pdf		10/23/2019
D064b	email_validation test cases.msg		10/25/2019
D053	exida_design_review_examples_20190521.pdf		5/21/2019
D043b	exida_engineering_change_example_20191014.pdf		10/14/2019
D088	exida_impact_analysis_examples_20190524.pdf		5/24/2019



ID	File	Version	Date
D058	exida_peer_review_examples_20190521.pdf		5/21/2019
D057	func_coverage.txt		10/23/2019
D043	manual.pdf	Rev. 1.3	7/29/2019
D051b	manual.pdf	Rev. 1.3	7/1/2019
D078	manual.pdf	Rev. 1.3	7/1/2019
D091	manual.pdf	Rev. 1.3	7/1/2019
D062	pclp-1.3.5-results.txt		10/24/2019
D062b	pclp-1.3-results.txt		10/24/2019
D079	pclp-sca.pdf		10/23/2019
D080	pclp-sca-review.pdf		10/23/2019
D074b	pf-results-detailed.txt		10/23/2019
D074	pf-results-summary.txt		10/23/2019
D061b	policy.Int		10/23/2019
D003	project_plan.pdf		10/18/2019
D061	static_analysis.pdf		10/23/2019
D043c	test_plan.pdf		10/23/2019
D065	test_plan_review.pdf		10/23/2019
D021b	tool_qualification.pdf		10/23/2019
D057b	uncovered_func_category_counts.txt		10/23/2019
D054	verification_results.pdf		10/23/2019

2.3.3 Documentation generated by *exida*

ID	Filename	Document Contents
[R1]	GIM 18-11-045 V1R1 SC001 IEC 61508 Tool Cert - PC-lint Plus.xlsm	IEC 61508 Safety Case for PC-lint Plus
[R2]	Gimpel PC-lint plus certification proposal v2.pdf	Assessment Project Proposal

2.4 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508 and ISO 26262.

The assessment was planned by *exida* and agreed with Vector Informatik [R2].

The following IEC 61508 objectives were subject to detailed auditing at Vector Informatik:

- FSM planning, including
 - Tool Life Cycle definition
 - Scope of the FSM activities
 - Documentation
 - Activities and Responsibilities (Training and competence)
 - Configuration management
- Tool Requirements Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Software related V&V activities including documentation, verification
- Tool Validation Testing

3. Product Description

PC-lint Plus is a configurable static analysis tool that finds issues in C and C++ programs. The purpose of the analysis is to determine potential problems in programs before integration or porting, or to reveal unusual constructs that may be a source of subtle, otherwise undetected, errors. Because it looks across several modules rather than just one, it can determine things that a compiler cannot.

PC-lint Plus is able to report bugs and potential bugs, such as null pointer de-reference, out of bounds access, and improper operation order. It will also point out the use of dubious constructs and substandard practices that are likely to result in buggy code or code that is difficult to reason about. PC-lint Plus can also be configured to diagnose common coding standard violations, such as the MISRA C and MISRA C++ guidelines. Each diagnostic message is assigned a unique number and a great deal of flexibility is provided for the control of when and how messages are delivered. In particular, the format of the messages emitted is customizable, and messages can be enabled/disabled for individual files, functions, lines and for specific symbols, calls, expressions, statements, types, etc.

PC-lint Plus offers a number of distinguishing features including:

- Value Tracking
- Strong Type Checking
- Dimensional Analysis
- User-defined Function Semantics

PC-lint Plus can be used to properly subset the C or C++ language, to meet the IEC 61508 and ISO 26262 requirements for use of those languages.

3.1 Software Version Number

This assessment is applicable to the 2.0 version of PC-lint Plus (and later).

4. Details of Assessment

4.1 IEC 61508 Requirements

4.1.1 On-line Support Tools

PC-lint Plus is considered an off-line support tool because it is only used during the development of the software (i.e., it is not used during the run time of the software analyzed). Therefore, the requirements for on-line support tools do not apply.

