CETC 中国电科

锐华TM高安全嵌入式操作系统之路
ReWorks Cert

自主可控 Self-controllability

安全可信 Safety and trusted

军民融合 Military-civilian integration

创新发展 Innovation

2019国产嵌入式操作系统技术与产业发展论坛

嵌入式系统联谊会 www.esbf.org

中国电子科技集团公司第三十二研究所
上海华元创信软件有限公司

01

PART

背景材料

锐华产品发布 Release of ReWorks products

2012

针对国产化平台发布锐华ReWorks/ReDe V4.7；

ReWorks/ReDe V4.7 is released for the localization platform;

2013

针对多核并行处理平台发布锐华ReWorks/ReDe V5.0；

ReWorks/ReDe V5.0 is released for multi-core parallel processing platform;

2014

发布SCA软件平台ReSCA V3.0；

SCA software platform ReSCA V3.0 is released;

2015

发布锐华DSP ReWorks V1.0；

DSP ReWorks V1.0 is released;

2016

发布锐华移动操作系统ReMo V1.0；

ReWorks mobile operating system ReMo V1.0 is released;

2017

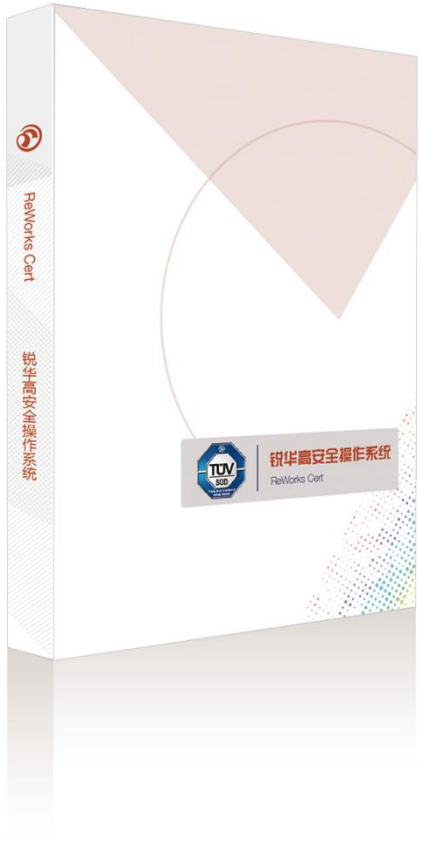
发布锐华移动操作系统ReMo V2.0；
发布SCA软件平台ReSCA V4.0；
针对64位和多核异构处理平台发布锐华ReWorks/ReDe V6.0；

ReWorks mobile operating system ReMo V2.0 is released;
SCA software platform ReSCA V4.0 is released;
ReWorks/ReDe V6.0 is released for 64-bit and multi-core heterogeneous processing platforms;

2018

发布锐华高安全嵌入式实时操作系统ReWorks Cert V1.0；

Safety embedded real-time operating system ReWorks Cert V1.0 is released .



锐华高安全操作系统

ReWorks Cert

CETC 中国电科

02

PART

产品背景

Background

安全关键系统已成为关系国计民生的重要基础设施，
一旦发生故障，将严重危害到人民生命和财产安全！

Safety-related systems have become a significant infrastructure for the national economy and the people's livelihood.
Once a failure occurs, it will seriously endanger the lives and property of people!

航空航天
Aerospace

医疗领域
Medical

核电控制
Nuclear Power

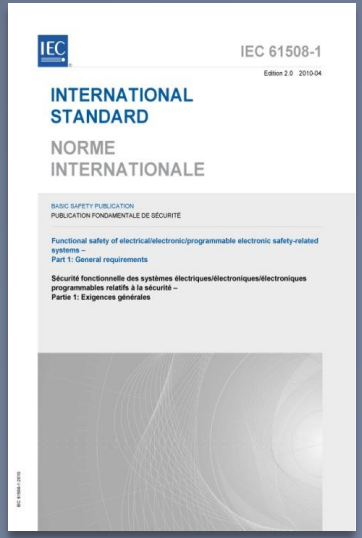
轨道交通
Railway

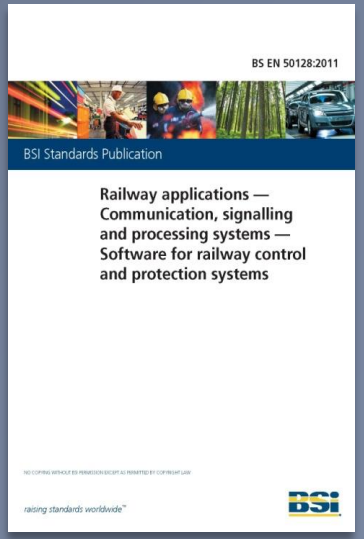
工业控制
Industrial control

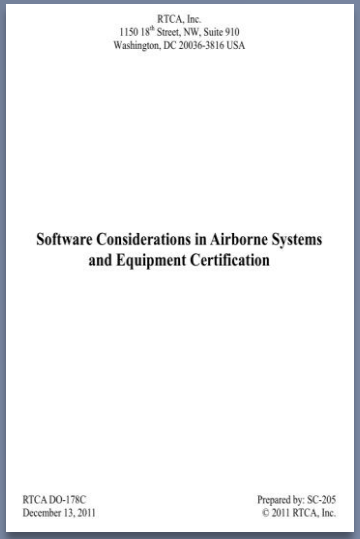
汽车电子
Automobile

安全关键领域要求其应用的系统和软件必须具有高安全的特征，必须符合功能安全标准的要求 (如IEC 61508, EN 5012X, DO-178B/C), 必须通过第三方认证公司的认证

Safety-related systems and software are required to meet the requirements of functional safety standards (such as IEC 61508, EN 5012X, DO-178B/C), and to be certified by a third-party certification company

