



it 2  
release 1/5

**Экспертиза КЯР США установки по  
производству смешанного оксидного  
(МОКС) топлива**

**Контроль качества программного  
обеспечения**

**Совещание с Госатомнадзором РФ**

**Июль-август 2003 г.**

**Уилкинс Смит и Пол Лозер**

**Комиссия ядерного регулирования США**



**NRC Review of the Mixed Oxide Fuel  
Fabrication Facility  
Software Quality Control**

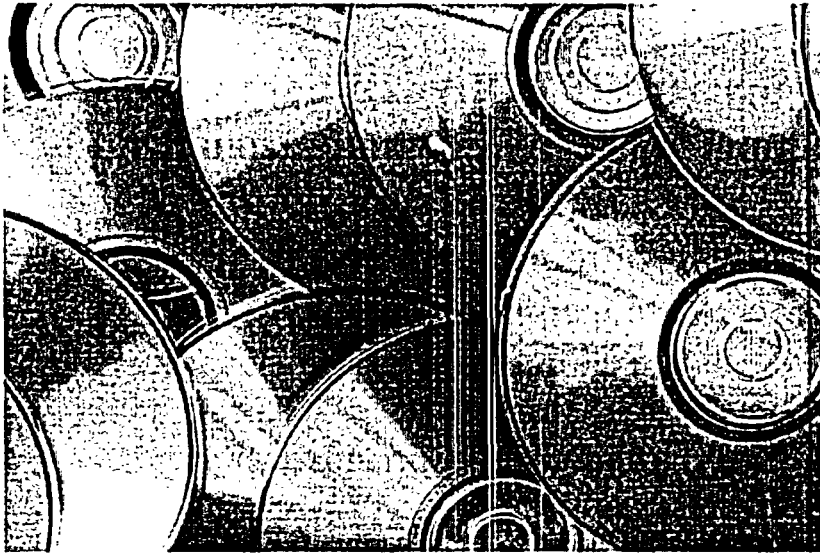
**Meeting with RF Gosatomnadzor  
July-August 2003**

**Wilkins Smith and Paul Loeser  
U.S. Nuclear Regulatory Commission**

A/5



# **Контроль качества программного обеспечения (ПО)**

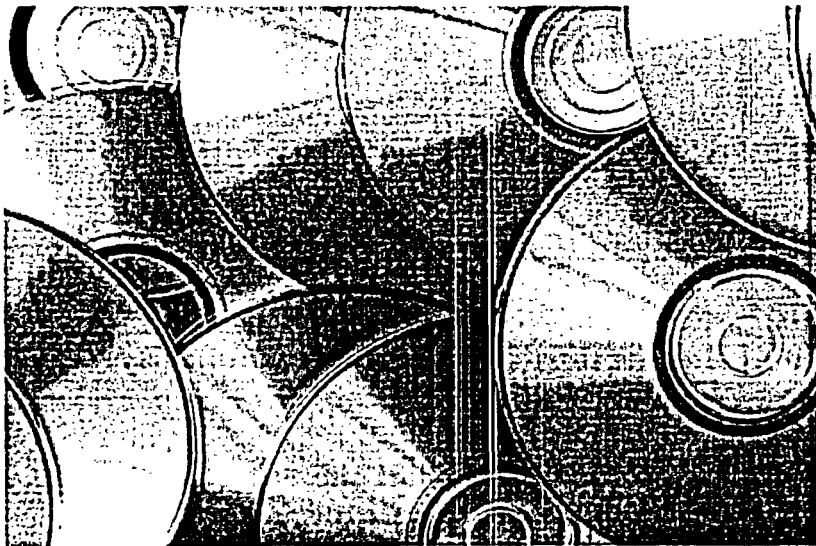


July 28 – August 1, 2003

SQC-3



# **Software Quality Control**



July 28 – August 1, 2003

SQC-4



## **Контроль качества ПО Описание**

- Требования
- Жизненный цикл ПО
- Верификация и валидация
- Управление конфигурацией ПО
- Конфигурационное управление ПО
- Процесс проведения экспертизы

July 28 – August 1, 2003

SQC-5



## **Software Quality Control Topics to be Covered**

- Requirements
- Software Life Cycle
- Verification and Validation
- Software Configuration Control
- Software Configuration Management
- Review Process

July 28 – August 1, 2003

SQC-6



## Требования к контролю качества ПО Установки по производству МОКС-топлива (УПМТ)

- Описание программы обеспечения качества
  - ASME NQA-1-1994, "Требования к обеспечению качества для ядерных установок" (отвечает требованиям 10 CFR 50, Приложение В, Требования к обеспечению качества реактора)
  - NQA-1, Часть I, Приложение IIS-2, "Дополнительные требования к тестированию компьютерных программ"
  - NQA-1, Часть II, раздел 2.7, "Требования к обеспечению качества компьютерного ПО для ядерных установок"
  - Относится к ПО, используемому для получения или обработки данных, непосредственно используемых при проектировании, анализе и эксплуатации
- Система конфигурационного управления
  - Относится ко всем сооружениям, системам, компонентам и изменениям

July 28 – August 1, 2003

SQC-7



## MOX Software Quality Control Requirements

- QA Program Description
  - ASME NQA-1-1994, "QA Requirements for Nuclear Facility Applications" (meets 10 CFR 50 Appendix B Reactor QA requirements)
  - NQA-1, Part I, Supplement IIS-2, "Supplementary Requirements for Computer Program Testing"
  - NQA-1, Part II, Subpart 2.7, "QA Requirements of Computer Software for Nuclear Applications"
  - Applies to software used to produce or manipulate data used directly in design & analysis and operation
- Configuration Management System
  - Applies to all structures, systems and components and changes

July 28 – August 1, 2003

SQC-8



## Нормативные требования КЯР для УПМТ

- Раздел 70.72, "Изменения в установке и процесс внесения изменений," требует создания лицензиатом системы конфигурационного управления для оценки, выполнения и прослеживания каждого изменения площадки, сооружений, процессов, систем, оборудования, компонентов, компьютерных программ и деятельности персонала

July 28 – August 1, 2003

SQC-9



## NRC MOX Regulatory Requirements

- Section 70.72, "Facility Changes and Change Process," requires that a licensee establish a configuration management system to evaluate, implement, and track each change to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel

July 28 – August 1, 2003

SQC-10



## **Что такое конфигурационное управление?**

- **Конфигурационное управление (КУ):**

Мера управления, которая обеспечивает надзор и контроль над проектно-конструкторской информацией, информацией по безопасности и записями о сделанных изменениях (как временных, так и постоянных), которые могут повлиять на способность элементов, важных для безопасности, выполнять при необходимости свои функции [10 CFR, Часть 70.4]

July 28 – August 1, 2003

SQC-11



## **What is Configuration Management?**

- **Configuration Management (CM) :**

management measure that provides oversight and control of design information, safety information and records of modifications (both temporary and permanent) that might impact the ability of items relied upon for safety to perform their functions when needed. [10 CFR Part 70.4]