4.1.2 Selection of Off-line Support Tools

These requirements apply to the organization that is selecting the tools to be used for a development project. Therefore, they apply to the tool user as opposed to the tool developer.

4.1.3 Product Manuals for T2 tools

PC-lint Plus has been classified by Vector Informatik in terms of (worst case) tool criticality as a T2 tool.

4.1.4 Failure Mechanisms of Tools and Potential Mitigation Measures

Potential failure mechanisms that may affect the executable software must be identified for all T2 and T3 tools. Once such mechanisms are identified, appropriate mitigation measures must be taken. This analysis is the responsibility of the tool user.

Known tool defects, and their effects on tool output, are published in a user document (release notes). Certification customers have access to a defect list through Vector Informatik.

4.1.5 Evidence of tool conformance to its documentation

A suitable combination of validation testing and confidence in use is required for T3 tools. While Vector Informatik performs extensive validation testing on PC-lint Plus, there are no IEC 61508 requirements for full validation testing of a T2 tool.

4.1.6 Tool Compatibility

Since PC-lint Plus analyzes text files and is a standalone tool, tool compatibility requirements are not really applicable.

4.1.7 Modification Process

The modification process and supporting development lifecycle processes have been assessed to SIL 1 process requirements. While this is not required for IEC 61508 tool qualification, it is required to meet ISO 26262 modification requirements.

4.2 ISO 26262 Requirements

This section documents how PC-lint Plus meets the confidence in use of software tool requirements from ISO 26262.

4.2.1 General Requirement

The requirements from ISO26262 related to confidence in use of software tools apply to all tools where activities or tasks required by ISO 26262 rely on the correct functioning of such tools. PC-lint Plus meets the requirements from ISO 26262 related to confidence in use of software tools. Therefore, it can be relied upon to carry out or support activities or tasks required by ISO 26262.

4.2.2 Validity of Predetermined Tool Confidence Level or Qualification

This report documents the qualification of Vector Informatik's PC-lint Plus. As part of this qualification, a confirmation review by an independent organization (*exida*) was performed. This meets the I3 level of independence from ISO 26262-2 which meets the requirements of ASIL D.

4.2.3 Environmental and Functional Constraints and General Operating Conditions

As Vector Informatik's PC-lint Plus is applicable to the source code for standard C and C++, the environmental and functional constraints and general operating conditions are very easily met. The version of the tool assessed is documented in this report (see section 3.1) and as the modification process has been assessed and found to be adequate, successive versions are also deemed compliant as long as the certificate is appropriately maintained. Users are required to ensure the tool is appropriate, in the context of its use for a particular application.

4.2.4 Planning Usage of a Software Tool

The usage of a software tool must be planned and documented. The user of the tool is responsible for this requirement.

4.2.5 Required Information about the Tool

Required information about Vector Informatik's PC-lint Plus is documented in the User Manuals and in the release notes for a given release. The tool user is responsible for documenting any measures for the detection of malfunctions and erroneous output of the software tool identified during the determination of the required level of confidence for this software tool.

4.2.6 Description of Software Tool Usage

The description of the usage of Vector Informatik's PC-lint Plus is documented in the User Manuals.

4.2.7 Intended Tool Usage and Tool Confidence Level

The Tool Impact will vary based on how a tool is used. Likewise, the Tool error detection will vary based on the overall development process in which the tool is used. As a result, the tool user is responsible for determining both the Tool Impact (TI) and the Tool error Detection (TD) for each software tool being used in development of a product. Vector Informatik has classified PC-lint Plus, based on its (worst case) expected use, as TCL2 (TI2 + TD2).

