

# SCADE

Комплекс средств разработки программного обеспечения ответственных систем управления, сертифицируемых по стандартам безопасности МЭК 61508/EN 50128, и его применение на железнодорожном транспорте



Демьянов А.В., АД Системс  
Дистрибьютор Esterel Technologies в России



# Стандарты МЭК 61508 и EN 50128



**МЭК = Международная Электротехническая Комиссия**

**[www.iec.ch/61508](http://www.iec.ch/61508)**

МЭК 61508 “Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью”

**EN = Европейская Нормаль CENELEC**

**[www.cenelec.eu](http://www.cenelec.eu)**

EN 50128 “Системы телекоммуникационные, сигнализационные и системы для обработки данных, применяемые на железных дорогах. Программное обеспечение для систем управления и защиты на железных дорогах”

**Уровни Полноты Безопасности SIL (Safety Integrity Level)**

Допустимое количество опасных отказов в час:

SIL4 ( $10^{-9}..10^{-8}$ ), SIL2 ( $10^{-8}..10^{-7}$ ), SIL3 ( $10^{-7}..10^{-6}$ ), SIL1 ( $10^{-6}..10^{-5}$ )



**Прикладное ПО**  
наиболее сложная, объемная  
и часто изменяемая часть

Подсистема ввода/вывода и драйверы

Операционная система и планировщик

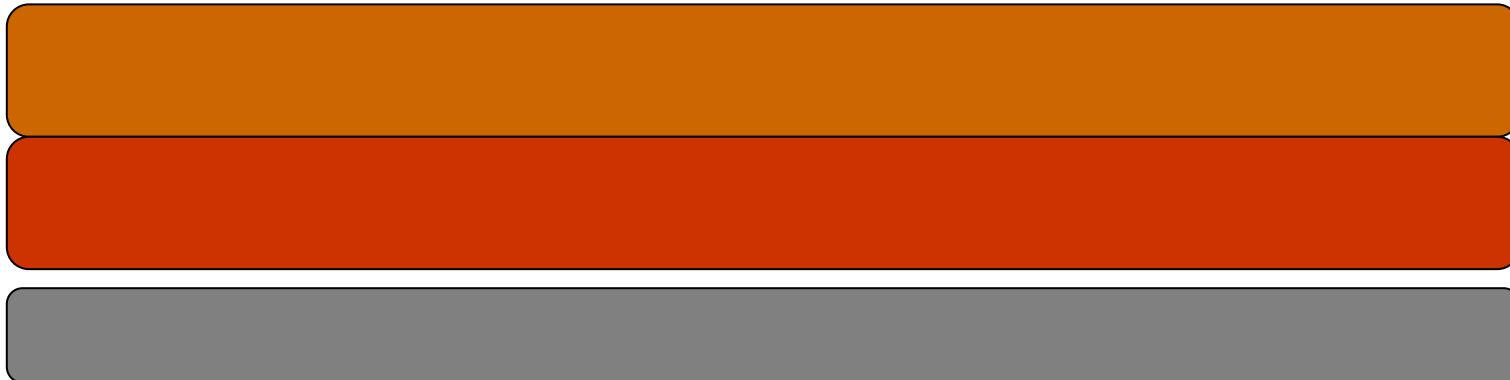
Аппаратура

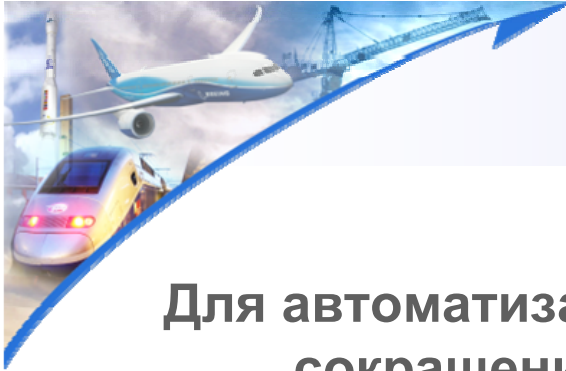
**Затраты на разработку ПО ответственных  
сертифицируемых по безопасности систем  
в 4 раза выше,  
чем ПО обычных встраиваемых систем**



### **Safety Critical Application Development Environment** **Среда разработки приложений** **с критичными требованиями к безопасности**

Комплекс средств визуального модельно-ориентированного программирования с генераторами С-кода, сертифицированного по стандартам безопасности DO-178B (Авиация), IEC 61508 (Промышленность и энергетика) и EN 50128 (Железнодорожный транспорт)





## Зачем нужен SCADE ?

Для автоматизации процесса разработки прикладного ПО и сокращения затрат на разработку, тестирование и сертификацию по стандартам безопасности.