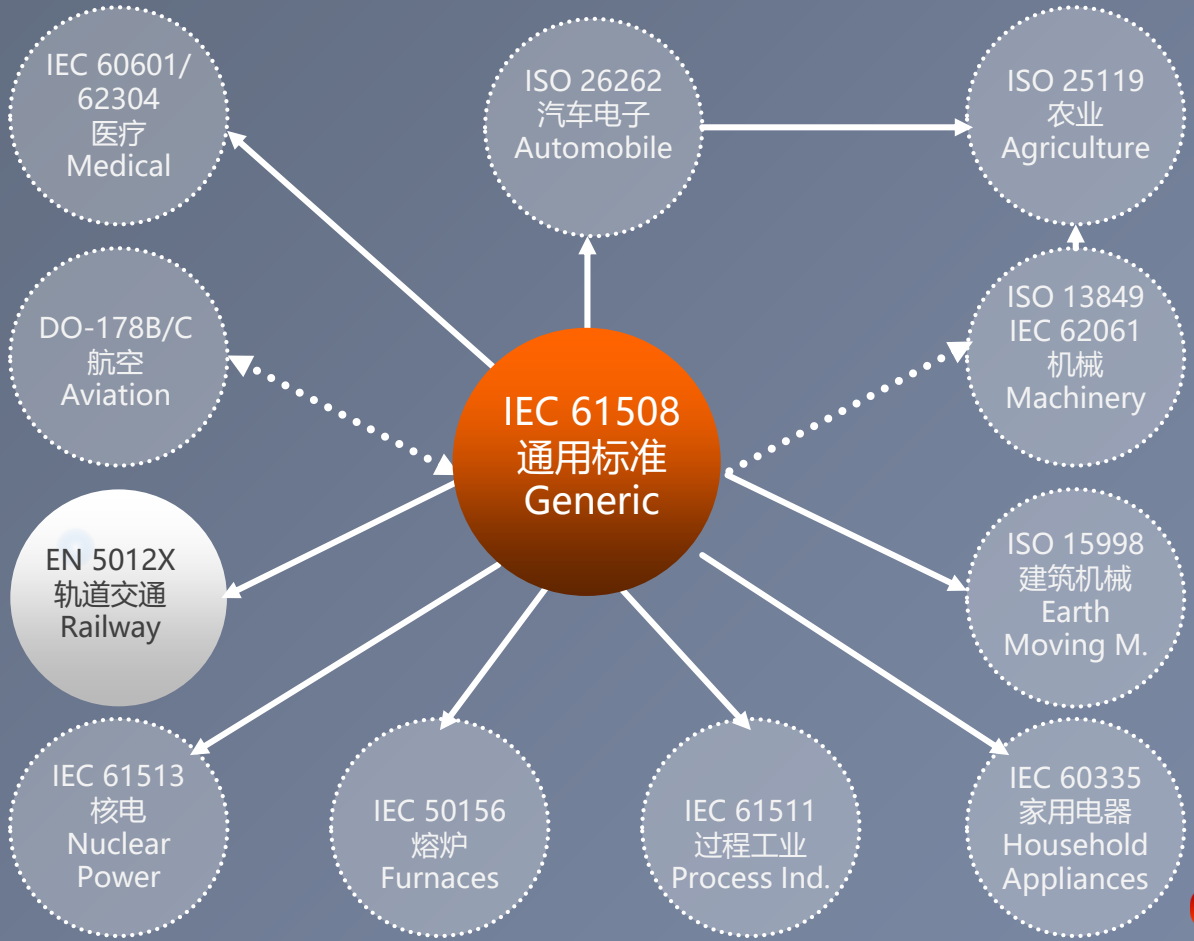






CETC 中国电科

功能安全标准的关系 Relations between functional safety standards



CETC 中国电科

提升系统安全性

Improve safety

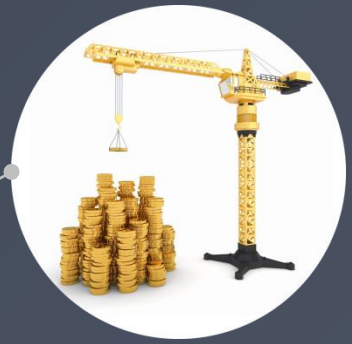
避免不可接受的风险

Avoid unacceptable risks

加速认证周期，降低系统认证成本

Accelerate certification cycles

reduce system certification costs



CETC 中国电科

03

PART

产品特征

Features

专业认证 Safety Certification

满足功能安全标准IEC 61508 SIL/SC3（通用）和EN 50128 SW SIL4（轨道交通）

Compliant with the functional safety standards IEC 61508 SIL/SC3(Generic)和EN 50128 SW SIL4(Railway)

满足上述标准的操作系统最高安全等级

the highest safety integrity level for operating systems that comply with IEC 61508 and EN 50128

国内目前唯一一个

通过国际第三方认证公司认证的嵌入式实时操作系统

The only single domestic embedded real-time operating system, which is certified by an international third-party certification company.

CERTIFICATE

No. Z10 101062 0001 Rev. 00

Holder of Certificate: East China Institute of Computing Technology (The 32nd Research Institute of China Electronics Technology Group Corporation)
No. 1485, Jialuo Road
Jiading District
201801 Shanghai
PEOPLE'S REPUBLIC OF CHINA

Factory(ies): 101062

Certification Mark:

Product: Software, Operating Systems
Real Time Operating System

Model(s): ReWorks Cert

Parameters: Safety Parameters: SIL 3 IEC 61508-3
SIL 4 EN 50128

The report referenced below and the user documentation in the currently valid revision are mandatory part of this certificate.