July 28 – August 1, 2003

SQC-12



## **Что такое контроль качества ПО?**

- Эти термины являются в высокой степени взаимозаменяемыми

**Управление качеством ПО**

**= Обеспечение качества ПО**

**= Контроль качества ПО**

**= Разработка ПО**

July 28 – August 1, 2003

SQC-13



## **What is Software Quality Control**

- Terms are essentially interchangeable

**Software quality management**

**= Software QA**

**= Software QC**

**= Software Engineering**

July 28 – August 1, 2003

SQC-14



## Контроль качества ПО (ККПО)

- ККПО – это система управления, которая определяет, управляет, контролирует, исполняет, документирует и проверяет ПО на соответствие техническим и функциональным требованиям, т.е. КАЧЕСТВУ ПО

July 28 – August 1, 2003

SQC-15



## Software Quality Control (SQC)

- SQC is a management system to specify, guide, control, perform, document and verify that software meets the technical and functional requirements, i.e., the *QUALITY* of the software

July 28 – August 1, 2003

SQC-16





## **Рекомендации и стандарты по ККПО**

- “Типовая программа проведения экспертизы,” NUREG-1718, август 2000 г.
- Нормативное руководство 1.169, “Проект конфигурационного управления для цифрового компьютерного ПО, используемого в системах безопасности атомных станций”, сентябрь 1997 г.
- Техническое положение отдела РЯР (NRR) HICB-14, Ред. 4, июнь 1997 г., “Руководство по экспертизе ПО для цифровых компьютеризованных систем КИП и автоматики”
- “Стандарт IEEE по программе конфигурационного управления ПО,” стандарты IEEE 828 1990 и 1998

July 28 – August 1, 2003

SQC-17



## **SQC Guidance and Standards**

- “Standard Review Plan,” NUREG-1718, August 2000
- Regulatory Guide 1.169, “Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants,” September 1997
- NRR Branch Technical Position HICB-14, Rev. 4, June 1997, “Guidance on Software Reviews for Digital Computer-Based Instrumentation & Control Systems”
- “IEEE Standard for Software Configuration Management Plans,” IEEE Std. 828 1990 & 1998

July 28 – August 1, 2003

SQC-18



## **Деятельность КЯР по экспертизе и верификации ККПО**

- Экспертиза и утверждение Программы обеспечения качества (ПОК)
- Экспертиза обязательств ККПО в отношении КИП и А при выдаче разрешения на строительство
- Экспертизы и аудиты программ и инструкций по обеспечению качества (ОК)
- Инспекции на этапе строительства
- Экспертизы для выдачи лицензии на эксплуатацию
- Экспертиза готовности к эксплуатации
- Инспекции в процессе эксплуатации

July 28 – August 1, 2003

SQC-19



## **NRC SQC Review and Verification Activities**

- Review & approval of QA Plan
- Review of SQC commitments in construction authorization for I&C
- Reviews & audits of QA Program & procedures
- Inspections during construction
- Reviews for Operations License
- Operational readiness review
- Inspections during operations

July 28 – August 1, 2003

SQC-20



## **Контроль качества ПО**

- ККПО занимает много времени, дорого стоит, и обычно очень хлопотен
- Зачем же его проводить?
  - Чтобы убедиться в том, что системы безопасности работают!
- Хорошо известно, что сложное ПО всегда будет содержать ошибки
- ККПО увеличивает шансы получения качественного продукта

SQC-21



## **Software Quality Control**

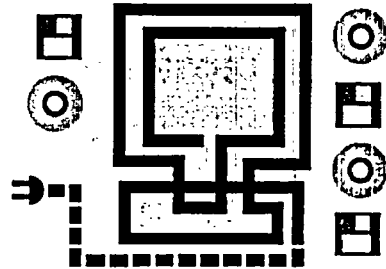
- SQC takes a lot of time, costs lots of money, and is generally a bother
- Why have it?
  - To make sure safety systems work!
- It is generally accepted that complex software will never be error free
- SQC improves the odds

SQC-22



## Контроль качества ПО (продолжение)

- Качество ПО следует из аккуратного и тщательного процесса разработки, с тестированием и верификацией каждого шага этого процесса и валидацией конечного продукта

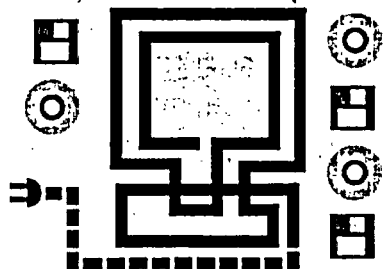


SQC-23



## Software Quality Control (continued)

- Software quality results from a careful and meticulous development process, thorough testing, verification of each step of the process, and validation of the product



SQC-24



## **Контроль качества ПО (продолжение)**

- Для того, чтобы процесс разработки был аккуратным и тщательным, весь процесс должен быть разбит на отдельные ступени
- Эти ступени также известны как жизненный цикл ПО

July 28 – August 1, 2003

SQC-25



## **Software Quality Control (continued)**

- In order to have a careful and meticulous development process, the process needs to be broken into various steps
- The various steps are also known as the software life cycle

July 28 – August 1, 2003

SQC-26



## Контроль качества ПО (продолжение)

- Одна модель жизненного цикла программы показана в стандарте IEEE 1012, “Стандарт IEEE на верификацию и валидацию ПО”



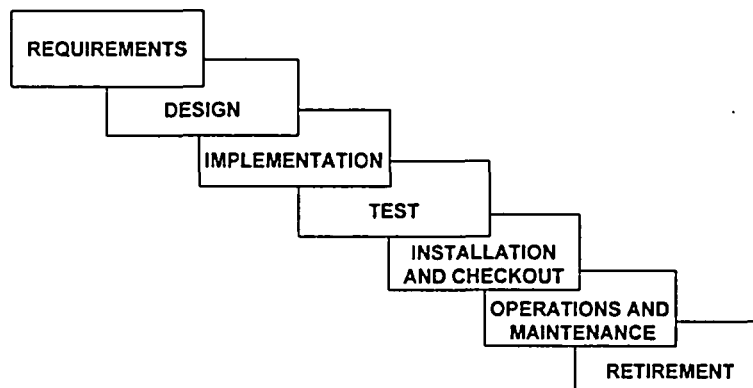
July 28 – August 1, 2003

SQC-27



## Software Quality Control (continued)

- One model of the software life cycle is shown in IEEE Std 1012, “IEEE Standard for the Software Verification and Validation”



July 28 – August 1, 2003

SQC-28



## **Контроль качества ПО (продолжение)**

- Эта версия жизненного цикла разбита на семь отдельных этапов:
  - Этап технических требований
  - Этап разработки
  - Этап реализации
  - Этап тестирования
  - Этап инсталляции и отладки
  - Этап эксплуатации и сопровождения
  - Этап вывода из эксплуатации

July 28 – August 1, 2003

SQC-29



## **Software Quality Control (continued)**

- This version of the life cycle has 7 separate phases:
  - Requirements Phase
  - Design Phase
  - Implementation Phase
  - Testing Phase
  - Installation and Checkout Phase
  - Operations and Maintenance Phase
  - Retirement Phase