### За счет чего это достигается ?

1. Максимально возможное исключение ручного кодирования, подверженного ошибкам и влиянию человеческого фактора
2. Применение автоматического кодогенератора позволяет полностью исключить тестирование отдельных программных модулей.
3. Применение кодогенератора, квалифицированного по стандарту безопасности, позволяет значительно упростить и удешевить процесс сертификации

# SCADE в железнодорожном транспорте

## Aerospace & Defense



55%

Airbus  
Boeing

...

Всего порядка 50 заказчиков  
включая

**Гражданские Самолеты Сухого**  
**ГосНИИ Авиационных Систем**  
**МНПК «Авионика»**

## Rail Transportation



25%

Alstom Transportation  
Ansaldo Signal  
AREVA Technicatome  
Deuta Werke  
RATP  
SNCF  
Siemens Rail Transportation  
Thales Rail Signalling Systems  
Union Switch  
**ВНИИАС МПС**

## Industrial, Automotive & Energy



20%

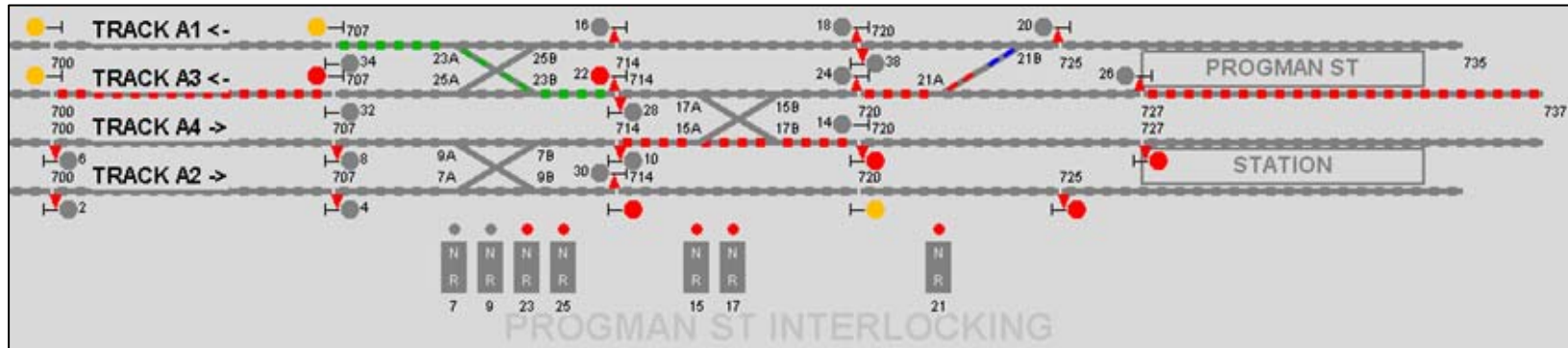
**Общий объем продаж в 2007г = \$19M**



# SCADE в железнодорожном транспорте

## ANSALDO SIGNAL

### Interlocking & Train Control System (I&TCS)



Проект OURAGAN для RATP  
Парижский метрополитен

Проект ST PANCRAS  
Новая Лондонская станция Eurostar

Проект PAI-NG для SNCF  
Новая система интервального  
регулирования

Гонконгский метрополитен (MTR)





## SCADE в железнодорожном транспорте



Отделение А и АЛС  
(Автоматики и Автоматической  
Локомотивной Сигнализации)



### КЛУБ-У

Комплексное Локомотивное Устройство  
Безопасности Унифицированное



### АБТЦ-М

Система автоблокировки с  
централизованным размещением  
аппаратуры, тональными рельсовыми  
цепями и дублирующими каналами  
передачи информации



# Сертификат TUV на кодогенератор SCADE KCG

ZERTIFIKAT ♦ CERTIFICATE ♦ 認証証書 ♦ СЕРТИФИКАТ ♦ CERTIFICADO ♦ CERTIFICAT

## CERTIFICATE

No. Z10 07 04 55460 002



**Holder of Certificate: Esterel Technologies SA**  
Parc Euclide  
8, rue Blaise Pascal  
78990 Elancourt  
FRANCE

**Factory(ies):** 55460

**Certification Mark:**



**Product:** Software Tool for Safety Related Development

**Model(s):** Code Generator KCG

**Parameters:** Qualified for each SIL according to IEC 61508 and EN 50128 as far as appropriate

The report no. EE 81045 C is a mandatory part of this certificate. The product complies with the following listed safety requirements only if the specifications documented in the currently valid revision of this report are met.

