Безопасность на максималках: как писать надёжный C/C++ код для встраиваемых систем

Докладчик:
Георгий Грибков

Докладчик

Георгий Грибков

Программист C++, один из разработчиков статического анализатора кода PVS-Studio

Разрабатывает набор диагностических правил, проверяющих код на соответствие стандартам MISRA C и MISRA C++

gribkov@viva64.com

Содержание

1. Стандарты кодирования: предпосылки появления
2. MISRA и AUTOSAR: что под капотом
3. Использование стандартов в ваших проектах

Предпосылки

Проблематика

- Популярность языка C

Проблематика

- Популярность языка C
- ПОПУЛЯРНОСТЬ языка C

Проблематика

- Популярность языка C
- ПОПУЛЯРНОСТЬ языка C
- Популярность языка C++

Проблематика

- Популярность языка C
- ПОПУЛЯРНОСТЬ языка C
- Популярность языка C++
- Несовершенство этих языков

Чем вызвана такая популярность

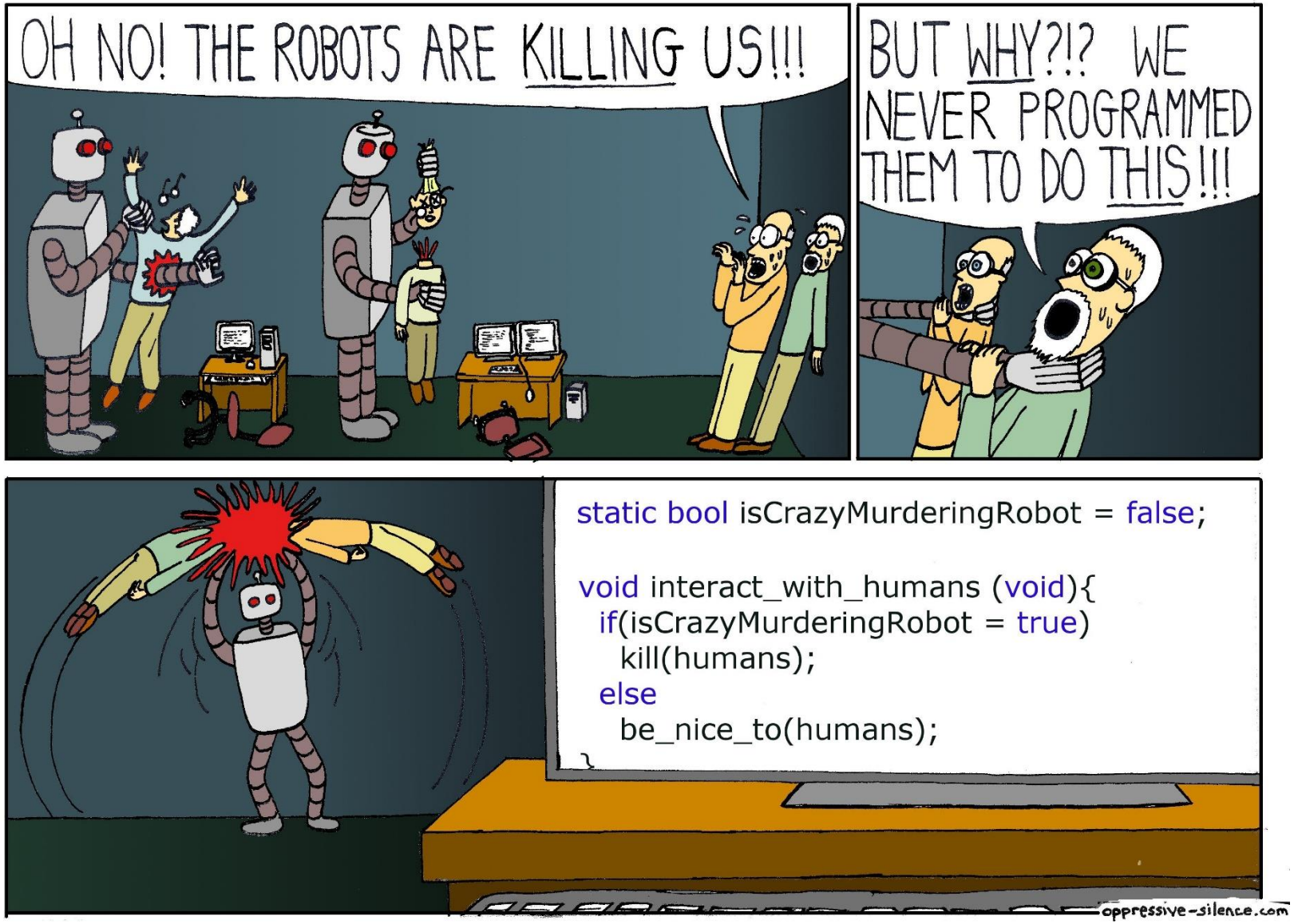
- Доступность компиляторов
- Стандартизированность
- Переносимость
- Длительный опыт использования
- Эффективность
- Поддержка средствами анализа