July 28 – August 1, 2003

SQC-30



## **Этап технических требований**

- На этом этапе определяются, документируются и проверяются технические требования по следующим признакам:
  - функциональность
  - рабочие показатели
  - проектные ограничения
  - свойства
  - внешние интерфейсы

July 28 – August 1, 2003

SQC-31



## **Requirements Phase**

- This is where requirements are specified, documented, and reviewed for the following attributes:
  - functionality
  - performance
  - design constraints
  - attributes
  - external interfaces

July 28 – August 1, 2003

SQC-32





## **Этап технических требований (продолжение)**

- **Результаты этапа технических требований:**
  - Системная спецификация
  - Программа управления ПО
  - План разработки ПО
  - План обеспечения качества ПО
  - Программа конфигурационного управления ПО
- **Дополнительно на этом этапе подготавливаются планы для верификации и валидации (ВиВ) ПО**

July 28 – August 1, 2003

SQC-33



## **Requirements Phase (continued)**

- **Products of the requirements phase are:**
  - System Specification
  - Software Management plan
  - Software Development plan
  - Software Quality Assurance Plan
  - Software Configuration Management Plan
- **In addition, in this phase the plans for software verification and validation (V&V) are prepared**

July 28 – August 1, 2003

SQC-34



## **Этап разработки**

- На этапе разработки создается, документируется и оценивается проект ПО
- На этом этапе определяется общая структура как управления, так и информационных потоков, а также происходит сведение общей структуры к физическим решениям (алгоритмы, уравнения, управляющая логика и структура данных). Проект может потребовать внесения изменений в документацию, содержащую технические требования

July 28 – August 1, 2003

SQC-35



## **Design Phase**

- In the design phase, the software design is developed, documented, and reviewed
- Here, the overall structure, both control and data flow, will be specified, and the reduction of the overall structure into physical solutions (algorithms, equations, control logic, and data structures) will occur. The design may necessitate the modification of the requirements documentation

July 28 – August 1, 2003

SQC-36



## **Этап разработки (продолжение)**

- **Результаты этапа разработки:**
  - Спецификация требований ПО
  - Экспертиза требований ПО
  - Описание разработки ПО
  - Экспертиза разработки ПО



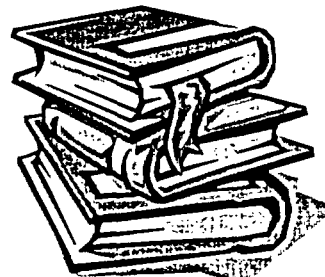
July 28 – August 1, 2003

SQC-37



## **Design Phase (continued)**

- **Products of the design phase are:**
  - Software Requirements Specification
  - Software Requirements Review
  - Software Design Description
  - Software Design Review



July 28 – August 1, 2003

SQC-38



## **Этап разработки (продолжение)**

- На этом этапе выполняются следующие работы по ВиВ:
  - Создание плана проведения испытаний, основанного на технических требованиях и разработке
  - Создание контрольных примеров на основании разработки
  - Экспертиза разработки ПО

July 28 – August 1, 2003

SQC-39



## **Design Phase (continued)**

- In this phase, V&V effort is:
  - generation of test plans based on the requirements and design
  - generation of design-based test cases
  - review of the software design

July 28 – August 1, 2003

SQC-40



## **Этап реализации**

- На этом этапе осуществляется программирование
- Результатами этапа реализации являются:
  - Листинг исходной программы
  - Экспертиза исходной программы
- На этом этапе работы по ВиВ заключаются в экспертизе исходной программы, а также ее проверке на соответствие стандартам и соглашениям программирования

July 28 – August 1, 2003

SQC-41



## **Implementation Phase**

- This is where coding takes place
- Products of the implementation phase are:
  - Source Code Listing
  - Source Code Review
- In this phase the V&V effort is source code review - also check for coding standards and conventions

July 28 – August 1, 2003

SQC-42



## **Этап тестирования**

- Это первый этап тестирования программного кода
- На этом этапе тестирование заключается в блочном тестировании отдельных частей программного кода
- Результатами выполнения этого этапа являются план проведения испытаний ПО и отчеты по тестированию

July 28 – August 1, 2003

SQC-43



## **Testing Phase**

- This is the first part of testing the code
- At this time, the testing is unit testing of individual parts of the software code
- Products of this phase are the Software Test Plan and testing reports

July 28 – August 1, 2003

SQC-44



## **Этап тестирования (продолжение)**

- **Работа по ВиВ на этом этапе :**
  - Валидация программного кода с целью проверки на соответствие требованиям
  - Убедиться в том, что ПО дает правильные результаты на контрольных примерах, то есть что оно работает

July 28 – August 1, 2003

SQC-45



## **Testing Phase (continued)**

- **V&V effort in this phase is:**
  - validation of the code to see if it meets the requirements
  - assure that the software produces correct results for the test cases (make sure it works)

July 28 – August 1, 2003

SQC-46



## **Этап инсталляции и отладки**

- На этом этапе различные компоненты ПО интегрируются с аппаратными средствами и данными и проходят тестирование как единая система. Сюда входят:
  - установка аппаратных средств
  - инсталляция программы
  - создание баз данных
  - тестирование системы
- Работа по ВиВ заключается в установке, проверке взаимодействия компонентов системы и приемочных испытаниях

July 28 – August 1, 2003

SQC-47



## **Installation and Checkout Phase**

- In this phase, the various software components are integrated with hardware and data, and tested as a system. This consists of:
  - installing hardware
  - installing the program
  - creating databases
  - testing the system
- V&V effort is installation and integration testing, and acceptance testing

July 28 – August 1, 2003

SQC-48





## **Этап эксплуатации и сопровождения**

- **Этот этап связан с сопровождением ПО после инсталляции и пуска**
  - **устранение скрытых ошибок (корректирующее сопровождение)**
  - **соответствие новым переработанным требованиям (профилактическое обслуживание)**
  - **адаптация ПО к изменениям в операционной среде (адаптивное сопровождение)**
- **На этом этапе работа по ВиВ заключается в утверждении и документировании изменений**

July 28 – August 1, 2003

SQC-49



## **Operations and Maintenance Phase**

- **This phase is concerned with the maintenance of the software once installed and running**
  - **to remove latent errors (corrective maintenance)**
  - **to respond to new or revised requirements (preventive maintenance)**
  - **to adapt the software to changes in the operating environment (adaptive maintenance)**
- **In this phase, the V&V effort is to approve and document changes**

July 28 – August 1, 2003

SQC-50



## Этап вывода из эксплуатации

- Произведите замену и выбросите старую версию



July 28 – August 1, 2003

SQC-51



## Retirement Phase.

- Replace it, and throw out the old stuff



July 28 – August 1, 2003

SQC-52



## **Верификация и валидация**

(Странно звучит, что кто-то другой должен проверить всю выполненную работу. Тем не менее, это должно быть сделано аккуратно и тщательно)