**Tested according to:**

- IEC 61508 1,3,4, 2000, SIL 3
- EN 50128: 2001, SIL 3/4

The listed product was tested on a voluntary basis and complies with the relating standards or directives. The certification mark shown above can be affixed on the product. The certification mark must not be altered in any way. See also notes overleaf.

**Test report no.:** EE 81045 C

**Date,** 2007-04-05

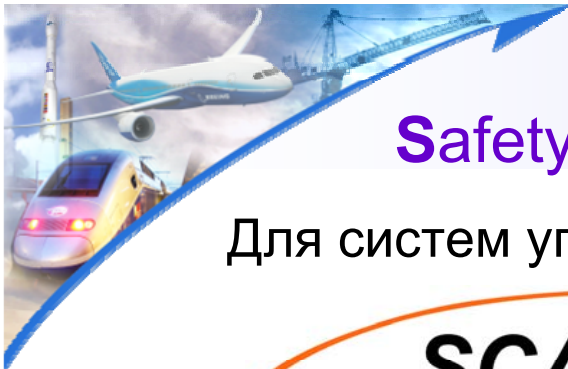


TUV SÜD Product Service GmbH - Zertifizierstelle - Röllnerstrasse 65 - 80339 München - Germany

# IEC 61508 SIL 3

# EN 50128 SIL 3/4





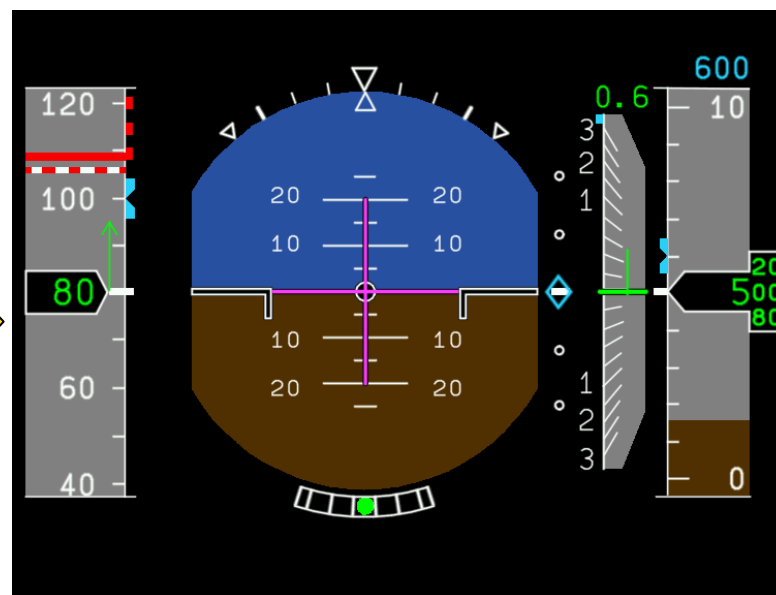
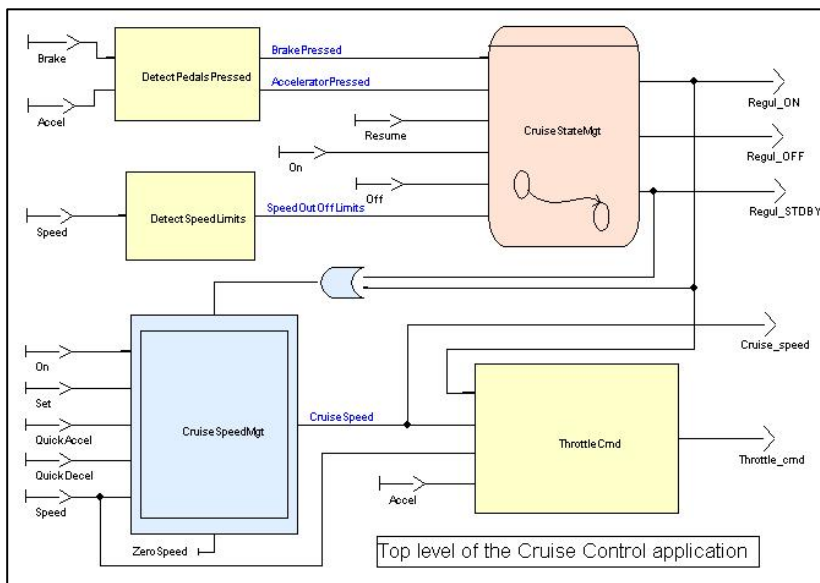
# SCADE

