恒润科技
HIRAIN TECHNOLOGIES

MISRA C:2012浅析

本文本供个人学习使用，不得用于商业宣传！

编程标准的目的

恒润科技
HIRAIN TECHNOLOGIES

- 程序员对编译器的误解
  - C语言中许多地方是未经完善定义的，其实际行为取决于编译器
  - “未定义行为”可能会随着编译器的改变而改变
- 编译器的错误
  - 编译器也是软件，也有缺陷
  - 对于C的一些难以理解的地方，编译器的编写者很容易错误地解释和实现
- 操作平台的差异
  - 不同的目标平台上表现不一样
- 运行时错误
  - 也许语言本身并没有问题，但某些特殊的数据会在代码运行时产生错误

编程标准的目的

恒润科技
HIRAIN TECHNOLOGIES

1. 定义一个更安全的C/C++语言子集

2. 提高代码质量
   - 可靠性
   - 可维护性
   - 轻便性
   - 可测试性

怎样判断一套好的编程标准？

恒润科技
HIRAIN TECHNOLOGIES

- 规模: 规模不能太大，要容易阅读、理解？规模不能太小，要覆盖重要的编程过程中的问题。
- 语言: 编程规范的描述语言是否能让开发工程师都能懂？
- 理论依据: 对于任何一条编程标准是否都有丰富的解释说明?
- 教育意义: 开发工程师是否能够从中有收获?

编程标准

恒润科技
HIRAIN TECHNOLOGIES

- 编程标准的基础
  - ISO-C:1990
  - ISO-C++:2003

- 常用的编程标准
  - C：MISRA C-汽车制造业嵌入式C编程标准
  - C++：JSF C++-联合攻击战斗机C++编程标准
    HICPP (High Integrity C++)-高可靠性C++编程标准
    MISRA C++– 汽车制造业嵌入式C++编程标准
  - 行业标准：GJB 5369– 航天型号C语言安全子集

MISRA C：2012

MISRA C概述

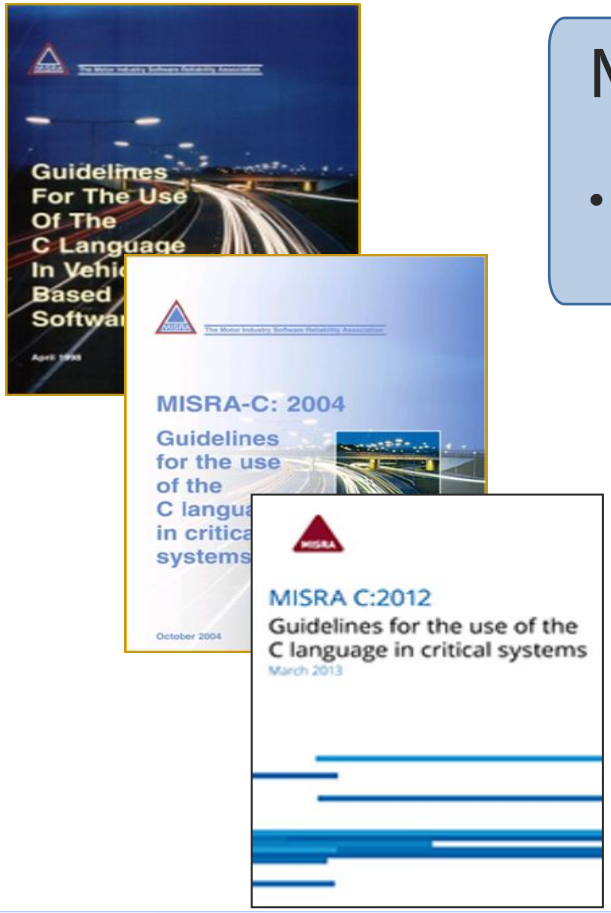
恒润科技 HIRAIN TECHNOLOGIES

- MISRA = The Motor Industry Software Reliability Association
  - 汽车工业软件可靠性联合会–源自于英国政府1990年成立的“安全IT”计划的一个项目
  - 1994年正式独立出来，总部在英国–致力于协助汽车厂商开发安全可靠的软件
- MISRA常设一个指导委员会，目前成员是
    - 福特汽车（Ford）
    - 捷豹路虎（Jaguar Land Rover）
    - 莲花公司（Lotus Engineering）
    - 米拉汽车设计（MIRA Ltd）
    - 里卡多公司（ Ricardo plc）
    - TRW汽车电子
    - 利兹大学（The University of Leeds ）