- **Верификация:** Подтверждение того, что результаты данного этапа удовлетворяют требованиям предыдущего этапа или этапов
- **Валидация:** Тестирование для подтверждения соответствия программного кода требованиям. Это делается с помощью составления и выполнения плана проведения испытаний и контрольных примеров для каждой фазы жизненного цикла ПО

July 28 – August 1, 2003

SQC-53



## **Verification and Validation**

(This is a fancy way of saying all the work should be checked by someone else. However, this must be done carefully and thoroughly)

- **Verification:** Ensure that the products of a given cycle phase fulfill the requirements of the previous phase or phases
- **Validation:** Testing to ensure that the code satisfies the requirements. This is done by writing and applying test plans and test cases into each phase of the software life cycle

July 28 – August 1, 2003

SQC-54



## **Верификация и валидация (продолжение)**

- Должна выполняться в процессе разработки и внесения изменений
- Предоставляет уверенность в реализации требований системы безопасности
- План ВиВ необходим для того, чтобы все знали, чего ожидать



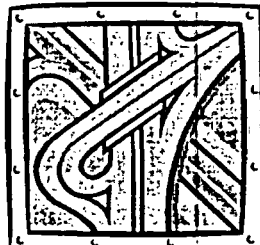
July 28 – August 1, 2003

SQC-55



## **Verification and Validation (continued)**

- Needs to be done during development and modification process
- Provides confidence that the safety system requirements have been implemented
- Need a V&V plan so everyone knows what to expect



July 28 – August 1, 2003

SQC-56



## **Верификация и валидация (продолжение)**

- План ВиВ перечисляет все действия и тесты, которые должны быть проверены, засвидетельствованы, выполнены или получили экспертную оценку
- Ключевой момент ВиВ – это использование людей, имеющих, по меньшей мере, такую же квалификацию, как и люди, выполнившие проектирование

July 28 – August 1, 2003

SQC-57



## **Verification and Validation (continued)**

- The V&V plan lists all activities and tests that shall be inspected, witnessed, performed, or reviewed
- Key to V&V is to have people who are at least as qualified as the people doing the design work

July 28 – August 1, 2003

SQC-58



## **Верификация и валидация (продолжение)**

- Организация, проводящая ВиВ, не должна зависеть от проектирующей организации
  - Независимость в управлении
  - Финансовая независимость
  - Независимость в составлении графика работ
- Это обеспечивает отсутствие давления на деятельность по ВиВ со стороны проектирующей организации

July 28 – August 1, 2003

SQC-59



## **Verification and Validation (continued)**

- V&V organization needs to be independent of design organization
  - Independent in management
  - Financially independent
  - Independent in schedule
- This ensures that the V&V activities are not compromised by pressure from the design organization

July 28 – August 1, 2003

SQC-60



## **Типичные работы по ВиВ**

### **Экспертиза документированных работ**

- **Засвидетельствование деятельности разработчика**
- **Проверки**
- **Сквозной контроль проектных решений**
- **Критический анализ программ**

July 28 – August 1, 2003

SQC-61



## **Typical V&V activities**

### **Reviews of documented work**

- **Witnessing of designer activities**
- **Inspections**
- **Design walkthroughs**
- **Code walkthroughs**

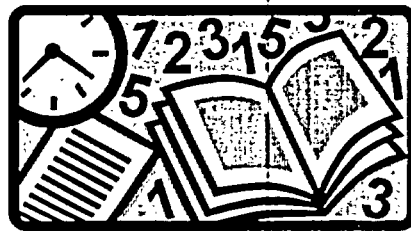
July 28 – August 1, 2003

SQC-62



## Типичные работы по ВиВ (продолжение)

- Сквозной контроль документированных результатов тестов
- Анализ – формальные доказательства, методы графического анализа и соответствующие методики
- Тестирование
  - Функциональное тестирование
  - Структурное тестирование



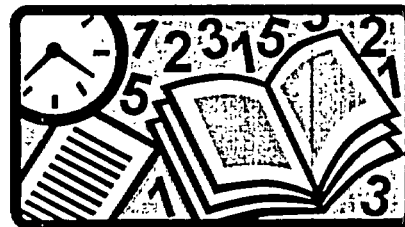
July 28 – August 1, 2003

SQC-63



## Typical V&V activities (continued)

- Walkthrough of documented test results
- Analysis - formal proofs, graphical analysis methods, and related techniques
- Testing
  - Functional testing
  - Structural testing



July 28 – August 1, 2003

SQC-64





## **Типичные документы, подлежащие экспертной оценке в ходе работ по ВиВ**

- Технические требования к системе
- Проект системы
- Требования к аппаратным средствам ЭВМ
- Программные требования
- Требования к взаимодействию компонентов системы
- Проектирование ПО

July 28 – August 1, 2003

SQC-65



## **Typical Documents Reviewed During V&V Activities**

- System requirements
- System design
- Computer hardware requirements
- Software requirements
- Integration requirements
- Software design

July 28 – August 1, 2003

SQC-66



## **Другие объекты, подлежащие экспертной оценке в ходе работ по ВиВ**

- Программная реализация и блочное тестирование
- Проверка взаимодействия компонентов системы
- Проверка валидации
- Проверка системы
- Планы эксплуатации и сопровождения
- Требования к надежности

July 28 – August 1, 2003

SQC-67



## **Other Items Reviewed During V&V Activities**

- Software implementation and unit testing
- Integration testing
- Validation testing
- System testing
- Operation and maintenance plans
- Reliability requirements

July 28 – August 1, 2003

SQC-68



## **Другие объекты, подлежащие экспертной оценке в ходе работ по ВиВ (продолжение)**

- Требования к интерфейсу
- Требования ко всем режимам эксплуатации, включая установку системы и ввод в эксплуатацию, проверку, нормальную эксплуатацию и эксплуатацию в аварийных условиях
- Возможности по обнаружению неисправностей, диагностике и восстановлению системы

July 28 – August 1, 2003

SQC-69



## **Other Items Reviewed During V&V Activities (continued)**

- Interfaces requirements
- Requirements in all operating conditions, including system installation and commissioning, test, normal operations, and emergency operation
- Fault detection, diagnostics, and recovery capabilities on the system

July 28 – August 1, 2003

SQC-70



## **Другие объекты, подлежащие экспертной оценке в ходе работ по ВиВ (продолжение)**

- Требования к интерфейсу оператор-машина
- Требования к синхронизации, времени отклика, пропускной способности и производительности
- Функциональное разнообразие или защита в глубину, по требованию

July 28 – August 1, 2003

SQC-71



## **Other Items Reviewed During V&V Activities (continued)**

- Operator/machine interface requirements
- Timing, response time, throughput, and performance requirements
- Functional diversity or defense-in-depth, as required

July 28 – August 1, 2003

SQC-72



## Отчеты о проблемах ВиВ

- Отчеты должны отслеживаться для обеспечения решения проблем
- Отчеты должны быть оформлены в письменном виде
- Отчеты должны включать следующую информацию:
  - Идентификация системы
  - Точный характер проблемы
  - Где обнаружена проблема – в каком программном модуле (например, в программе, задаче или подпрограмме) или в аппаратной части

