

Coverity Support for ISO/IEC TS 17961

Fully ensure the safety,
reliability, and security
of software written in C

Overview

The technical specification ISO/IEC TS 17961 is a set of well-documented and well-enforced coding rules for the C programming language. It is an important milestone in introducing best practices for ensuring the safety, reliability, security, and integrity of software written in C. Notably, the specification is designed to be enforceable by software code analyzers using static analysis techniques. This greatly reduces the cost of compliance by way of automation.

Adhering to coding standards is a crucial step in establishing best coding practices. Standards adherence is particularly important in safety-critical, high-impact industries, such as automotive, medical, and networking. Software defects in products coming from these industries manifest themselves physically and tangibly—often with life-threatening consequences.

Synopsys provides a comprehensive solution that checks for all secure coding rules specified in the ISO/IEC TS 17961 standard.

ISO/IEC TS 17961

ISO/IEC TS 17961 is defined by two publications from the International Organization for Standardization:

- ISO/IEC TS 17961:2013: Information technology—Programming languages, their environments and system software interfaces—C secure coding rules (<https://www.iso.org/standard/61134.html>)
- ISO/IEC TS 17961:2013/Cor 1:2016: Information technology—Programming languages, their environments and system software interfaces—C secure coding rules, Technical Corrigendum 1 (<https://www.iso.org/standard/72086.html>)

The technical specification defines secure coding rules for C. These rules are designed to provide a check against programming flaws that lead to vulnerabilities, regardless of whether the code is deployed in a security-critical environment.

The specification is focused on security vulnerabilities. Some rules pertain to data taint analysis: tracing data propagation from sources to sinks. Tainted data should be sanitized before being used. Coverity by Synopsys, with its state-of-the-art dataflow analysis techniques, can accurately identify such vulnerabilities in source code.