Слабые места C и C++

- Неполная спецификация стандартом
- Undefined, unspecified, implementation-defined behavior
- Неправильное обращение с языком

```
if ( i = 0 ) или if ( i == 0 )?
```

Слабые места C и C++



Что, если ответственность высока?

Пример очень дорогой ошибки

- 4 июня 1996 года европейская ракета-носитель Ariane 5 превратилась в конфетти на 37 секунде полета

Пример очень дорогой ошибки

- Расследование показало, что причиной аварии послужила программная ошибка (целочисленное переполнение)
- На борту ракеты были четыре спутника
- Убытки составили 370 000 000 $

Вывод: надо что-то делать!!!

Стандарты кодирования:
что под капотом

MISRA: что это такое

- MISRA – это набор рекомендаций

Актуальные версии:

- MISRA C:2012 – 143 правила
- MISRA C++:2008 – 228 правил

MISRA: что это такое

- MISRA – это «Motor Industry Software Reliability Association»:
  - Bentley Motor Cars
  - Ford Motor Company
  - Jaguar Land Rover
  - Delphi Diesel Systems
  - HORIBA MIRA
  - Protean Electric
  - Visteon Engineering Services
  - The University of Leeds
  - Ricardo UK
  - ZF TRW

Немного про AUTOSAR

- AUTOSAR – это AUTomotive Open System Architecture

Немного про AUTOSAR

- AUTOSAR – это AUTomotive Open System Architecture
  - BMW Group
  - Bosch
  - Continental
  - Daimler AG
  - Ford
  - General Motors
  - PSA Peugeot Citroën
  - Toyota
  - Volkswagen
  - …и еще более 200 партнёров