July 28 – August 1, 2003

SQC-73



## V&V Problem Reports

- Reports need to be tracked to ensure that problems are solved
- These need to be written reports
- Reports should include the following information:
  - System identification
  - exact nature of the problem
  - Where the problem occurred - which software module (e.g., program, task, or subroutine) or hardware component

July 28 – August 1, 2003

SQC-74



## **Отчеты о проблемах ВиВ (продолжение)**

- **Отчеты должны включать следующую информацию:**
  - **Ситуация в момент отказа – что происходило**
  - **Длительность отказа (например, постоянный, периодический, переходный или не повторяющийся)**
  - **Механизм отказа (что именно произошло)**
  - **Указание механизма восстановления (устранение неисправности)**

July 28 – August 1, 2003

SQC-75



## **V&V Problem Reports (continued)**

- **Reports should include the following information:**
  - **Condition at time of failure - what was happening**
  - **Duration of failure (e.g., permanent, intermittent, transient, or could not duplicate)**
  - **Failure mechanism (what happened)**
  - **Identification of recovery mechanism (how did it get fixed)**

July 28 – August 1, 2003

SQC-76



## **Отчеты о проблемах ВиВ (продолжение)**

- **Отчеты должны включать следующую информацию:**
  - **Степень распространения неисправности (отдельный программный модуль, множественные программные модули, все модули ПО в одном компьютере, функция безопасности, все функции безопасности в одном канале или в нескольких каналах)**
  - **Основная причина, если она определена**
  - **Указание способа устранения неисправности**

July 28 – August 1, 2003

SQC-77



## **V&V Problem Reports (continued)**

- **Reports should include the following information:**
  - **Extent of failure (individual software module, multiple software modules, all software modules within a single computer, safety function, all safety functions within a channel, or multiple channels)**
  - **Root cause when determined**
  - **Identification of fix**

July 28 – August 1, 2003

SQC-78



## **Управление конфигурацией ПО**

- Основная конфигурация должна определяться по окончании каждого из основных этапов разработки ПО
- Утвержденные изменения, выполненные после разработки основной конфигурации, должны быть в нее добавлены
- Основная конфигурация должна определять самую последнюю из утвержденных конфигураций ПО

July 28 – August 1, 2003

SQC-79



## **Software Configuration Control**

- A configuration baseline shall be defined at the completion of each major phase of the software development
- Approved changes created subsequent to a baseline shall be added to the baseline
- A baseline shall define the most recent approved software configuration

July 28 – August 1, 2003

SQC-80





## **Управление конфигурацией ПО (продолжение)**

- Система присваивания обозначений элементам конфигурации должна применяться так, чтобы:
  - (a) однозначно определять каждый объект конфигурации
  - (b) определять изменения в объектах конфигурации с помощью обновлений
  - (c) позволять однозначно определить каждую конфигурацию обновленного ПО, подлежащего использованию

July 28 – August 1, 2003

SQC-81



## **Software Configuration Control (continued)**

- A labeling system for configuration items shall be implemented that:
  - (a) uniquely identifies each configuration item;
  - (b) identifies changes to configuration items by revision; and
  - (c) provides the ability to uniquely identify each configuration of the revised software available for use

July 28 – August 1, 2003

SQC-82



## **Управление конфигурацией ПО (продолжение)**

- Очень простая концепция – знаешь, что у тебя есть на данный момент, и следишь за этим
- Несмотря на кажущуюся простоту, эта концепция трудно выполнима
- ПО не является физическим объектом, и может существовать много копий одного и того же ПО
- Многие ошибки в ПО появляются по вине плохого конфигурационного управления
- Плохо, когда неправильное ПО тестируется, исправляется или устанавливается

July 28 – August 1, 2003

SQC-83



## **Software Configuration Control (continued)**

- A very simple concept - know what you have, and keep track of it
- The concept is simple, but the execution is difficult
- Software is not a physical thing, and many copies of the same software may exist
- Many software errors are traced to poor configuration management
- The wrong software is tested, fixed, or installed

July 28 – August 1, 2003

SQC-84



## **План конфигурационного управления ПО (КУПО)**

- Должен существовать в виде отдельного документа либо входить в другой проектный документ
- Определяет права и обязанности в рамках работ по КУПО
- Проектные организации, к которым применимо КУПО
- Обязанности этих организаций по КУПО
- Ссылки на стратегию и директивы КУПО, которые применимы к данному проекту

July 28 – August 1, 2003

SQC-85



## **Software Configuration Management (SCM) Plan**

- This needs to exist either in stand-alone form or embedded in another project document
- The plan will define the responsibilities and authorities for SCM activities
- the project organization(s) within which SCM is to apply
- the SCM responsibilities of these organizations
- references to the SCM policies and directives that apply to this project

July 28 – August 1, 2003

SQC-86



## Деятельность по КУПО

- Работы по КУПО традиционно группируются в четыре функции:
  - Определение конфигурации
  - Управление конфигурацией
  - Учет состояния
  - Аудиты и экспертизы конфигурации



July 28 – August 1, 2003

SQC-87



## SCM Activities

- SCM activities are traditionally grouped into four functions:
  - configuration identification
  - configuration control
  - status accounting
  - configuration audits and reviews



July 28 – August 1, 2003

SQC-88



## Определение конфигурации

- Определяет, дает наименование и описывает свойства кода, спецификации, разработку и элементы, которые должны контролироваться для выполнения данного проекта
- Регулируемыми элементами могут быть:
  - промежуточные и конечные продукты (такие как исполняемый код, исходный код, пользовательская документация или листинги программы)

July 28 – August 1, 2003

SQC-89



## Configuration Identification

- Identifies, names, and describes the characteristics of the code, specifications, design, and data elements to be controlled for the project
- Controlled items may be:
  - intermediate and final outputs (such as executable code, source code, user documentation, or program listings)

July 28 – August 1, 2003

SQC-90



## **Определение конфигурации (продолжение)**

- **Регулируемыми элементами могут быть:**
  - **базы данных**
  - **контрольные примеры**
  - **планы проведения испытаний**
  - **спецификации**
  - **планы управления**
  - **системное окружение (такое как компиляторы, операционные системы, инструментальные программные средства и испытательные стенды)**

July 28 – August 1, 2003

SQC-91



## **Configuration Identification (continued)**

- **Controlled items may be:**
  - **data bases**
  - **test cases**
  - **test plans**
  - **specifications**
  - **management plans**
  - **support environment (such as compilers, operating systems, programming tools, and test beds)**

July 28 – August 1, 2003

SQC-92



## Управление конфигурацией

- Все изменения в ПО должны быть занесены в документацию и содержать:
  - Определение и информацию о необходимых изменениях
  - Анализ и оценку запроса на внесение изменений
  - Утверждение запроса или отказ
  - Верификацию, имплементацию и внесение изменений
- Изменение должно быть оценено и одобрено до имплементации

July 28 – August 1, 2003

SQC-93



## Configuration Control

- All changes to software need to be documented and contain:
  - Identification and documentation of the need for a change
  - Analysis and evaluation of a change request
  - Approval or disapproval of a request
  - Verification, implementation, and release of a change
- The change must be evaluated and approved prior to implementation