Tested according to: EN 50128:2011
IEC 61508-1:2010
IEC 61508-3:2010
IEC 61508-4:2010

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: CS92714C
Valid until: 2023-08-05

Date, 2018-08-06 (Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

证书

编号 Z10 101062 0001 Rev.00

证书持有人： 华东计算技术研究所（中国电子科技集团公司第三十二研究所）
中国上海市嘉定区嘉罗路 1485 号

工厂编号： 101062

认证标识：

产品： 软件，操作系统
实时操作系统

型号： 锐华认证版

参数： 安全参数: SIL 3 IEC 61508-3
SIL 4 EN 50128

下面引用的报告和当前有效版本的用户文档都是该证书的必要部分

评估标准： EN 50128:2011
IEC 61508-1:2010
IEC 61508-3:2010
IEC 61508-4:2010

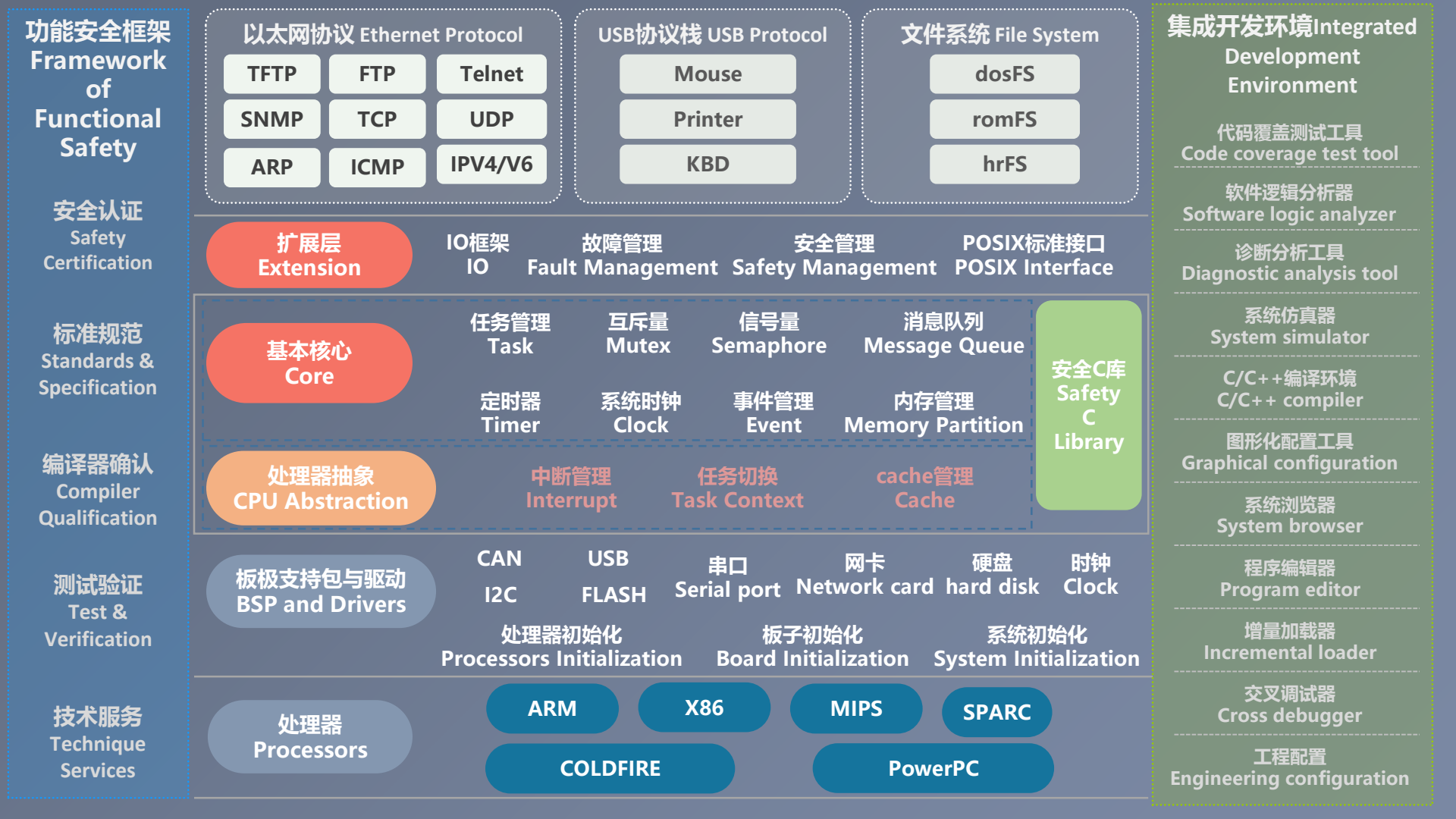
本产品的评估基于自愿申请原则，并且遵照必要规范。上述所示认证标识可贴附于认证的产品上，但不允许以任何方式改变此认证标识。此外，证书持有人不应该转移此证书到第三方。相关须知请参考证书背面内容。