Немного про AUTOSAR

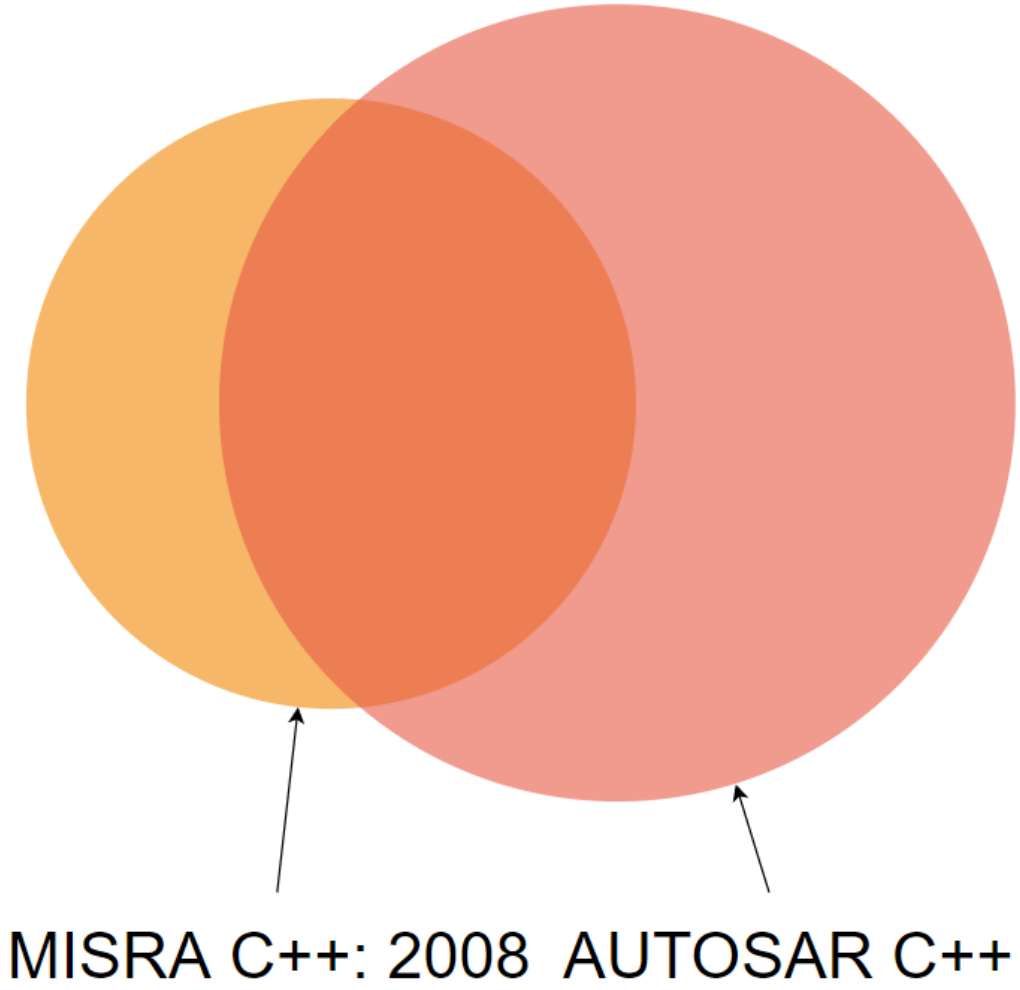
- AUTOSAR – это AUTomotive Open System Architecture
- AUTOSAR – это методология разработки
- AUTOSAR C++ – часть этой методологии

Актуальная версия:

- AUTOSAR C++: 19-03 – более 350 правил

MISRA C++ и AUTOSAR C++

	MISRA C++	AUTOSAR C++
C++03	✓	✓
C++11	X	✓
C++14	X	✓



Где используются MISRA и AUTOSAR

Категории правил:

1. Mandatory – обязательные к следованию
2. Required – допустимы отклонения
3. Advisory – следование опционально

Примеры правил

Обязательные правила:

- Не используйте значение неинициализированной переменной
- Не используйте указатель на *FILE* после закрытия потока
- Не пишите недостижимый код
- Счетчик цикла не должен иметь floating-point тип
- …

Примеры правил

Необходимые правила:

- Не используйте *goto* и *longjmp*
- Каждый *switch* должен заканчиваться *default*
- Тела операторов *if*, *else*, *for*, *while*, *do*, *switch* должны быть завернуты в скобки
- Не используйте вариативные функции
- …

Примеры правил

…и все остальные:

- Суффикс ‘*L*’ должен всегда быть заглавным (*42L*)
- Не используйте адресную арифметику (кроме *[]* и *++*)
- Не используйте оператор «запятая»
- Не изменяйте параметр функции внутри тела
- …

Философия

ПИСАТЬ БЕЗ ОШИБОК

ПИСАТЬ ТАК, ЧТОБЫ ОШИБКИ НЕ ПОЯВЛЯЛИСЬ

ПИСАТЬ ТАК, ЧТОБЫ НЕ ПОЯВЛЯЛИСЬ ОШИБКИ, ИЗ-ЗА КОТОРЫХ ПОЯВЛЯЮТСЯ ОШИБКИ

MISRA

А что есть помимо правил?