July 28 – August 1, 2003

SQC-94



## **Учет состояния**

- Для ведения текущего перечня всех элементов конфигурации должна записываться следующая информация:
  - Утвержденная конфигурация
  - Состояние предложенных изменений в конфигурации
  - Состояние утвержденных изменений

July 28 – August 1, 2003

SQC-95



## **Status Accounting**

- In order to maintain a current list of all configuration items, the following information needs to be recorded:
  - the approved configuration
  - the status of proposed changes to the configuration
  - the status of approved changes

July 28 – August 1, 2003

SQC-96





## **Учет состояния (продолжение)**

- В плане управления конфигурацией (ПУК) должно быть перечислено, какие данные об элементах конфигурации должны быть собраны. Сюда должно входить следующее:
  - Данные по основной конфигурации и изменениям, которые должны прослеживаться и заноситься в отчет
  - Виды и периодичность требуемых отчетов о состоянии
  - Способы сбора, хранения, обработки и внесения в отчет информации
  - Управление доступом к данным о состоянии

July 28 – August 1, 2003

SQC-97



## **Status Accounting (continued)**

- The CMP should list what data will be collected on the configuration items. This list should included the following:
  - What data elements are to be tracked and reported for baselines and changes
  - What types of status accounting reports are to be generated and their frequency
  - How information is to be collected, stored, processed, and reported
  - How access to the status data is to be controlled

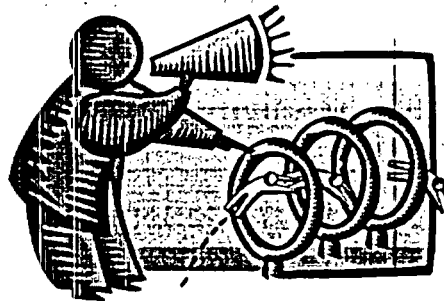
July 28 – August 1, 2003

SQC-98



## **Учет состояния (продолжение)**

- Точный уровень детализации и необходимые данные должны соответствовать нуждам конкретного проекта



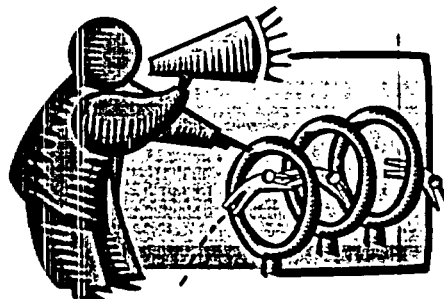
July 28 – August 1, 2003

SQC-99



## **Status Accounting (continued)**

- The exact level of detail and specific data required should be tailored to meet the needs of the specific project



July 28 – August 1, 2003

SQC-100



## **Проверки и экспертизы конфигурации**

- Проверки конфигурации показывают, насколько хорошо работает план конфигурационного управления при оформлении реальной конфигурации
- Эти проверки являются инструментами управления для создания основной конфигурации
- Для каждой проверки должна быть определена следующая информация:
  - Цели данной проверки
  - Элементы конфигурации, которые подлежат проверке или экспертизе

July 28 – August 1, 2003

SQC-101



## **Configuration Audits and Reviews**

- Configuration audits show how well the configuration management plan is working at recording the actual configuration
- These audits are management tools for establishing a baseline
- For each audit, the following information should be defined:
  - The objective of the audit
  - The configuration items to be audited or reviewed

July 28 – August 1, 2003

SQC-102



## **Проверки и экспертизы конфигурации (продолжение)**

- Для каждой проверки должна быть определена следующая информация :
  - Расписание проверки или экспертизы
  - Инструкции по проведению проверки или экспертизы
  - Кто будет выполнять проверку
  - Какая информация должна быть доступна для экспертизы или необходима для проведения проверки или экспертизы
  - Порядок записи любых обнаруженных недостатков и составления отчетов с корректирующими действиями

July 28 – August 1, 2003

SQC-103



## **Configuration Audits and Reviews (continued)**

- For each audit, the following information should be defined:
  - The schedule of audit or review
  - The procedures for conducting the audit or review
  - Who is to do the audit
  - What information is required to be available for review or to support the audit or review
  - The procedure for recording any deficiencies and reporting corrective actions

July 28 – August 1, 2003

SQC-104



## **Хватит теорий! Вот что мы действительно делаем**

Сначала, что мы не делаем:

- Мы не изучаем продукт и не определяем независимо, будет ли новая система выполнять, в случае необходимости, свою функцию безопасности
- Мы не проводим экспертизу ПО, мы проводим экспертизу процесса, с помощью которого это ПО разрабатывается
  - Реальная экспертиза потребует слишком много времени и усилий
  - Реальная экспертиза будет повторять ВиВ

July 28 – August 1, 2003

SQC-105



## **Enough Theory Here Is What We Actually Do**

First, what we do not do

- We do not examine the product or determine independently if the new system will perform the safety function when needed
- We do not review software, we review the process by which the software is developed
  - Actual review would take too much time and effort
  - Actual review would duplicate the V&V

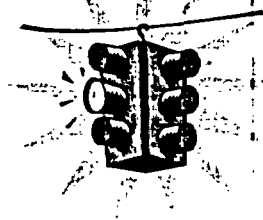
July 28 – August 1, 2003

SQC-106



## **Хватит теорий! Вот что мы действительно делаем**

- Мы полагаем, что лицензиат использовал правильный процесс разработки и тестирования системы, а если произойдет отказ этой системы, то мы полагаем, что разнопринципность и защита в глубину выполняют ту же функцию безопасности



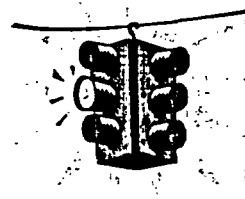
July 28 – August 1, 2003

SQC-107



## **Enough Theory Here Is What We Actually Do**

- We depend on the licensee using a good process to develop and test the system, and if that system fails, we depend on diversity and defense-in-depth to perform the same safety function



July 28 – August 1, 2003

SQC-108



## **Процесс проведения экспертизы Что мы действительно делаем**

- Мы проводим экспертизу процесса разработки ПО
  - Экспертиза системных спецификаций
  - Экспертиза проектирования системы
  - Экспертиза аппаратных и программных спецификаций
  - Экспертиза программы ВиВ
  - Экспертиза истории программного и аппаратного обеспечения
  - Проверка цепочки выполняемых задач для модельных параметров станции

July 28 – August 1, 2003

SQC-109



## **Review Process What We Actually Do**

- We review the process by which the software is written
  - review the system specifications
  - review of system design
  - hardware and software specifications
  - review of the V&V Program
  - review of software and hardware history
  - thread audit of sample plant parameters

July 28 – August 1, 2003

SQC-110



## **Процесс проведения экспертизы Что мы действительно делаем (продолжение)**

- Мы проводим экспертизу процесса разработки ПО
  - Экспертиза стандартов кодирования
  - Экспертиза систем ПО и аппаратного обеспечения по синхронизации или проблемам программно-аппаратного взаимодействия
  - Экспертиза программы тестирования и результаты тестов
  - Проверка квалификации сотрудников, которые разрабатывали систему, и сотрудников, выполнявших ВиВ