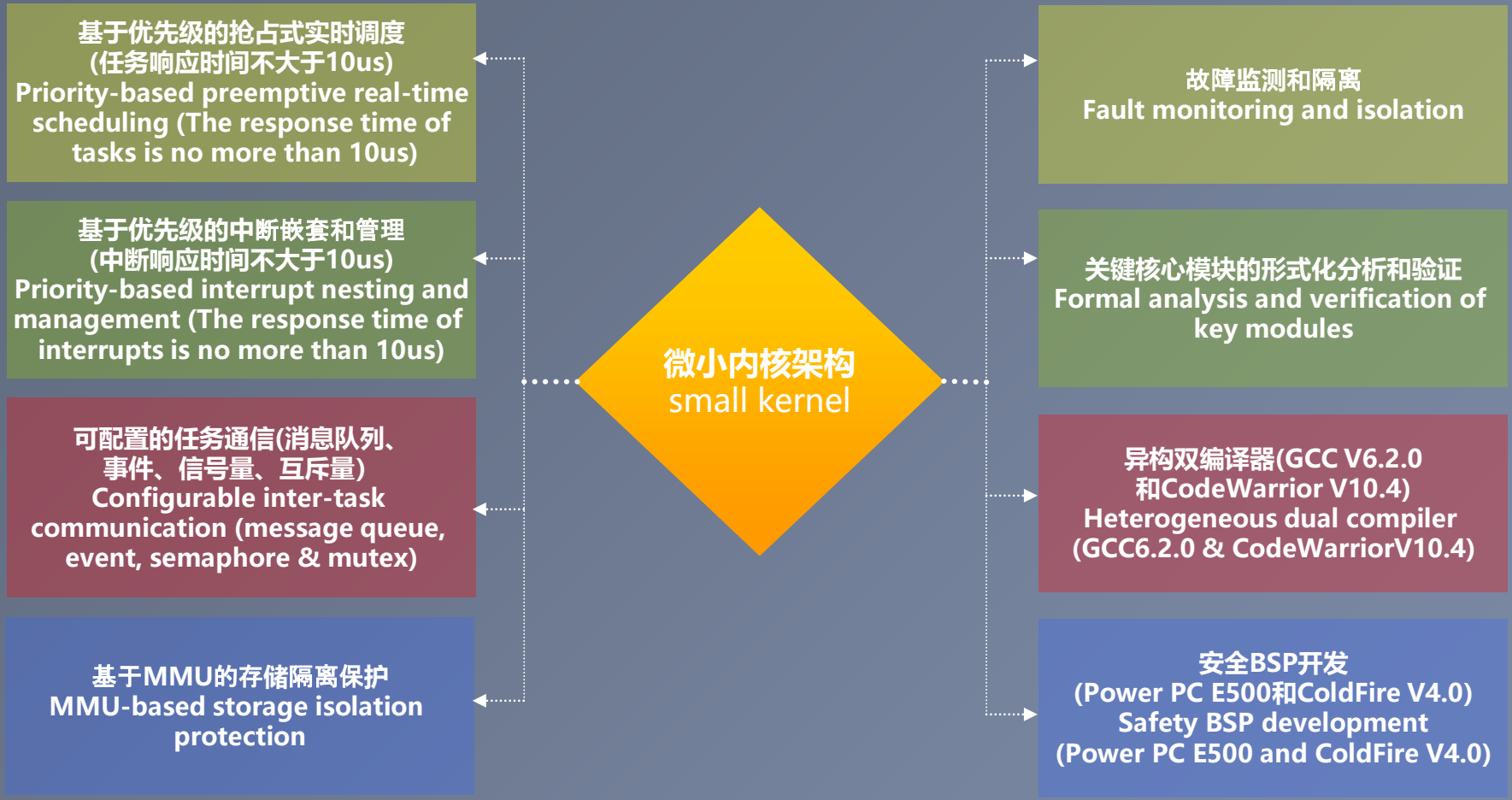
评估报告编号： CS92714C
有效期至： 2023-08-05

签发日期：2018-08-06 (Christian Dirmeier)

第 1 页 共 1 页
This is a translation of the English original certificate. In case of issues, only the original certificate is binding.

ZERTIFIKAT • CERTIFICATE • CERTIFICADO • СЕРТИФИКАТ • CERTIFICAT


功能安全框架
Framework of Functional Safety
安全认证
Safety Certification
标准规范
Standards & Specification
编译器确认
Compiler Qualification
测试验证
Test & Verification
技术服务
Technique Services
以太网协议 Ethernet Protocol
TFTP
FTP
Telnet
SNMP
TCP
UDP
ARP
ICMP
IPV4/V6
USB协议栈 USB Protocol
Mouse
Printer
KBD
文件系统 File System
dosFS
romFS
hrFS
扩展层
Extension
IO框架
IO
故障管理
Fault Management
安全管理
Safety Management
POSIX标准接口
POSIX Interface
基本核心
Core
任务管理
Task
互斥量
Mutex
信号量
Semaphore
消息队列
Message Queue
定时器
Timer
系统时钟
Clock
事件管理
Event
内存管理
Memory Partition
安全C库
Safety C Library
处理器抽象
CPU Abstraction
中断管理
Interrupt
任务切换
Task Context
cache管理
Cache
板极支持包与驱动
BSP and Drivers
CAN
I2C
USB
FLASH
串口
Serial port
网卡
Network card
硬盘
hard disk
时钟
Clock
处理器初始化
Processors Initialization
板子初始化
Board Initialization
系统初始化
System Initialization
处理器
Processors
ARM
X86
MIPS
SPARC
COLDFIRE
PowerPC
集成开发环境Integrated Development Environment
代码覆盖测试工具
Code coverage test tool
软件逻辑分析器
Software logic analyzer
诊断分析工具
Diagnostic analysis tool
系统仿真器
System simulator
C/C++编译环境
C/C++ compiler
图形化配置工具
Graphical configuration
系统浏览器
System browser
程序编辑器
Program editor
增量加载器
Incremental loader
交叉调试器
Cross debugger
工程配置
Engineering configuration

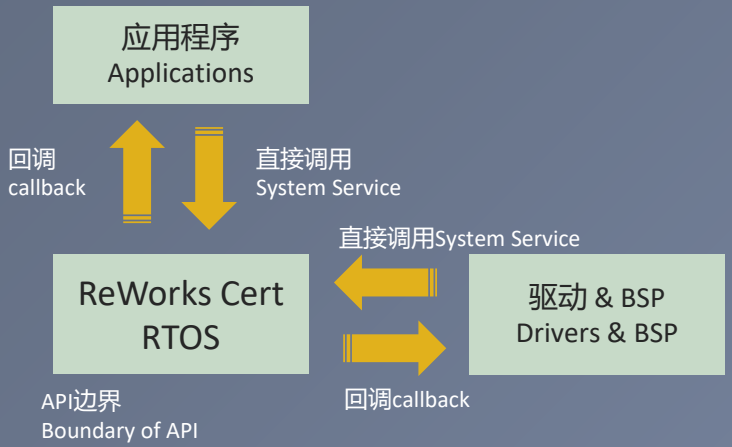

基于优先级的抢占式实时调度
(任务响应时间不大于10us)
Priority-based preemptive real-time scheduling (The response time of tasks is no more than 10us)
基于优先级的中断嵌套和管理
(中断响应时间不大于10us)
Priority-based interrupt nesting and management (The response time of interrupts is no more than 10us)
可配置的任务通信(消息队列、事件、信号量、互斥量)
Configurable inter-task communication (message queue, event, semaphore & mutex)
基于MMU的存储隔离保护
MMU-based storage isolation protection
微小内核架构
small kernel
故障监测和隔离
Fault monitoring and isolation
关键核心模块的形式化分析和验证
Formal analysis and verification of key modules
异构双编译器(GCC V6.2.0和CodeWarrior V10.4)
Heterogeneous dual compiler (GCC6.2.0 & CodeWarriorV10.4)
安全BSP开发
(Power PC E500和ColdFire V4.0)
Safety BSP development
(Power PC E500 and ColdFire V4.0)