Еще есть много всего!

- Классификация правил по разным признакам
- Применимость к генерированному коду
- Полный список undefined/unspecified/etc… поведений
- Чек-листы по настройке анализаторов, процессу проверки, и т.д
- Матрица пересечений с другими стандартами
- Примеры документации

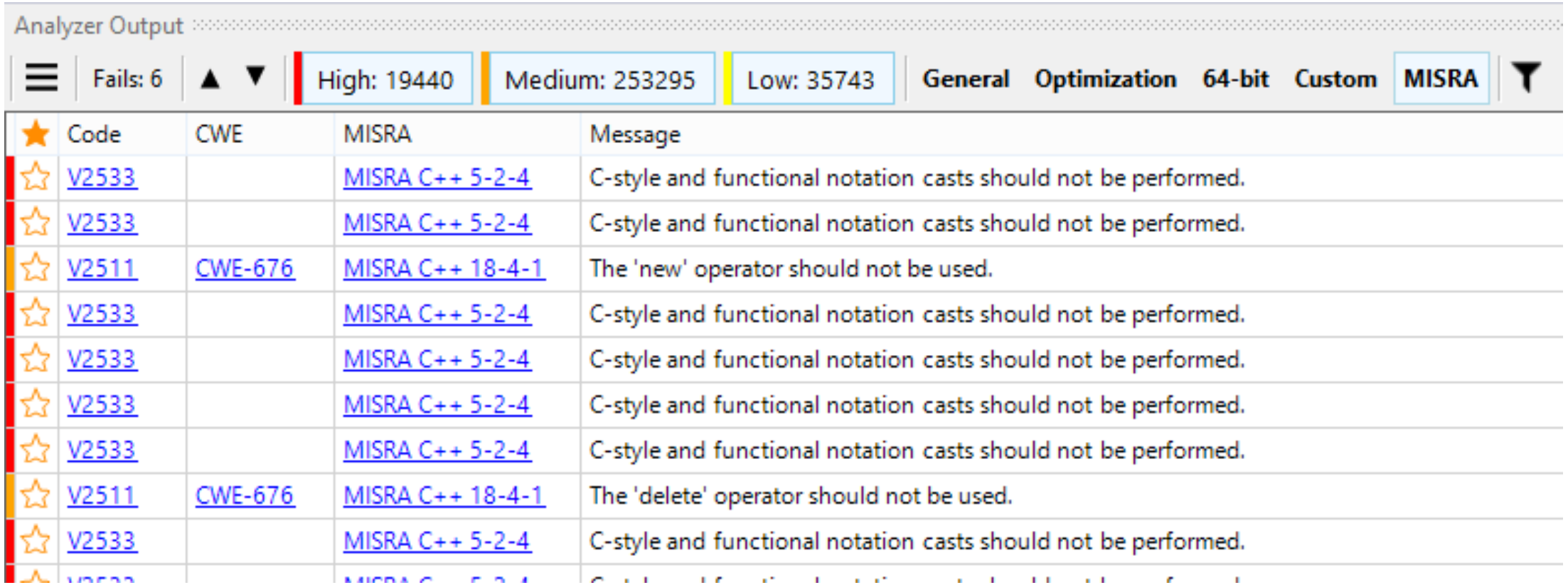
Использование стандартов в ваших проектах

Проверка кода на соответствие

- Проверять вручную? Кошмар!
- Используйте статические анализаторы кода
- Статический анализ – это автоматизированный процесс code review