## Safety Critical Application Development Environment

Для систем управления



Для систем отображения



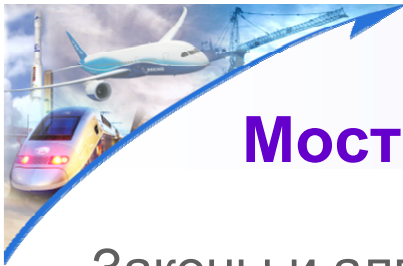
### SCADE Suite KCG

Квалифицированный по DO-178В  
генератор С-кода

### SCADE Display KCG

Квалифицированный по DO-178В  
генератор вызовов графических функций

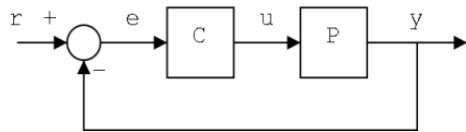




# SCADE Suite

## Мост между инженерами по САУ и программистами

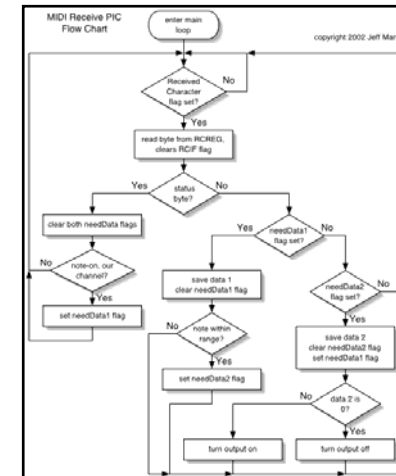
Законы и алгоритмы управления



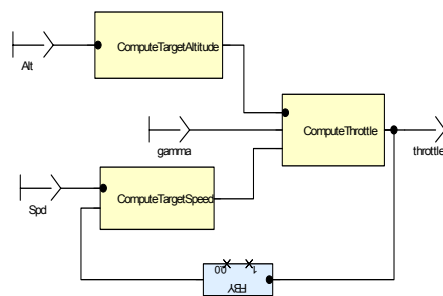
$$X(z) \triangleq \sum_{n=-\infty}^{\infty} x(n)z^{-n} \quad (\text{bilateral } z \text{ transform})$$



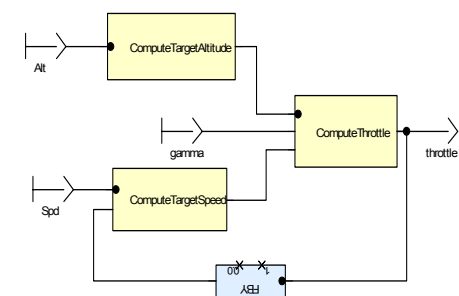
Программы



Визуальные модели



Визуальные модели



### Ввод и моделирование

Graphical Editor – графический редактор

Graphical Simulator – графический симулятор

Model Reporter – генератор проектной документации

Configuration Management Gateway – шлюз к системам управления

### Шлюзы к системам управления требованиями и средствам системного проектирования

(DOORS, RequisitePro, Simulink, Rhapsody)

### Верификация и валидация (V&V)

Model Test Coverage (MTC) – анализ тестового покрытия на уровне моделей

Design Verifier (DV) – верификатор дизайна

### Генерация кода

Qualified Code Generator (KCG) – квалифицированный кодогенератор

Compiler Verification Kit (CVK) – комплект верификации компилятора

## SCADE и окупаемость инвестиций (ROI)

Этап разработки проекта	Доля затрат	Экономия при применении SCADE (по данным пользователей SCADE)
Определение концепций	5%	0%
Системное проектирование	12%	0%
Разработка системных требования к ПО	14%	50%
Проектирование ПО (детализация спецификаций)	15%	50%
Кодирование	10%	70%
Модульное тестирование	12%	70%
Интеграционное тестирование	7%	30%
Системное тестирование	10%	30%
Документирование	15%	70%
<b>Суммарная экономия при применении SCADE</b>		<b>46%</b>