高安全特征 Safety Design

失效防护设计
the fail-safe design strategy

确认安全边界，采用软件FMEA方法识别失效模式并提供风险缓解措施

confirming the safety boundary & identifying the failure mode and deriving the risk mitigation measures

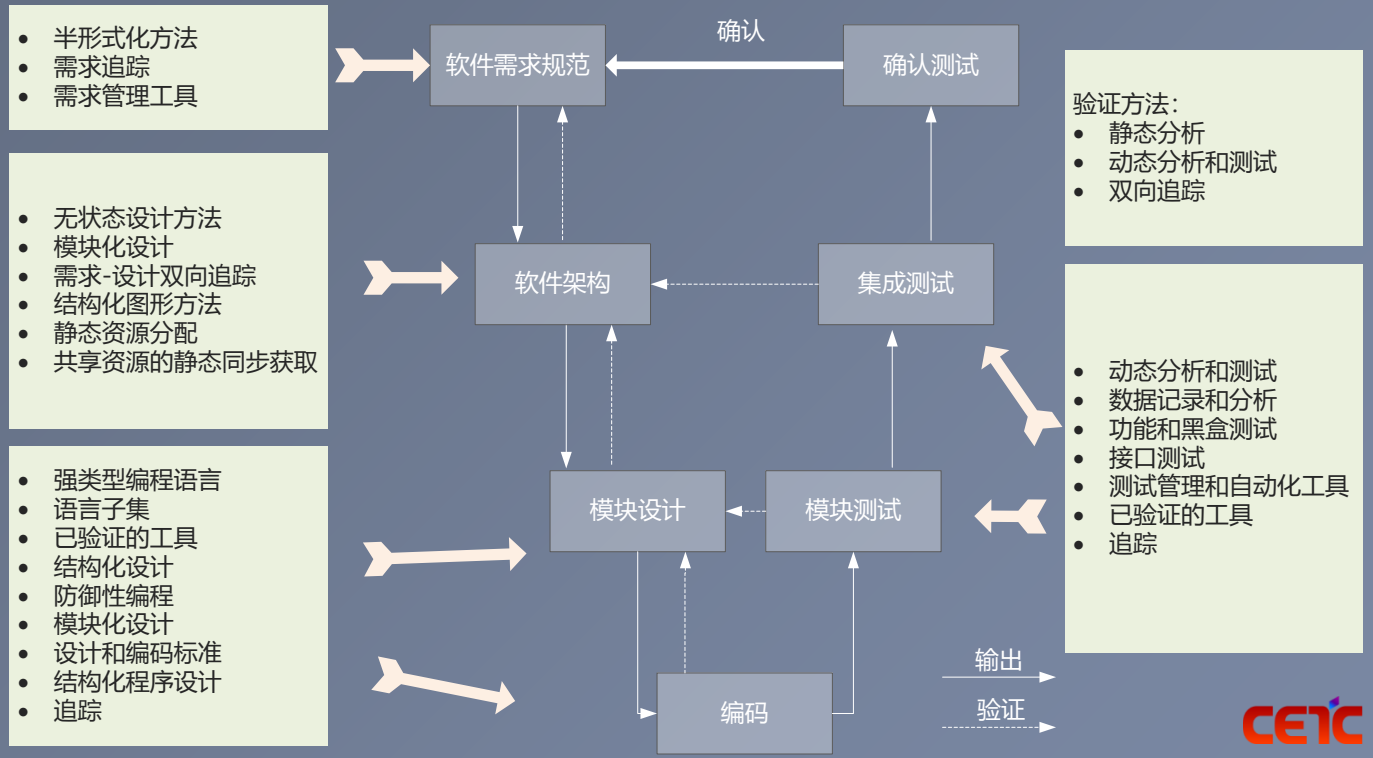


Items	ID	Failure Modes	Failure Effect	Mitigation Measures	Status
Task	SVA-106	Task fails during initialization, activation or operation.	It generally has some side effect on the normal use of RTOS and some task errors even cause unpredictable behaviors of RTOS.	Some task errors are detected by RTOS through API calls and returned as error responses to applications. Other task errors that cannot be detected by RTOS will lead to an exception. RTOS offers a default exception handler, which calls a fatal error hook handler function. If applications intend to employ this handler, they should connect the default exception handler to the exception vectors and modify the fatal error hook code to meet their actual needs. Applications also can define their specific exception routines. They should connect the specific handler to the exception vectors and guarantee all the exception vectors are attached by handlers.	Closed/ User Issue
Memory	SVA-113	A memory partition is created when dynamic allocation of resources is forbidden	It will lead to the overflow of resources and/or undefined behaviors of RTOS.	It is forbidden to create memory partitions when dynamic allocation of resources is prohibited. If memory partitions are created in this situation, RTOS will return an error number to applications.	Closed

