ICS 35.080
L 77

中华人民共和国国家标准

GB/T 37691—2019

可编程逻辑器件软件安全性设计指南

Guide for programmable logic device software safety design

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:中国航天科工集团公司第三研究院第三〇四研究所、中国电子技术标准化研究院、中国电子科技集团第三十研究所、国家卫星海洋应用中心。

本标准主要起草人:孟伟、杨楠、王黎、姜晓辉、胡勇、黄琼、王国锋、张津荣、李文鹏、朱琳、张国宇、肖崇俭、寇科男、李恺、巫忠跃、彭鸣、毛伟、许卓琦、张旸旸、陈元、史玥、陈鹏、刘廷、杨永生、王希、孙健、葛永娇。

可编程逻辑器件软件安全性设计指南

1 范围

本标准给出了可编程逻辑器件软件安全性设计的指导和建议，并给出了需考虑要点有关的信息。

本标准适用于可编程逻辑器件软件的系统需求分析、软件需求分析、设计和实现时的安全性设计。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 11457—2006 信息技术 软件工程术语

GB/T 18349 集成电路/计算机硬件描述语言 Verilog

GB/T 33781—2017 可编程逻辑器件软件开发通用要求

GB/T 33783—2017 可编程逻辑器件软件测试指南

3 术语和定义

GB/T 11457—2006、GB/T 33781—2017 和 GB/T 33783—2017 界定的以及下列术语和定义适用于本文件。

3.1

可编程逻辑器件 programmable logic device

允许用户编程(配置)实现所需逻辑功能的器件。

[GB/T 33781—2017，定义 3.1.1]

3.2

可编程逻辑器件软件 programmable logic device software

针对 FPGA、CPLD 等可编程逻辑器件进行设计而产生的程序、文档和数据。

[GB/T 33781—2017，定义 3.1.5]

3.3

软件安全性 software safety

软件运行不引起系统事故的能力。

3.4

软件失效 software failure

软件系统丧失完成规定功能能力的事件。

3.5

安全关键功能 safety critical function

针对特定的危险事件，为达到或保持受控设备的安全状态而实现的功能。

3.6

安全关键可编程逻辑器件软件 safety critical programmable logic device software

具有安全关键功能的可编程逻辑器件软件。