Средства разработки программного обеспечения критически важных для безопасности сертифицируемых встраиваемых компьютерных систем

Демьянов А.В., ООО «АВД Системы»
www.avdsys.ru

Путин - «оборонке»:
Время пройдет, гособоронзаказ сократится.
Что делать будете?

"Высокотехнологичная гражданская продукция" ... А что это ?

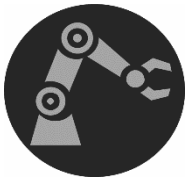
→ Это оборудование со встроенным компьютером и ПО.

Как минимизировать риски функционала ПО критически важных систем? Как тестировать ПО таких систем?

Отраслевые стандарты безопасности ПО

DO-178/ED-12/КТ-178

Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники.



МЭК 61508/ГОСТ Р МЭК 61508

Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью.

EN 50128/МЭК 62279/ГОСТ Р МЭК 62279

Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах.

ISO 26262/ГОСТ Р ИСО 26262

Дорожные транспортные средства – функциональная безопасность.

МЭК 60880/ГОСТ Р МЭК 60880

Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем.

МЭК 62304/ГОСТ Р МЭК 62304

Изделия медицинские. Программное обеспечение. Процессы жизненного цикла.

«Safety» и «Security»

Safety

Безопасность функциональная
Устройство не должно нанести вред внешнему миру

Security

Безопасность информационная (защищенность)
Внешний мир не должен нанести вред устройству

Safety critical

Критически важной для безопасности является такая компьютерная система, некорректная работа которой несет угрозу здоровью или жизни людей (например, авария на транспорте), или может нанести существенный ущерб окружающей среде (например, выброс на вредном производстве) или чревата значительным экономическим ущербом (например, потерей космического аппарата).

Security critical

Отдельная большая и сложная тема.
В последнее время

Затраты на разработку ПО критических для безопасности сертифицируемых ВКС

в среднем в 4 раза выше,

чем на разработку ПО обычных ВКС

Динамический и статический анализ ПО

Динамический анализ

Исполнение ПО (прогон) и анализ результатов его исполнения.

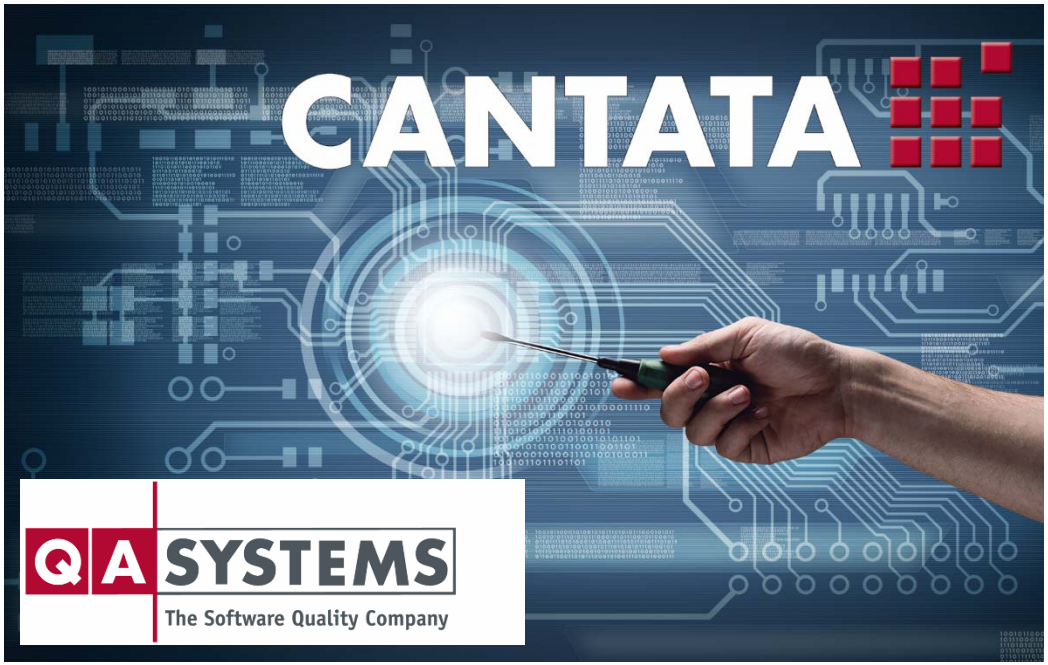
Пример динамического анализа: тестирование и анализ полноты тестового покрытия.