4.2.8 Qualification of Software Tools

For a tool classified as TCL2, for ASIL D, method 1c (Validation of the Software Tool) is “highly recommended” and methods 1a (Increased Confidence from Use), 1b (Evaluation of the Development Process) and 1d (Development in accordance with safety standard) are “recommended”. However, the methods are given as alternatives, which mean that an appropriate combination of methods may be applied. Validation testing has been automated and, with a comprehensive set of scripts, provides very strong verification of the static analysis rules claimed to be supported by PC-lint Plus. All requirements of released features have been fully tested and only tests related to functionality intended for a future release are not run. While all requirements have been fully tested, confidence in use and evaluation of tool development (modification process) have been considered in the compliance argument as well. The combination of these methods demonstrates adequate support for ASIL D compliance of the tool requirements.

4.2.9 Documentation of Tool Qualification

The tool qualification is documented by this report, with the exceptions stated in this report. The pre-determined maximum ASIL, or specific ASIL, of any safety requirement which might be violated if the software tool malfunctions and produces corresponding erroneous output must be determined/documented by the tool user (e.g., with a Tool HAZOP analysis).

4.2.10 Validation of the Software Tool

Vector Informatik has a very extensive validation test suite to test the product against its functional requirements. Any test failures are documented per assessed modification procedures, by documenting a change request, impact analysis, etc. (see section 4.2.12).

4.2.11 Increased Confidence from Use

PC-lint and PC-lint Plus have been on the market since 1985. Vector Informatik’s PC-lint Plus has a 2-year history of use in the marketplace across many different applications and companies. Additionally, it was beta tested by about 100 entities for over 12 months prior to its initial release. Based on this data, confidence in use is judged to be fairly high.

4.2.12 Evaluation of the Tool Development Process

Development of PC-lint Plus is ongoing and is supported by an assessed modification process. Each modification (features and fixes) to the product is documented, including the results of an impact analysis and the results of following a documented lifecycle model that documents each phase of development (starting with the phase of development specified in the impact analysis), including inputs, outputs, activities, verification activities and verification outputs for each phase. The lifecycle for several of these changes has been assessed to ensure the procedures are followed for each change.

The Tool Development Process has been judged to be compliant with IEC 61508 SIL 1, which is judged to be sufficient to meet the “recommended” requirement for a development process compliant with a safety standard.



5. 2023 IEC 61508 Functional Safety Surveillance Audit

5.1 Roles of the Parties Involved

Vector Informatik

Manufacturer of the PC-lint Plus

exida

Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Vector Informatik contracted *exida* in December 2022 to perform the surveillance audit for the above PC-lint Plus. The surveillance audit was conducted remotely with the Vector Informatik's facility in PA, USA in January 2023.

5.2 Surveillance Methodology

As part of the IEC 61508 functional safety surveillance audit the following aspects have been reviewed:

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if any of the changes could affect the safety function of the PC-lint Plus.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the *exida* Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

5.2.1 Documentation provided by Vector Informatik

Doc. ID	Project Document Filename	Version	Date
D004	configuration_management.pdf	a7e8920	10/11/2022
D004b	configuration_auditing_report_form.pdf	a7e8920	10/11/2023



D010	documentation_change.pdf	a7e8920	10/11/2022
D016	customer_notification_procedure.pdf	a7e8920	10/11/2022
D023	project_plan.pdf	79b9524	10/11/2022
D049	arch.pdf	d638a27	10/7/2022
D054	carf-windows-pclp-2.0.pdf	4b14488c	11/18/2022
D060	coding_guidelines.pdf	4b14488	
D061	static_analysis.pdf	a7e8920	10/11/2022
D061b	policy.Int		11/11/2022
D069c	pf-req.html		snapshot
D069c	test_plan.pdf	a7e8920	10/11/2022
D074	step1-debug.txt		11/16/2022
D078	manual.pdf	Rev. 2.0	11/1/2022
D078b	pclp-1.4.1-manual.pdf	Rev. 1.4.1	4/1/2021
D078c	pclp-2.0-beta3-manual.pdf	v2.0 beta 3	9/16/2022
D079	pclp-sca.pdf	V2.0	2/7/2023
D081b	PCLP-2999.pdf		snapshot
D081c	PCLP-3486.pdf		snapshot
D081d	PCLP-3526.pdf		snapshot
D081e	1109.diff		10/29/2022
D093	aid-034.pdf		11/1/2022