MISRA C概述

恒润科技 HIRAIN TECHNOLOGIES

- MISRA ——The Motor Industry Software Reliability Association



MISRA C:1998

- 从PRQA给福特和路虎定制的标准演变而来

MISRA C:2004

- 修正和扩充，添加了配套示范

MISRA C:2012

- 经过4年的努力，在2013年3月18日发布

MISRA C概述

恒润科技 HIRAIN TECHNOLOGIES

MISRA C标准为人们提供了C语言使用的限制子集
–MISRA C:1998
• 基于ISO 9899:1990 “Programming languages – C”， 即C90
• 127条规则
–MISRA C:2004
• 基于C90。废除了15条旧规则，部分规则细化，新引入一些数学操作的规则
• 共141条规则
121条强制：必须遵守。
20条建议：通常情况下要遵守。
–MISRA C3
• 基于C99
• 159条规则

MISRA C:2012规则一览表

恒润科技
HIRAIN TECHNOLOGIES

序号	分类	Mandatory	Required	Advisory	总计
1	指令		16		16
2	规则-标准C环境		2	1	3
3	规则-不可达代码		2	5	7
4	规则-注释		2		2
5	规则-字符集		1	1	2
6	规则-标识符		8	1	9
7	规则-类型		2		2
8	规则-常量		4		4
9	规则-声明和定义		10	4	14
10	规则-初始化	1	4		5
11	规则-Essential type		7	1	8
12	规则-指针类型转换		7	2	9

MISRA C:2012规则一览表

恒润科技 HIRAIN TECHNOLOGIES

序号	分类	Mandatory	Required	Advisory	总计
13	规则-表达式		1	3	4
14	规则-副作用	1	3	2	6
15	规则-控制语句表达式		4		4
16	规则-控制流		4	3	7
17	规则-switch语句		7		7
18	规则-函数	3	3	2	8
19	规则-指针和数组		6	2	8
20	规则-存储折叠	1		1	2
21	规则-预处理指令		11	3	14
22	规则-标准库		11	1	12
23	规则-其他	4	2		6
	总计	10	101	32	159

MISRA C:2012新特性

恒润科技
HIRAIN TECHNOLOGIES

- MISRA包内容增多
  - 编码规范增多（2012:159 ,2004:142 ）
  - 在MISRA 2004的基础上内容有所改善
- 更新了多条规范
  - 被重新改写或者完善
  - 规范的编号有调整
- 前一版本基础上的改进
  - 增加了新的需求点
  - 取消了部分编码规范限制

C语言标准支持情况

恒润科技 HIRAIN TECHNOLOGIES

ISO:C90

- 可以很好的支持ISO: C90
- 对代码的风险有很好的把控
- 缺陷 – 例如：不支持bool类型

MISRA C:1998
MISRA C:2004
MISRA C:2012

ISO:C99

- 增加新特性，例如：——Bool和inline函数
- 新风险考虑，例如：增加新的undefined behaviour
- 大部分编译器不支持C99的特性

MISRA C:2012

ISO:C11

- 相对比较新
- 支持C11有很多限制

MISRA C:2012

恒润科技 HIRAIN TECHNOLOGIES

标题

扩展解释

规则背景

示例

例外情况

Rule 8.8 The *static* storage class specifier shall be used in all declarations of objects and functions that have internal linkage

Category Required

Analysis Decidable, Single Translation Unit

Applies to C90, C99

Amplification

Since definitions are also declarations, this rule applies equally to definitions.

Rationale

The Standard states that if an object or function is declared with the *extern* storage class specifier and another declaration of the object or function is already visible, the linkage is that specified by the earlier declaration. This can be confusing because it might be expected that the *extern* storage class specifier creates external linkage. The *static* storage class specifier shall therefore be consistently applied to objects and functions with internal linkage.

Example

```
static int32_t x = 0;         /* definition: internal linkage  */
extern int32_t x;             /* Non-compliant                 */

static int32_t f ( void );    /* declaration: internal linkage */
int32_t f ( void )            /* Non-compliant                 */
{
  return 1;
}

static int32_t g ( void );    /* declaration: internal linkage */
extern int32_t g ( void )     /* Non-compliant                 */
{
  return 1;
}
```

MISRA C:2012

恒润科技 HIRAIN TECHNOLOGIES

规则类型

Directive / Rule

规则类别

- Advisory
- Required
- Mandatory

Rule 8.8	The *static* storage class specifier shall be used in all declarations of objects and functions that have internal linkage
Category	Required
Analysis	Decidable, Single Translation Unit
Applies to	C90, C99

Amplification

Since definitions are also declarations, this rule applies equally to definitions.