Внедрение

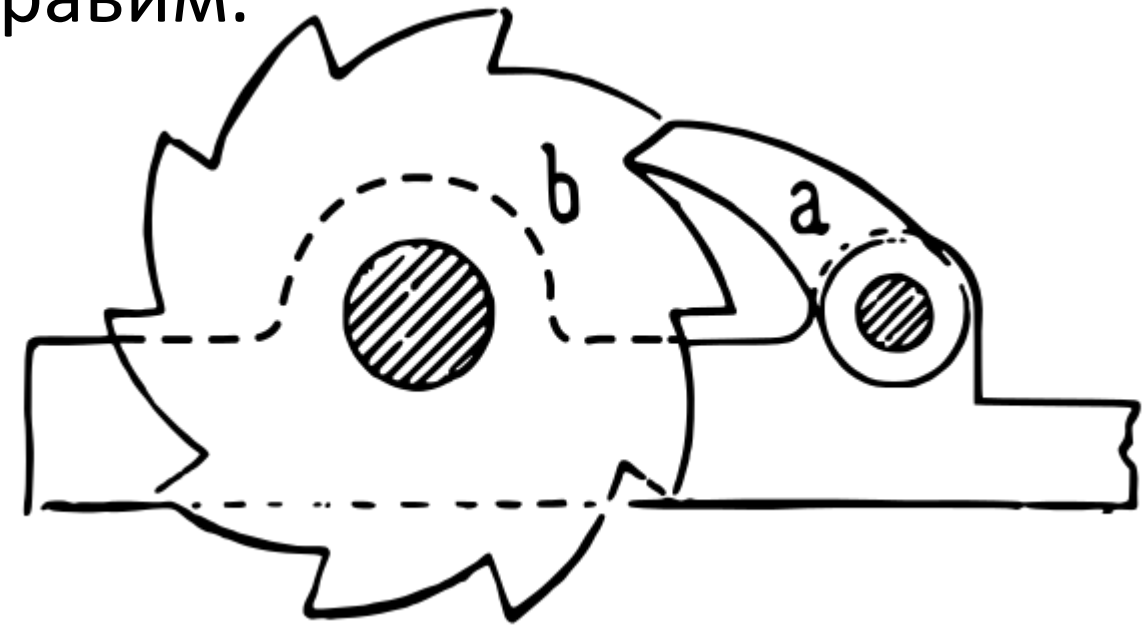
- Начните использовать стандарт ДО начала проекта
- Если уже есть код – подумайте несколько раз



