

IEC Certification Kit 1.4

for IEC 61508 and ISO 26262

Certify embedded systems developed using Simulink and Polyspace products to IEC 61508 and ISO 26262

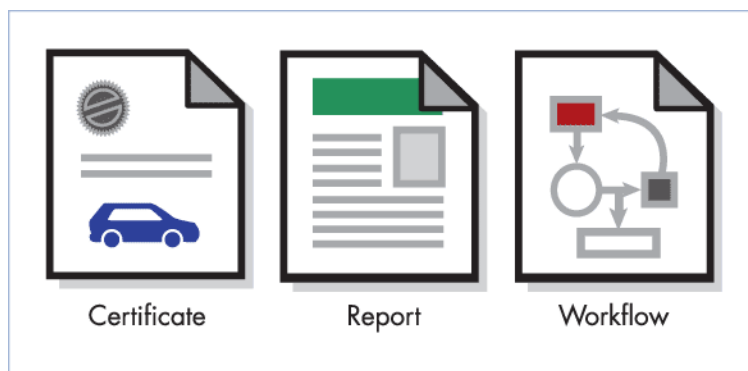
Introduction

IEC Certification Kit provides documentation, certificates, and templates that help you use Embedded Coder™ or Polyspace® code verification products for projects based on the IEC 61508 and ISO 26262 standards. The kit includes certificates and reports from certification authority TÜV SÜD that are based on documented, application-specific verification workflows. With the kit, you can streamline certification of your embedded systems developed using Simulink® or Polyspace products.

Specific versions of Embedded Coder and Polyspace Verifier for C, which includes the MISRA-C:2004 code analyzer, have been certified by TÜV SÜD for use with the IEC 61508 standard. For each certified version of these products, the kit contains certificates, reports, and additional materials necessary to document compliance with the standard. You can modify these artifacts as needed for your project and submit them to your certification authority as evidence of product or application compliance with IEC 61508-3 and ISO/DIS 26262-8.

Key Features

- TÜV SÜD certificates and reports for Embedded Coder
- TÜV SÜD certificates and reports for Polyspace code verifiers
- TÜV SÜD certificates and reports for Simulink PLC Coder™
- Application-specific verification workflow documents for Simulink and Polyspace products
- Customizable templates for delivering documentation to certification authorities



IEC Certification Kit contents, including certification artifacts and workflow guidance for projects using Model-Based Design or Polyspace code verification.

What is IEC 61508?

IEC 61508 is the international, industry-independent safety standard entitled "Functional safety of electrical/electronic/programmable electronic safety-related systems." The seven-part standard spans IEC 61508-1 to IEC 61508-7. IEC 61508-3 is concerned with software development, verification, and validation; it highly recommends certified tools and translators for safety integrity levels of SIL 2 and higher.

IEC 61508 certification confirms that a product or system complies with objectives set by the standard. Successful IEC 61508 certification yields a certificate and, if applicable, an associated technical report.

Working with IEC Certification Kit

IEC Certification Kit follows an in-context approach to IEC 61508 certification that is based on a specific workflow or set of workflows used when the applicant applies specific tools to develop or verify software for IEC 61508-compliant or IEC 61508-certified applications. The applicant must ensure that the tools are used within the referenced workflows and within the constraints specified in their respective certificates.

To use the IEC Certification Kit product, follow these steps:

1. Decide whether you will pursue a self-certification or an external certification.
2. Document compliance with relevant IEC 61508 requirements.
3. Propose initial certification package to certification authorities.
4. Provide completed certification package to certification authorities.

Although IEC Certification Kit provides guidance and information for all of the above steps, its main goal is to help you achieve step 4 with MathWorks tools. To that end, IEC Certification Kit includes the artifacts, templates, and documentation for MathWorks tools, as noted in the accompanying tables.

Kit Contents for Supported MathWorks Products

Embedded Coder

Purpose	IEC 61508-3 Reference	Documents and Artifacts
Evidence for using certified translators	Measure/Technique 5a, "Certificated Translator," in Table A-3, in Clause 7.4.4.3a	<ul style="list-style-type: none"> ▪ Certificate for Embedded Coder ▪ Certificate Report for Embedded Coder
Evidence for IEC 61508-3-compliant verification and validation of models and generated code	Applicable requirements of overall software safety life cycle that relate to verification and validation of models and generated code	<ul style="list-style-type: none"> ▪ Workflow documentation describing the verification and validation of models and generated code ▪ Tailored and completed Conformance Demonstration Template

Polyspace Verifier for C

Purpose	IEC 61508-3 Reference	Documents and Artifacts
Evidence for using certified tools	Measure/Technique 4a, "Certificated Tool," in Table A-3, in Clause 7.4.4.3a	<ul style="list-style-type: none"> ▪ Certificate for Polyspace Verifier for C ▪ Certificate Report for Polyspace Verifier for C
Evidence for IEC 61508-3-compliant verification of C code	Applicable requirements of overall software safety life cycle that relate to static code inspection against formal criteria and software quality assurance	Workflow documentation describing the verification of C code using Polyspace products

Note: Embedded Coder and Polyspace code verifiers were not developed using an IEC 61508-compliant process. Using certified tools does not ensure the safety of the software or the system under consideration.

Resources

Product Details, Demos, and System Requirements

www.mathworks.com/products/iec-61508

Trial Software

www.mathworks.com/trialrequest

Sales

www.mathworks.com/contactsales

Technical Support

www.mathworks.com/support

Online User Community

www.mathworks.com/matlabcentral

Training Services

www.mathworks.com/training

Third-Party Products and Services

www.mathworks.com/connections

Worldwide Contacts

www.mathworks.com/contact