Статический анализ

Анализ исходного текста или бинарного кода без исполнения ПО с целью предсказания динамических характеристик ПО.

Пример статического анализа: расчет времени исполнения наихудшего случая WCET (Worst Case Execution Time).

Среда автоматизированного тестирования Cantata фирмы QA Systems (Германия)




SGS TÜV SAAR

CERTIFICATE NO FS/71/220/18/0303 PAGE 1/1

LICENCE HOLDER
QA Systems GmbH
Schwieberdinger Straße 56
70435 Stuttgart
Germany

MANUFACTURING PLANT
QA Systems Ltd
2 Palace Yard Mews
Bath, BA1 2NH
United Kingdom

PROJECT NO/-ID: K3UX-AU07
LICENSED TEST MARK
CERT. REPORT NO.: K3UX0008

Tested according to: IEC 61508:2010; ISO 26262-8:2011; clause 11.4.8 and 11.4.9; EN 50128:2011; IEC 60880:2006; IEC 62304:2015

Certified product(s): Cantata, Core product

Model(s): Version: 8.0; Build_id: RELEASE_8_0.4

Technical Data and Parameter: Suitable for verification of safety-related software acc. to:
- ISO 26262 up to ASIL D
- IEC 61508 up to SIL 4, class T2 tool
- EN 50128 up to SIL 4, class T2 tool
- IEC 62304 up to SW safety Class C
- IEC 60880 for category A functions

Specific Requirements: The certificate is based on voluntarily tests. Any changes to the design, components or processing may require repetition of some parts of the pre-qualification in order to retain the certification. The certificate report is an integral part of this certificate. The safety related application guidelines shall be maintained.