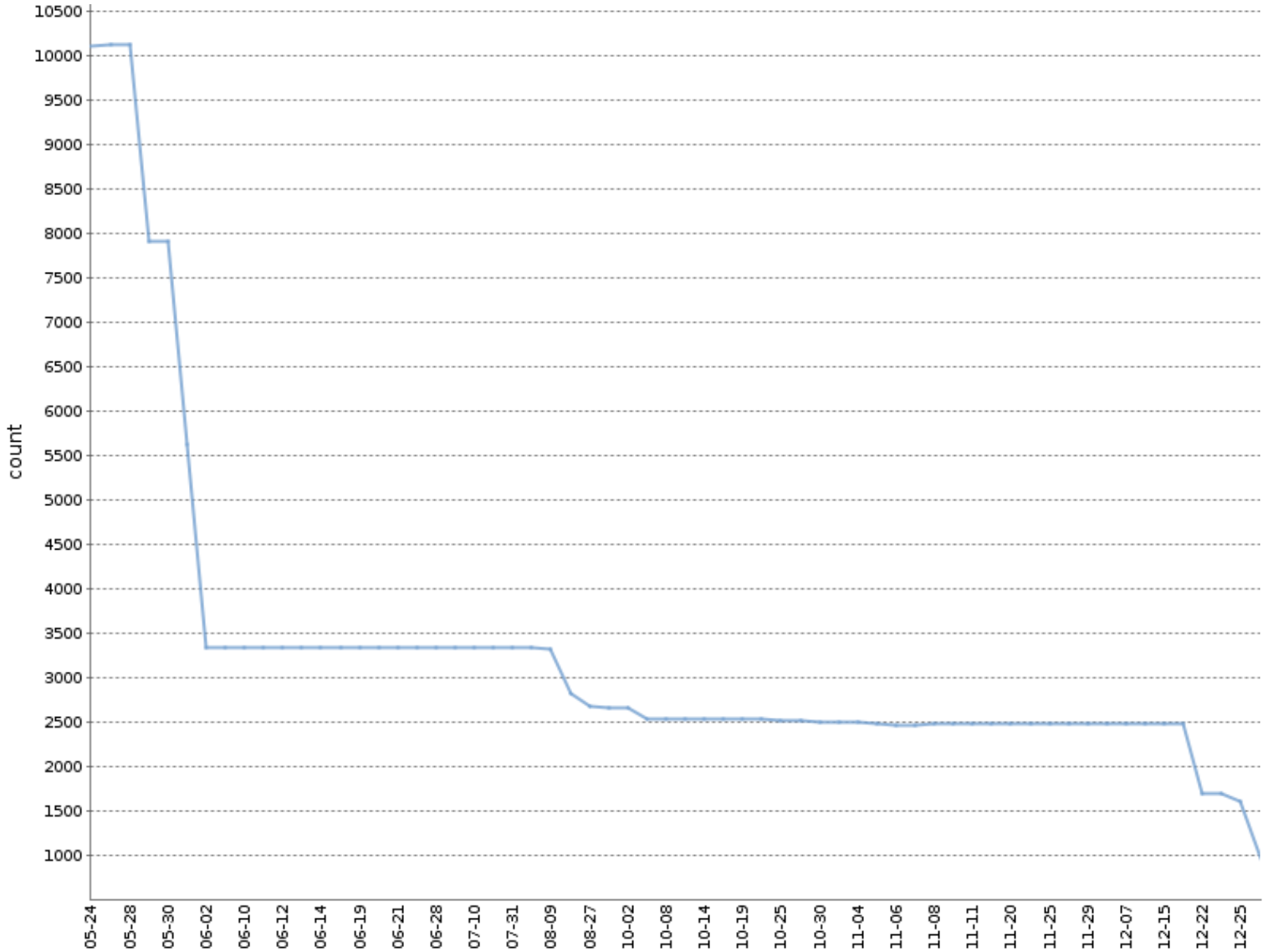
Code	CWE	MISRA	Message
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.
V2511	CWE-676	MISRA C++ 18-4-1	The 'new' operator should not be used.
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.
V2511	CWE-676	MISRA C++ 18-4-1	The 'delete' operator should not be used.
V2533		MISRA C++ 5-2-4	C-style and functional notation casts should not be performed.

Используйте подавление сообщений!

- Прячем старые ошибки – работаем в привычном темпе
- С этого момента видим только новые предупреждения
- Получаем пользу от анализатора СРАЗУ
- Спрятанные ошибки не забываем! Возвращаемся и потихоньку правим.



Как работать с suppress-базой



Как и где стоит проводить проверку

- Локально на компьютерах разработчиков (плагины для IDE, системы мониторинга компиляции)