CETC 中国电科

安全设计的方式方法 Safety Design Methods

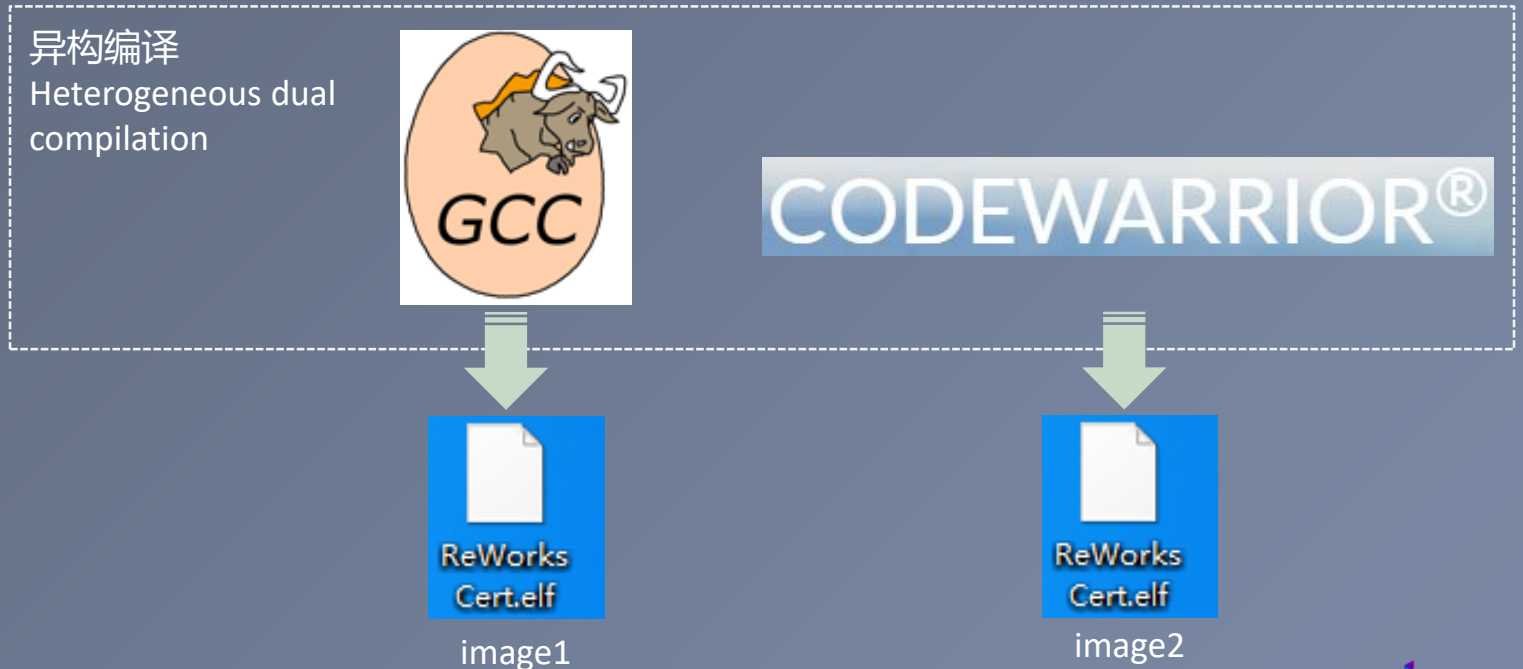
- 半形式化方法（状态图、UML方法） Semi-formal methods (state diagrams, UML)
- 静态分析（编码规范的符合性、程序复杂度分析等） Static analysis (code specification compliance, program complexity analysis)
- 防御性设计方法，MC/DC覆盖率达到100%、自动化工具等 Defensive design methods, MC/DC coverage analysis, automation tools



CETC 中国电科

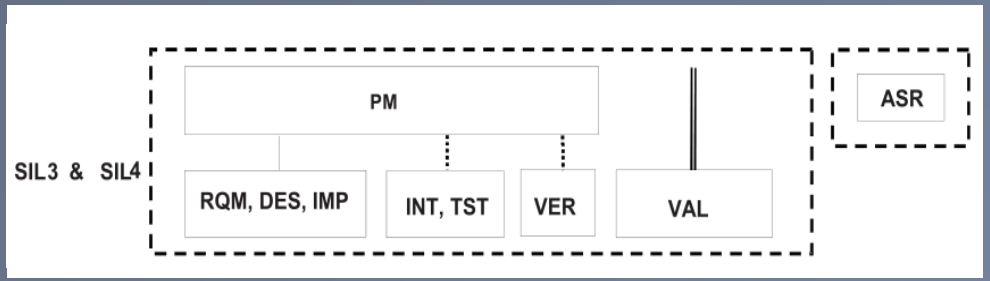
编译器正确性确认 Qualification of Compilers

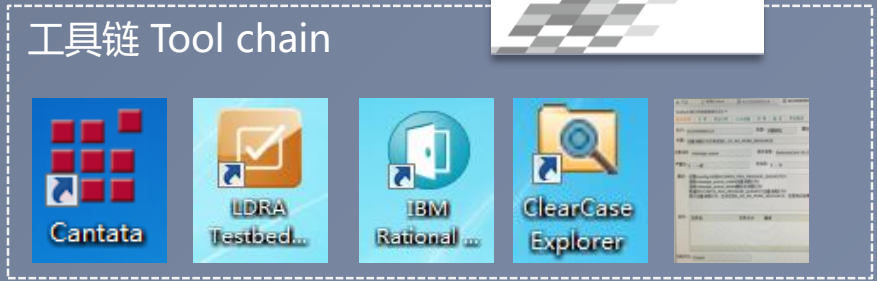
- 异构双编译器: GCC 6.2.0和Code Warrior V10.4 Heterogeneous dual compilers GCC 6.2.0 and Code Warrior V10.4
- 编译器的正确性经过验证，符合IEC 61508和EN 50128标准中T3类工具的要求 The correctness of the compilers is qualified according to the requirements of T3 tools in functional safety standards.