Certification Body for Functional Safety SGS-TÜV Saar GmbH

Munich, 27.07.2018

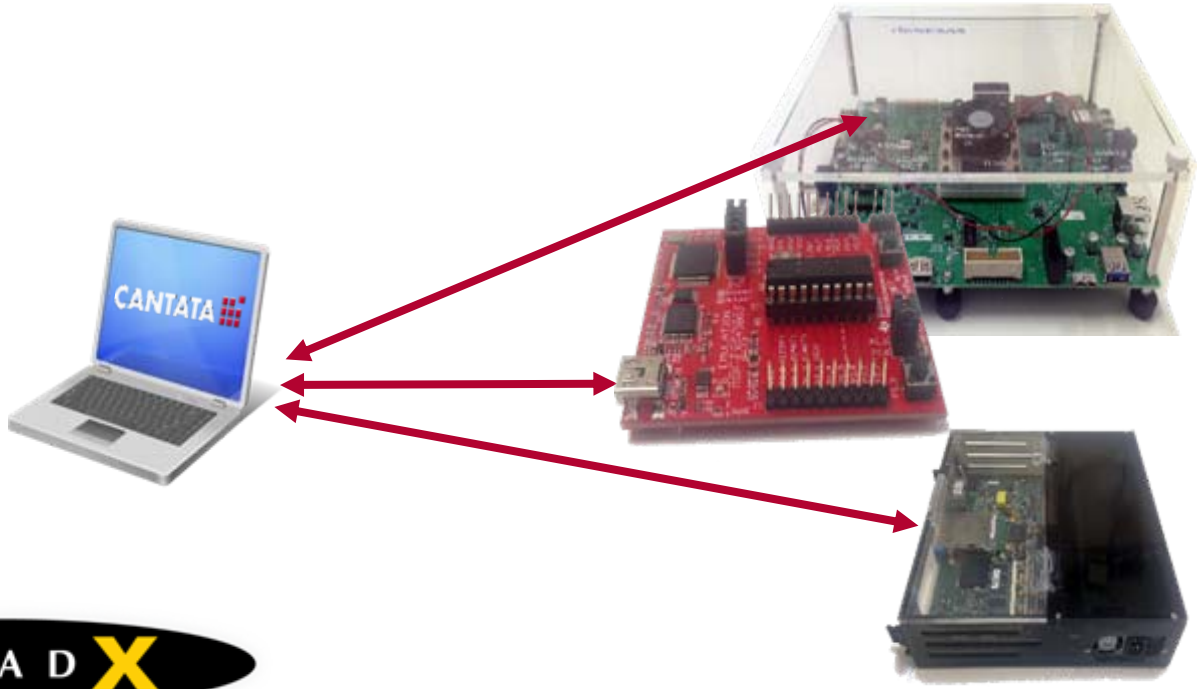
Gudrun Neumann

CERTIFICATE

Сертифицирована SGS-TüV Saar GmbH как «средство верификации программного обеспечения, относящегося к безопасности», соответствующее стандартам:
МЭК 61508 (общепромышленное оборудование) - до уровня SIL 4;
EN 50128 (железнодорожные системы) - до уровня SIL 4;
ISO 26262 (автоэлектроника) - до уровня ASIL D;
МЭК 62304 (медицинская техника) - до класса C;
МЭК 60880 (системы контроля АЭС) - для категории A.
Сопровождается комплектом квалификационных материалов по DO-178

CANTATA

Интеграция с IDE и системами управления требованиями



THREADX

WIND

Green Hills

CodeWarrior Development Studio

QNX

COSMIC Software

RENESAS

LYNUXWORKS

IAR Embedded Workbench

KEIL Tools by ARM

Code Composer Studio

Visual Studio

TASKING

ARM

X

PTC Integrity

POLARION

Direct Integration

IBM

codeBeamer

Средства статического анализа фирмы AbsInt Angewandte Informatik (Германия)

Тестирование может показать наличие ошибок, но не может доказать их отсутствие

Для доказательства отсутствия ошибок используется математический аппарат Abstract Interpretation

По бинарному коду:

aiT	расчет времени исполнения наихудшего случая WCET (Worst-Case Execution Time)
StackAnalyzer	анализ размера используемого стека и предсказание ситуаций его переполнения

По исходному тексту:

Astree	анализ C-программ на отсутствие run-time ошибок и состязаний за данные
RuleChecker	контроллер нормативов кодирования (ограничений использования конструкций языка) и сбор метрик программного кода на языке C

Все инструменты сопровождаются комплектом квалификационных материалов Qualification Support Kit

Компилятор и средства разработки для языка программирования Ada фирмы AdaCore (Франция)

Язык программирования Ada был разработан в начале 80-х годов.
Целью разработки было создание языка для встраиваемых систем реального времени с повышенными требованиями к надежности ПО.