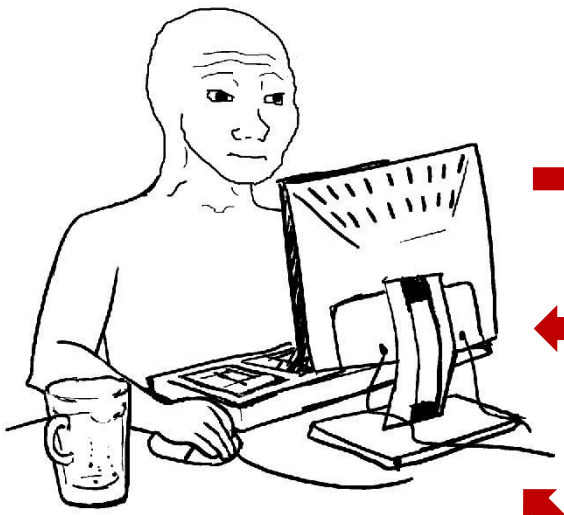
Как и где стоит проводить проверку

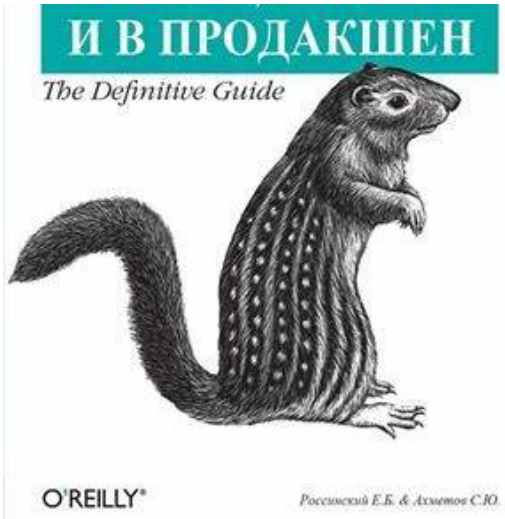
- В системах непрерывной интеграции (command-line утилиты, плагины для CI-систем, системы мониторинга)

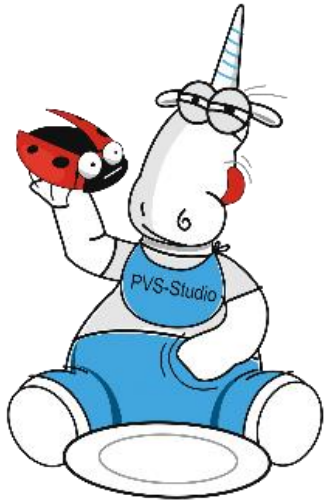





Как и где стоит проводить проверку







Как доказать соответствие вашего проекта?

Вам понадобятся:

- Код, соответствующий уровням Mandatory и Required
- План обеспечения соответствия (guide enforcement plan)
- Документация по всем отклонениям
- Документация по всем предупреждениям компиляторов и статических анализаторов
- Резюме о соответствии правилам (guideline compliance summary)

План обеспечения соответствия

Пример guide enforcement plan:

Правило	Компилятор		Анализатор		Обзор кода
	“A”	“B”	“A”	“B”	
…					
5.1	No errors	No errors	---	---	Procedure x
5.2	No errors	No errors	Warning V2561	No messages	
…					
10.4	Warning 458	No errors	No warnings	No messages	
…					

Тщательно документируйте отклонения

- Иногда четко следовать стандарту невозможно.
  Пример:

```
const unsigned char *PORT = 0x10u;
```

- Специфика отклонений разная

Тщательно документируйте отклонения

- Документация отклонения должна содержать:
  - Номер нарушенного правила
  - Локацию нарушения
  - Обоснованность
  - Доказательство безопасности
  - Потенциальные последствия

Резюме о соответствии правилам

Пример guideline compliance summary

Правило	Категория MISRA	Соответствие
…		
5.1	Mandatory	Соответствует
5.2	Required	Есть отклонения
…		
10.4	Advisory	Не используется
…		

Итог:

- Весь C/C++ код соответствует Mandatory и Required 
- План обеспечения соответствия полностью заполнен 
- Все отклонения задокументированы 
- Все предупреждения компиляторов и анализаторов исправлены или размечены 
- Заполнено резюме о соответствии 

Поздравляю! Вы достигли **безопасности на максималках**!!!

Подробнее про соответствие стандартам MISRA

MISRA Compliance: 2016

Achieving compliance with MISRA Coding Guidelines

The Power of 10: золотые правила NASA

1. Долой сложные ветвления, goto и рекурсию
2. Все циклы должны быть ограничены
3. Динамические аллокации памяти – в топку
4. Всякая функция должна умещаться на листе бумаги
5. Не больше двух runtime-ассертов на функцию

The Power of 10: золотые правила NASA

6. Данные должны объявляться в самом низком scope
7. Функция что-то возвращает? Обязательно проверить!
8. Не используйте препроцессинг
9. Никаких вложенных указателей
10. «Правило нуля предупреждений»

The Power of 10: золотые правила NASA

Статья по теме:

47

Заключение

Подведем итоги

- Иногда классических способов обеспечения качества недостаточно
- Внутри MISRA и AUTOSAR C++
- Использование стандартов в ваших разработках

END

Q&A