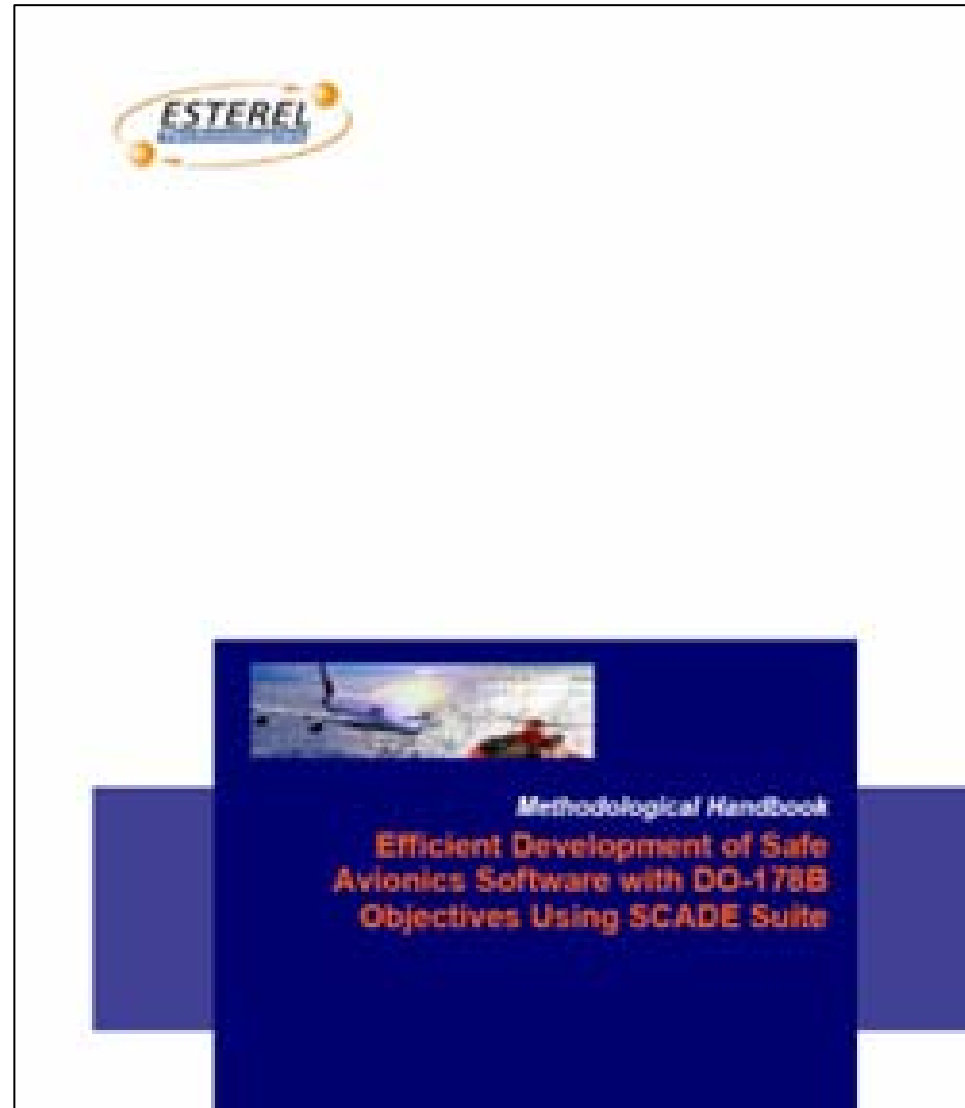


# SCADE Methodological Handbooks

**DO-178B Handbook**

**IEC 61508 Handbook**

**EN 50128 Handbook**





# SCADE Suite Evaluation CD



avdsys@aha.ru



Дополнительная информация

**Esterel Technologies**

**[www.esterel-technologies.com](http://www.esterel-technologies.com)**

**АВД Системс**

**[www.avdsys.ru](http://www.avdsys.ru)**

**Вопросы ?**