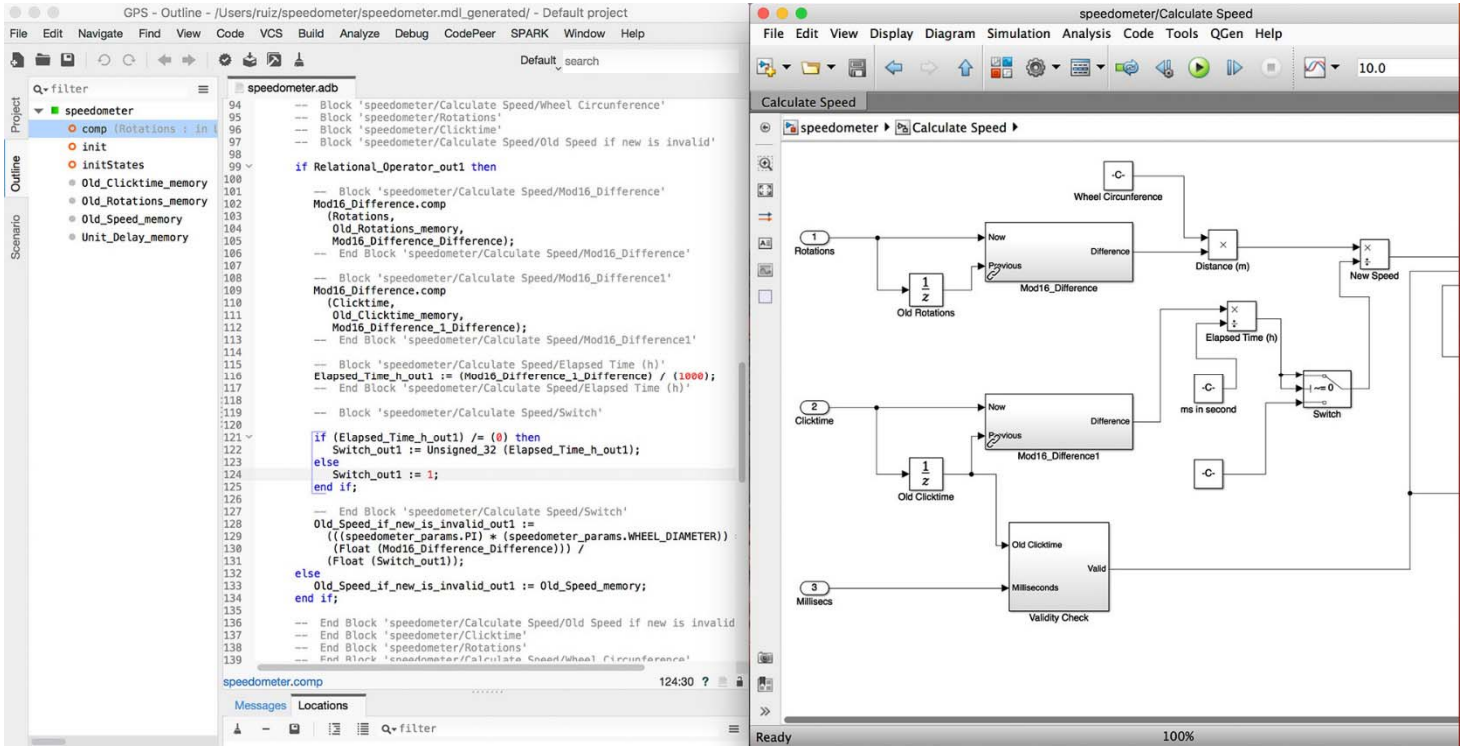
Ada 83	Ada 95	Ada 2005	Ada 2012
ГОСТ 27831-88	---	---	---

Международный стандарт ISO 8652:2012

Введена конструкция для задания «контрактов» - требований к результатам работы программного модуля, описанных непосредственно в тексте программы на языке Ada. «Контракт» предназначен для использования компилятором для выполнения динамических проверок или средствами статического анализа для формальной верификации – доказательства математическими методами, что ПО делает то, что от него требуется и не делает того, что не требуется. (DO-333 Formal Methods Supplement to DO-178C)

www.adacore.com/books

QGen – квалифицируемый генератор программного кода из моделей Simulink



- **Квалифицируемый по DO-178C на уровень TQL1 (Tool Qualification Level), что позволяет исключить верификацию сгенерированного кода**
- **Поддерживает «безопасное» подмножество ~120 блоков Simulink и Stateflow**
- **Производит код на языках MISRA C (сертифицируемое подмножество языка C) и SPARK (формально-верифицируемое подмножество языка Ada)**
- **Включает отладчик на уровне моделей, позволяющий проводить совместную отладку автоматически сгенерированного и рукописного кода**

www.adacore.com/qgen