Rationale

f an object or functi class specifier and
e object or functio t specified by the
an be confusing bec *extern* storage class
linkage. The *static* re be consistently
ctions with internal

```
                                /* definition: internal linkage  */
                                /* Non-compliant                 */
id );   /* declaration: internal linkage */
int32_t f ( void )              /* Non-compliant                 */
{
  return 1;
}

static int32_t g ( void );   /* declaration: internal linkage */
extern int32_t g ( void )    /* Non-compliant                 */
{
  return 1;
}
```

语言

- C90
- C99
- C90, C99

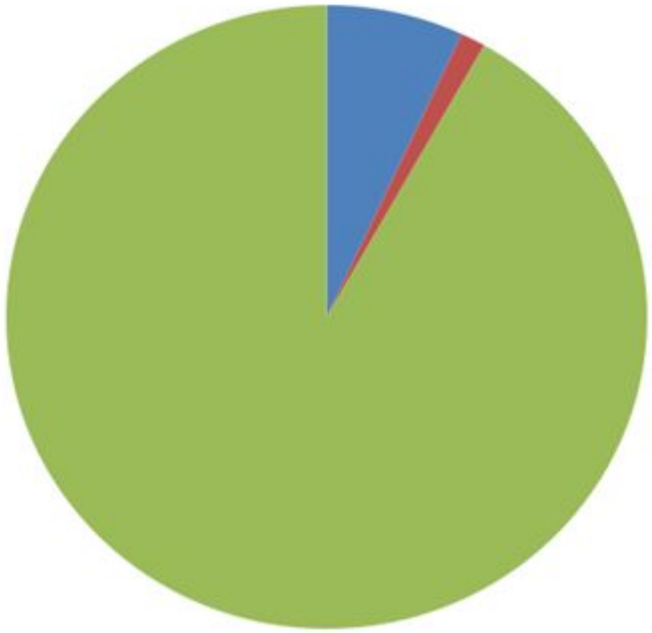
判定

- Decidable
- Undecidable

分析作用域

- Single Translation Unit
- System

MISRA C:2012



只适用于C90:2条规则

只适用于C99：11条规则

即适用于C90也适用于C99的规则

恒润科技 HIRAIN TECHNOLOGIES

- 两种规则类型：

Rules

- 有明确的要求
- 静态分析时强制执行(受到一定限制)
- 例如：Rule 8.6:函数应在文件范围内声明

Directives

- 要求并不十分明确
- 可能涉及“过程”或“文件”的要求
- 例如： Dir 3.1:所有源码应文档化以实现可溯性

- 三种规则类别：

- **Advisory** guidelines
  - 该种类型为建议类
  - 用户可酌情选择是否遵守该类规则
  - 违规处应文档化
  - 不要求背离文档
- **Required** guidelines
  - 背离该类规则时需要由背离文档
- **Mandatory** guidelines
  - 必须遵守

恒润科技培训-中秋国庆 好礼限时送

恒润科技 HIRAIN TECHNOLOGIES

双节同庆，好礼不停！

喜逢中秋、国庆双节，恒润科技祝各位工程师节日快乐！

伴着双节将近，恒润科技培训中心推出贺双节，培训课程优惠活动！只要您在2015年9 月30 日前报名参加恒润科技培训中心第四季度（2015 年10 月-12 月）的培训课程，培训结束后会获得精美礼品一份！

双节同庆，礼物翻倍！如果您的朋友有这方面的需求，不妨推荐他来参加培训，当然，培训结束后，您和朋友都可获得奖品！（注：推荐时间从即日起到2015 年9 月30 日止，推荐人向我们发送邮件告知或将推荐信在发送给朋友的同时抄送一份training@hirain.com，我们将以此邮件作为赠送礼品的证明）

精美礼品，绝对超值！还等什么呢？大家快来报名参加吧！

第四季度课程候选列表

恒润科技
HIRAIN TECHNOLOGIES

CAN/LIN总线技术基础	CANoe功能使用
CAN诊断协议详解及应用	QAC功能应用
SAE J1939协议详解及应用	CANalyzer功能使用
CAN标定协议详解及应用	汽车电子电磁兼容(EMC)技术及标准
CAN/LIN网络测试技术及实践	AUTOSAR功能及使用
嵌入式软件初级测试	ISO26262道路车辆功能安全
HIL网络基础及测试技术	ASPICE过程评估模型
MISRA C程序编写规范	基于模型设计软件基础应用

咨询及报名方式：

恒润科技
HIRAIN TECHNOLOGIES

1.恒润科技官方网站：

http://www.hirain.com/

2.咨询电话：

北京：010-6484 0808-6187/6189/6190

上海：021-6432 5416-855

3.报名邮箱：

发送您的报名信息至training@hirain.com

THANK YOU

http://www.hirain.com/

The end