流程和安全保障体系 Process management and safety assurance systems

- 使用需求、设计和编码规范
  Requirements, design and coding standards
- 实施安全准则并建立需求、设计和测试的双向追踪
  Safety guidelines and bi-traceability between requirements, design and testing
- 人员独立性 Independence between roles
- 构建符合功能安全应用开发所需的工具链
  An integrated tool chain for functional safety

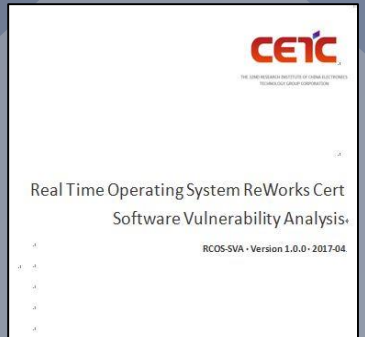


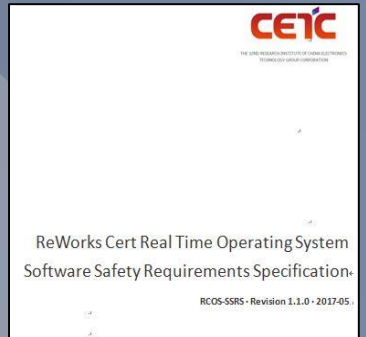


CETC 中国电科

完整的认证证据包 Complete certification evidence package

- ReWorks Cert Software Development Plan
- ReWorks Cert Software Safety Plan（安全计划）
- ReWorks Cert Software Verification &Validation Plan
- ReWorks Cert Software Quality Assurance Plan
- ReWorks Cert Software Configuration Management Plan
- ReWorks Cert Software Vulnerability Analysis（脆弱性分析）
- ReWorks Cert Software Safety Requirements Specification（安全需求规范）
- ReWorks Cert Overall Software Test Specification/Report
- ReWorks Cert Software Architecture Design Specification
- ReWorks Cert Software Integration Test Specification/Report
- ReWorks Cert Software Detailed Design Specification
- ReWorks Cert Software Unit Test Specification / Report
- ReWorks Cert Software Validation Report
- ReWorks Cert Safety Manual（安全手册）
  - ReWorks Cert Traceability Matrix
  - Release Notes
  - Verification Report for each phase
  - Code和documents
- Tool Validation Report（编译器确认报告）
  - GCC和CodeWarrior
- Code
  - Source Code
  - Overall Test Code
  - ReWorks Cert Software Integration Test Code
  - ReWorks Cert Software Unit Test Code





CETC 中国电科

04

PART

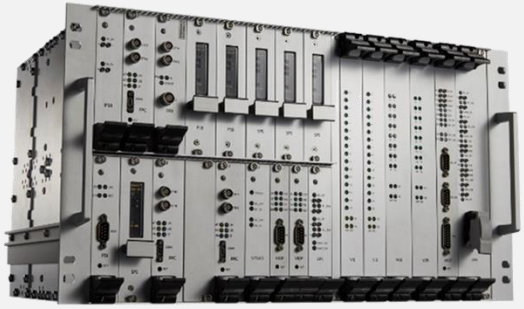
产品应用

Application

轨道交通领域的应用 Application in Railway

卡斯柯 CASCO

- 列车控制系统 CC
- 计算机联锁系统 CBI
- 区域控制器 ZC
- 列控中心系统 CC
- 无线闭塞中心系统 RBC
- 临时限速服务系统 TSRS
- 线路控制器 LC



VCU安全计算机平台 VCU Safety Computer Platform

✓2*2取2冗余架构 2 from 2*2 redundant architecture

✓多级BIT自检 Multi-level BIT Test

✓多模冗余异构操作系统境像
Multi-mode Redundant Heterogeneous RTOS

Certificate of Conformity

Generic Product Vital Control Unit (VCU) System

Certificate No. 1370/5/ISP/18/CCS/EN/539

Certification Body	BUREAU VERITAS ITALIA Notified Body N° 1370 Directive 2008/57/CE Via Paolo Imperiale 4, 16126 Genova – Italia.
Owner of Certificate	CASCO Signal Ltd. 27(C/D), Triumphal Arch building, No. 428 Tian Mu Zhong Road, Shanghai, 200070 P.R.China
Product Identification	Vital Control Unit (VCU) System version "VCU_Bproduct_V1.0.0"
Manufacturer	CASCO Signal Ltd. 27(C/D), Triumphal Arch building, No. 428 Tian Mu Zhong Road, Shanghai, 200070 P.R.China
Bases of Assessment	EN50126:1999, EN50128:2011, EN50129:2003 Safety Integrity Level up to 4 according to EN50129:2003.
Assessment Report 1)	BVC.VCUCV/OR246/17 AS02, rev.1.0 issued on September 27th, 2018 – "Final Safety Assessment Report of the Generic Product VCU".
Assessment results 2)	The Assessor confirms that the manufacturer has supplied technical evidence that: • The Development, Quality, Safety, Verification, Validation and Manufacturing activities planned and performed by CASCO for the VCU Generic Product are adequate to fulfil the requirements of the CENELEC standards EN50126:1999, EN50128:2011, EN50129:2003, - applicable to Railway Signalling System characterised by a Safety Integrity Level up to 4 (SIL4). The VCU generic product fulfils the system requirements specified in the "VCU System Requirement Specification", ref: VCU/2002/ v 1.5.0). The Safety Related Application Conditions defined in the "Vital Control Unit Platform Safety Related Application Conditions" (ref: RA16009/4513/v 1.1.0) shall be taken into account.
Validity	The Certificate is valid starting from its date of issue, and it is valid for the configuration as referred in the "Generic Product VCU System Safety Case" (ref. VCU/4516/v 1.1.0).