July 28 – August 1, 2003

SQC-111



## **Review Process What We Actually Do (continued)**

- We review the process by which the software is written
  - review the coding standards
  - software and hardware systems review for timing or software / hardware interface problems
  - look at the test program and test results
  - qualifications of the personnel who designed the system and those who did the V&V

July 28 – August 1, 2003

SQC-112





## **Процесс проведения экспертизы (продолжение)**

- Типичная оценка безопасности состоит в детальной экспертизе процесса проектирования системы и программы ВиВ ПО, с рассмотрением процесса проектирования системы с точки зрения программирования
  - Экспертиза доступной информации по истории программного и аппаратного обеспечения включая предыдущие неполадки программного и аппаратного обеспечения
  - Экспертиза определенных приложений включая любые необходимые специфические возможности

July 28 – August 1, 2003

SQC-113



## **Review Process (continued)**

- A typical safety evaluation is a detailed review of the system design process and the software V&V program, with a programmatic look at the design process
  - review available information on the software and hardware history including previous software and hardware failures
  - review the specific application including any special features that were required

July 28 – August 1, 2003

SQC-114



## **Экспертиза ВиВ**

- **Подробная экспертиза конкретной ВиВ программного обеспечения, которое используется в данном приложении, включает:**
  - **Наблюдение за разработкой программного кода**
  - **Изучение взаимодействия поставщик/лицензиат и процесса обратной связи**
  - **Экспертизу отчетов по проблемам/ошибкам ПО и внесению соответствующих поправок**
  - **Экспертизу процесса ВиВ с помощью опроса сотрудников, занятых в этом процессе**

July 28 – August 1, 2003

SQC-115



## **V&V Review**

- **Detailed review the specific V&V performed on the software used in the application includes:**
  - **following the code development**
  - **examining the vendor/licensee interface and feedback process**
  - **reviewing software problem/error reports and resulting corrections**
  - **review the V&V process interviewing personnel involved in the process**

July 28 – August 1, 2003

SQC-116



## **Экспертиза ВиВ (продолжение)**

- **Подробная экспертиза конкретной ВиВ программного обеспечения, которое используется в данном приложении, включает:**
  - Проверку независимости лиц, проводящих верификацию ПО
  - Экспертизу разработки функциональных требований и последующих документов по разработке ПО
  - Экспертизу жизненного цикла программы и будущего взаимодействия поставщик/лицензиат
  - Экспертизу результатов верификации и валидации

July 28 – August 1, 2003

SQC-117



## **V&V Review (continued)**

- **Detailed review the specific V&V performed on the software used in the application includes:**
  - verifying the independence of the software verifiers
  - reviewing the development of the functional requirements and subsequent software development documents
  - reviewing software life-cycle and future vendor/licensee interface
  - reviewing the verification and validation results

July 28 – August 1, 2003

SQC-118



## **Организация верификации и валидации**

**Ожидается:**

- **Независимость от группы разработчиков ПО**
  - **Независимые проверяющие инженеры**
  - **Сотрудники со сравнимой технической квалификацией**
- **Формализованная программа**

July 28 – August 1, 2003

SQC-119



## **Verification and Validation Organization**

**Look for:**

- **independence from the software development group**
  - **separate supervisory engineers**
  - **personnel with comparable technical qualifications**
- **formalized program**

July 28 – August 1, 2003

SQC-120



## **Организация верификации и валидации (продолжение)**

**Ожидается:**

- **Подробные инструкции и стратегии для:**
  - **Технической экспертизы**
  - **Функций проверки**
  - **Экспертиз и проверок ПО**
  - **Тестирования и анализа ПО**
  - **Динамической системы тестирования, моделирующей нормальные и проектные события**

July 28 – August 1, 2003

SQC-121



## **Verification and Validation Organization (continued)**

**Look for:**

- **detailed procedures and policies for:**
  - **technical review**
  - **audit functions**
  - **software reviews and audits**
  - **software test and analysis**
  - **dynamic system testing simulating normal and design basis events**

July 28 – August 1, 2003

SQC-122



## **Организация верификации и валидации (продолжение)**

**Ожидается:**

- **Документированная экспертиза программного кода**
- **Разработка контрольного примера**
- **Экспертиза аномального режима**
- **Определенная степень независимости группы исполнителей и процесса ВиВ**
- **План проведения испытаний для всех компонентов систем**

July 28 – August 1, 2003

SQC-123



## **Verification and Validation Organization (continued)**

**Look for:**

- **documented code reviews**
- **test case development**
- **abnormal conditions review**
- **the degree of independence of the V&V team and process**
- **test plans for all system components**

July 28 – August 1, 2003

SQC-124



## **Организация верификации и валидации (продолжение)**

**Ожидается:**

- Тестирование как часть процесса ВиВ, включая статическое и динамическое тестирование, а также типовые методики тестирования, такие как тестирование модульности, интеграции, регрессии и окончательной приемки, проводимое в течение всего процесса разработки
- Разработка следящей матрицы
- Сообщение об отклонениях и корректирующих действиях по их устранению

July 28 – August 1, 2003

SQC-125



## **Verification and Validation Organization (continued)**

**Look for:**

- tests as part of the V&V process, including static and dynamic testing, as well as standard testing methodologies such as unit, integration, regression, and final acceptance testing occurred throughout the development process
- the development of a tracking matrix
- discrepancy reporting and corrective action

July 28 – August 1, 2003

SQC-126



## **Экспертиза конфигурационного управления**

**Ожидается:**

- Строгий контроль над конфигурационным управлением
- Метод управления изменениями при разработке и официальном оформлении ВиВ
- Управление версиями исходного кода предварительного выпуска; управление версиями
- Запись истории и архивирование выпущенных проверенных модулей исходного кода; запись истории и архивирование верифицированных и валидированных модулей абсолютного программного кода

July 28 – August 1, 2003

SQC-127



## **Configuration Management Review**

**Look for:**

- strict configuration management control
- method for change control of development and V&V documentation
- version control of pre-released source code; version control
- historical recording and archiving of released verified source code modules; historical recording and archiving of verified and validated absolute code

July 28 – August 1, 2003

SQC-128





## **Экспертиза конфигурационного управления (продолжение)**

**Ожидается:**

- Управление производством программно-аппаратных средств
- Как и где хранится ПО в процессе конфигурационного управления
- Доступ к ПО
- Библиотекарь ПО (не должен быть разработчиком ПО)

July 28 – August 1, 2003

SQC-129



## **Configuration Management Review (continued)**

**Look for:**

- control of firmware manufacturing
- how and where the software under configuration management is stored
- access to the software
- software librarian (not a developer of the software)