5.2.2 Surveillance Documentation generated by *exida*

[R3]	VEC 22-10-029 CACL01 V1R0 Surveillance Audit Checklist - PC-lint Plus.xlsx	2023 Surveillance Audit Checklist
[R4]	VEC 18-11-045 V2R0 SC001 IEC 61508 Tool Cert - PC-lint Plus.xlsm	Safety Case WB

5.3 Surveillance Results

5.3.1 Procedure Changes

Changes to the procedure (D004, 004b, D010, D016, and D060) were reviewed and were found to be consistent with the requirements of IEC 61508.

5.3.2 Engineering Changes

Engineering changes were properly documented and associated with impact analyses.

5.3.3 Impact Analysis

The impact analyses of 3 of the many changes (D081b, D081c, and D081d) were reviewed in detail to ensure that the modification process is used to document the impact of identified issues on functional safety, root cause analysis of any problems found, impacts of the modification on functional safety, verifications performed, validations performed and changes to user documentation. The impact analyses of the other changes were also reviewed to a lesser extent.

5.3.4 Field History

All reported field errors were logged as issues, reviewed, dispositioned, and corrected per the modification process described in the project plan.

5.3.5 Safety Manual

Updates to the safety manual, that occurred during the certification period, were reviewed and found to be compliant with IEC 61508:2010.

5.3.6 FMEDA Update

This software tool does not require this analysis.

5.3.7 Evaluate use of certificate and/or certification mark

The Vector Informatik website was searched and no misleading use or misuse of the certification, or certification marks, was found.

5.3.8 Previous Recommendations

Previous recommendations for improvement were reviewed and were resolved satisfactorily to the requirements of IEC 61508.

5.4 Surveillance Audit Conclusion

The result of the Surveillance Audit Assessment can be summarized by the following observations:

The Vector Informatik PC-lint Plus continues to meet the relevant requirements of IEC 61508:2010 for use with application development up to SIL 4 and ASIL D based on the initial assessment and considering:

- field failure history
- permitted modifications completed on the product
- resolution of past action items
- changes to the safety manual

This conclusion is supported by the updated Safety Case and certification documents.

6. Terms and Definitions

ASIL	Automotive Safety Integrity Level
MISRA	Motor Industry Software Reliability Association
SIL	Safety Integrity Level
TCL	Tool Criticality Level

7. Status of the document

7.1 Liability

exida prepares reports based on methods advocated in international standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q18/11-045	VEC 18-11-045 R001 V2R2	Errors and omissions; DEB – February 9, 2023
Q18/11-045	VEC 18-11-045 R001 V2R1	Errors and omissions; DEB – February 8, 2023
Q18/11-045	VEC 18-11-045 R001 V2R0	Surveillance Audit; DEB – January 31, 2023
Q18/11-045	GIM 18-11-045 R001 V1R3	Error correction; DEB - April 17, 2020
Q18/11-045	GIM 18-11-045 R001 V1R2	Error correction; November 21, 2019
Q18/11-045	GIM 18-11-045 R001 V1R1	Errors and omissions correction; November 20, 2019
Q18/11-045	GIM 18-11-045 R001 V1R0	Initial version; October 31, 2019

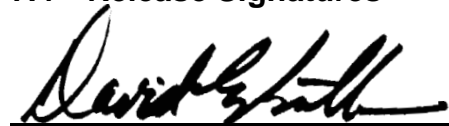
Review: V2, R0: Jonathan Moore; January 30, 2023

Status: Released, 1/31/2023

7.3 Future Enhancements

Future enhancements prepared at the request of the client.

7.4 Release Signatures



David Butler, CFSE, Senior Safety Engineer



EUR-ING Jonathan Moore, C.Eng., CFSE, Director Advanced Systems