1) The Assessment Report is an integral part of the certificate
2) The Assessment results are provided in detail in the referred Assessment Report

Date of Issue 27th September 2018

Signature:

Name: Tommaso Ghiara Title: General Manager Rail

On behalf of BUREAU VERITAS ITALIA, NoBo N° 1370, Via Paolo Imperiale, 4 – 16126 Genoa – Italy (I)

ACCREDIA

PRD N° 0098 - ISP N° 006E

BUREAU VERITAS

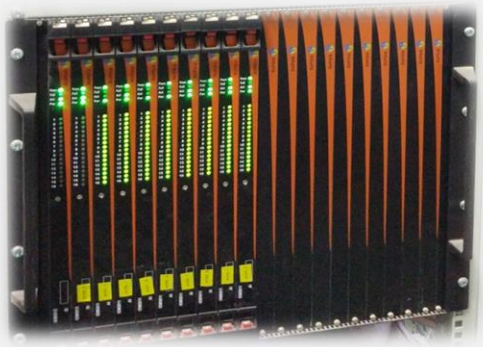
Bureau Veritas Italia S.p.A.
Head Office, via P. Imperiale 4, 16126 – Genoa (IT)
Legal Head Office, viale Monza 347, 20126 – Milan (IT)
www.bureauveritas.it

目前ReWorks Cert已率先成功应用于轨道交通信号领域龙头公司**卡斯柯信号有限公司**的安全计算机平台中，该计算机平台已成功通过EN 50126 SIL4等级认证。ReWorks Cert有望在城市轨道交通领域首先获得规模化。

ReWorks Cert has been successfully adopted in the EN 50126 SIL4-certified safety computer platform in CASCO in the field of railway. It is expected to achieve large-scale production in the urban rail transit .

工业控制领域的应用 Application in Industrial Control

- 汽轮机保护系统 Turbine Protection System
- 炉膛保护系统 Furnace Protection System
- 反应堆保护系统 Reactor Protection System



安全控制系统 Safety Control System

- ✓ 3取2冗余架构　2 from 3 redundant architecture
- ✓ 多级BIT自检　Multi-level BIT Test

正在应用于**上海自动化仪表股份有限公司**的IEC 61508 SIL3级功能安全控制DCS系统中（三取二架构）。
ReWorks Cert also has been applied to the IEC 61508 SIL3 functional safety control system (take two from three architecture) in the Shanghai Automation Instrument Co., Ltd.

05

PART

专业服务

Professional Service

锐华嵌入式基础软件产品体系
Product Series of ReWorks

锐华嵌入式实时操作系统
ReWorks Real-time ReWorks

强实时
Strong real-time

锐华DSP操作系统
ReWorks DSP

为多核DSP芯片提供国产基础软件解决方案
Domestic fundamental software solutions for multi-core DSP chips

锐华机器人操作系统ReROS
ReWorks Robot ReROS

致力于ROS在中国的推广和应用
Promotion and application of ROS in Domestic

锐华移动操作系统ReMo
ReWorks Mobile ReMo

旨在实现安卓系统的国产替代
A domestic alternative to Android

锐华高安全操作系统
ReWorks Cert-61508& 50128

提升轨道交通和工业控制领域高端装备运行的安全性
Improving the safety of high-end equipment in railway and industrial control fields

锐华高安全操作系统航空版
ReWorks Cert-DO178B/C

提升航空航天领域高端装备运行的安全性
Improving the safety of high-end equipment in aerospace field

CETC 中国电科

应用行业
Application Industry

电子对抗
Electronic Warfare

雷达
Radar

预警探测
Early Warning Detection

无人装备
Unmanned equipment

工业控制
Industrial Control

车载电子设备
Car Electronics Equipment

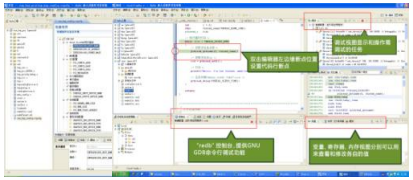
空间站
Space Station

舰载电子装备
Shipboard Electronic Equipment

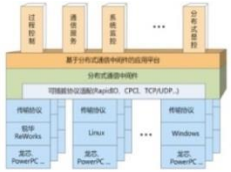
通讯导航
Communication Navigation

轨道交通
Railway

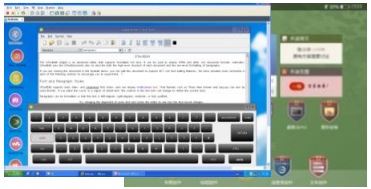
软件平台
Software Platform



嵌入式开发环境
Embedded Development Environment



行业支撑软件
Industry-Specific Software



图形系统
Graphic System

锐华嵌入式生态环境
Embedded Ecosystem of ReWorks

Loongson 飞腾 PHYTIUM freescale 飞思卡尔 ARM intel ATMEL 申威 TEXAS INSTRUMENTS 瑰芯

芯片 Chip

参考设计 Reference design

锐华基础软件 ReWorks Fundamental Software

支撑软件 软件平台 Supporting Software Software platform

模块 Module

解决方案 Solution

整机设备 应用软件 Equipment Application software

CASIC CSIC AVIC CETC 北方工业 NORINCO CSSC

龙芯3A、申威、华睿、飞腾1500
Loongson3A, SUNWAY, HUARUI, PHYTIUM1500

JSC8245、TI 6678、飞腾M6678、P1020、昆仑固件
JSC8245, TI 6678, PHYTIUMM6678, P1020, KunLun Firmware

安全认证咨询服务能力
Safety Certification Consulting Service

- 关键人员具有FSP和FSE资质能力
  Qualification ability of FSP and FSE owned by team key members
- 功能安全软件的研发、测试、验证和咨询服务
  Developing, testing, verification and consulting services for functional safety software

安全BSP包开发和定制能力
Safety BSP Development and Customization Services

- 针对用户需求定制安全BSP开发包
  Customizing the BSP development kit according to user needs
- 安全认证证据包
  Safety certification evidence package
- 核心硬件的在线自检
  Online self-test for core hardware
- 冗余节点间时钟同步和状态同步
  Clock synchronization and state synchronization between redundant nodes


CERTIFICATE

Qian Ma

Has successfully completed the Functional Safety Certification Program requirements for

Functional Safety Professional

In accordance with
IEC 61508:2010
IEC 62061:2015
ISO 13849:2015

Date issued: 9-Jan-2018
ID number: TA18040888
Field: Factory automation
Subject: Functional safety management
Hardware and software design

G. Greil
Certifier

W. Henke
Trainer

CETC 中国电科

CETC 中国电科

责任 创新 卓越 共享 Responsibility Innovation Excellence Shared