July 28 – August 1, 2003

SQC-130



## **Проверка цепочки выполняемых задач**

- Единственный раз, когда мы в действительности рассматриваем программный код, это во время “проверки цепочки выполняемых задач”
- Эта цепочка заключается в выборе примерных параметров станции и прослеживании реализации ПО этих параметров, начиная от составления закупочной спецификации и разработки функциональных требований к написанию и тестированию программного кода

July 28 – August 1, 2003

SQC-131



## **Thread Audit**

- The only time we actually look at the software code is during the “thread audit”
- This consists of picking a sample of plant parameters and tracing the software implementation of these parameters from the purchase specification and development of the functional requirements to the writing and testing of the code

July 28 – August 1, 2003

SQC-132



## **Проверка цепочки выполняемых задач (продолжение)**

- **Проверка цепочки выполняемых задач  
состоит из:**
  - Экспертизы фактических разделов программного кода на выборочной основе
  - Проверки различных уровней документации по разработке ПО и ее сравнения с программным кодом
  - Проверки отчетов о найденных ошибках и верификации внесенных поправок
  - Проверки инженерных междотраслевых интерфейсов, чтобы убедиться в правильности учета потребностей ядерной энергетики в программном коде

July 28 – August 1, 2003

SQC-133



## **Thread Audit (continued)**

- **The thread audit consists of:**
  - reviewing actual sections of the code on a sample basis
  - examining the various levels of software development documents and comparing them to the code
  - examining problem reports and verifying the corrections
  - examining the engineering cross-discipline interfaces to ensure that nuclear specific needs were correctly incorporated into the code

July 28 – August 1, 2003

SQC-134



## **Проверка цепочки выполняемых задач (продолжение)**

- Проверка цепочки выполняемых задач состоит из:
  - Проверки интерфейса лицензиата с тем, чтобы убедиться в правильности учета конкретных требований
  - Обеспечения выполнения процесса ВиВ согласно плану поставщика
  - Экспертизы окончательных результатов данного процесса



July 28 – August 1, 2003

SQC-135



## **Thread Audit (continued)**

- The thread audit consists of :
  - examining the licensee interface to ensure specific requirements are correctly incorporated
  - ensuring that the V&V process is followed according to the vendor's plan
  - reviewing the final results of the process



July 28 – August 1, 2003

SQC-136



## **Документация, рассматриваемая при проведении экспертизы**

- **Спецификация системы**
  - Процессорная подсистема
  - Подсистема ввода-вывода
  - Тестовая подсистема
  - Прочие подсистемы, при необходимости

July 28 – August 1, 2003

SQC-137



## **Documentation Reviewed**

- **System Specification**
  - Processor subsystem
  - Input/Output Subsystem
  - Test Subsystem
  - Other Subsystems as needed

July 28 – August 1, 2003

SQC-138



## **Документация, рассматриваемая при проведении экспертизы (продолжение)**

- **Описание аппаратного обеспечения**
  - Физическое описание
  - Архитектура системы
  - Оценка качества окружающей среды
  - Температура и влажность
  - Сейсмическая квалификация
  - Радиация
  - Электромагнитное излучение/радиопомехи
  - Требования к качеству электроэнергии
  - Системы изоляции и взаимодействия, являющиеся системами безопасности и не относящиеся к системам, важным для безопасности

July 28 – August 1, 2003

SQC-139



## **Documentation Reviewed (continued)**

- **Hardware Description**
  - Physical description
  - System architecture
  - Environmental Qualifications
  - Temperature and Humidity
  - Seismic Qualification
  - Radiation
  - EMI / RFI
  - Power Quality requirements
  - Isolation and Interaction Safety and Non -safety systems

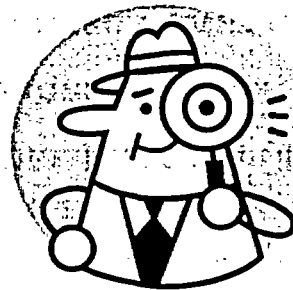
July 28 – August 1, 2003

SQC-140



## Экспертиза ПО

- **Описание ПО**
  - **Описание ввода-вывода ПО**
  - **Описание ПО для передачи данных**
  - **Описание ПО для тестирования и диагностики**



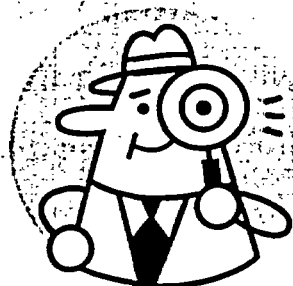
July 28 – August 1, 2003

SQC-141



## Software Review

- **Software Description**
  - **I/O Software Description**
  - **Communications Software Description**
  - **Test and diagnostic Software Description**



July 28 – August 1, 2003

SQC-142



## **Экспертиза ПО (продолжение)**

- **Документация по ПО**
  - Спецификация системы поставщик/заказчик
  - План управления разработкой и сопровождением ПО
  - План разработки ПО
  - Программа обеспечения качества ПО
  - План конфигурационного управления ПО
  - Спецификация аппаратного и программного обеспечения
  - Экспертиза требований к ПО

July 28 – August 1, 2003

SQC-143



## **Software Review (continued)**

- **Software Documentation**
  - Vendor / Customer System Specification
  - Software Management plan
  - Software Development plan
  - Software Quality Assurance Plan
  - Software Configuration Management Plan
  - Hardware and Software Specification
  - Software Requirements Review (SRR)

July 28 – August 1, 2003

SQC-144





## **Экспертиза ПО (продолжение)**

- **Документация по ПО**
  - Спецификация требований к ПО
  - Описание разработки ПО
  - Экспертиза проекта ПО
  - Листинги исходного кода
  - Экспертиза исходного кода

July 28 – August 1, 2003

SQC-145



## **Software Review (continued)**

- **Software Documentation**
  - Software Requirements Specification (SRS)
  - Software Design Description (SDD)
  - Software Design Review (SDR)
  - Source Code Listing
  - Source Code Review

July 28 – August 1, 2003

SQC-146



## **Экспертиза ПО (продолжение)**

- **Документация по ПО**
  - Анализ безопасности
  - План верификации и валидации ПО
  - Отчет по верификации и валидации
  - План тестирования ПО
  - Руководство пользователя

July 28 – August 1, 2003

SQC-147



## **Software Review (continued)**

- **Software Documentation**
  - Safety analyses
  - Software Verification and Validation Plan (SVVP)
  - Verification and Validation Report
  - Software Test Plan
  - User Instruction Manual

July 28 – August 1, 2003

SQC-148



## **Заключительная сессия вопросов и ответов**

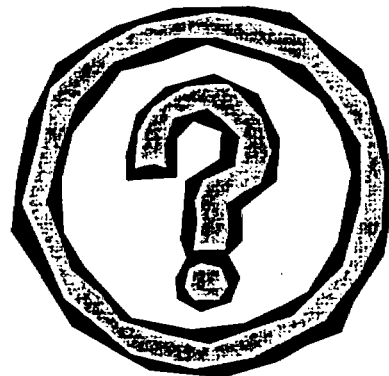


July 28 – August 1, 2003

SQC-149



## **End-of-Topic Questions-and-Answers Session**



July 28 – August 1, 2003

SQC-150